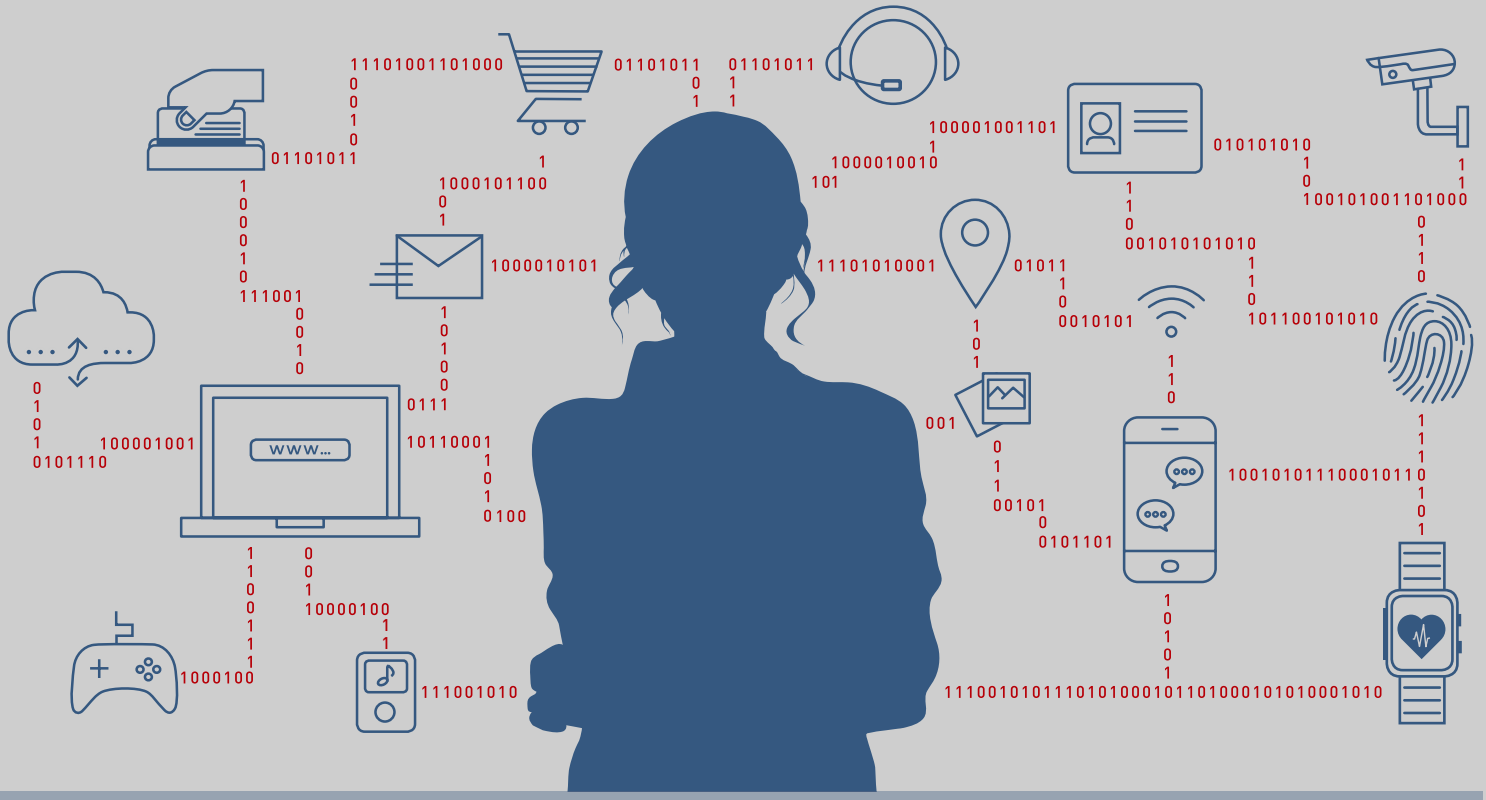
Leopoldina
Nationale Akademie
der Wissenschaften

acatech
DEUTSCHE AKADEMIE DER
TECHNIKWISSENSCHAFTEN

UNION
DER DEUTSCHEN AKADEMIEN
DER WISSENSCHAFTEN

2018
Stellungnahme

Privatheit in Zeiten der Digitalisierung



Nationale Akademie der Wissenschaften Leopoldina | www.leopoldina.org
acatech – Deutsche Akademie der Technikwissenschaften | www.acatech.de
Union der deutschen Akademien der Wissenschaften | www.akademienunion.de

Impressum

Herausgeber
Deutsche Akademie der Naturforscher Leopoldina e. V.
– Nationale Akademie der Wissenschaften –
Jägerberg 1, 06108 Halle (Saale)

Union der deutschen Akademien der Wissenschaften e. V.
Geschwister-Scholl-Straße 2, 55131 Mainz

acatech – Deutsche Akademie der Technikwissenschaften e. V.
Residenz München, Hofgartenstraße 2, 80539 München

Redaktion
Dr. Stefanie Westermann, Dr. Elke Witt
Nationale Akademie der Wissenschaften Leopoldina,
Abteilung Wissenschaft – Politik – Gesellschaft (Leitung: Elmar König)

Gestaltung und Satz
unicommunication.de, Berlin
Titelbild: Sisters of Design - Anja Krämer & Claudia Dölling GbR, Halle (Saale)

Druck
druckhaus köthen GmbH & Co. KG
Friedrichstr. 11/12
06366 Köthen (Anhalt)

Lektorat
Katharina Schmalz, Regensburg

ISBN: 978-3-8047-3642-9

Bibliografische Information der Deutschen Nationalbibliothek
Die deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie, detaillierte bibliografische Daten sind im Internet unter http://dnb.d-nb.de abrufbar.

Zitiervorschlag:
Nationale Akademie der Wissenschaften Leopoldina (2018):
Privatheit in Zeiten der Digitalisierung. Halle (Saale).

Privatheit in Zeiten der Digitalisierung

Inhaltsverzeichnis

1 Hintergrund und Ziel der Stellungnahme

Als der Begriff des „Privaten“ im 16. Jahrhundert in der deutschen Sprache geprägt wurde, umfasste er jene Bereiche des Lebens, die dem Zugriff und der Herrschaftsgewalt des Staates bzw. der Öffentlichkeit entzogen waren.[1] Heute gilt Privatheit als ein wesentlicher Schutz- und Rückzugsraum, den für sich zu definieren und in Anspruch zu nehmen jeder Einzelne das Recht hat und in den weder der Staat noch ein Unternehmen, noch eine Privatperson ohne Einwilligung eindringen darf, soweit nicht gesetzlich eine Ausnahme vorgesehen ist. Das Recht auf Privatheit zählt zu den Freiheitsrechten. Es wird als wichtige Grundlage für die freie Entwicklung und Entfaltung der Persönlichkeit, aber auch der politischen Partizipation begriffen (► Box „Privatheit“).

Allerdings zeichnet sich seit einigen Jahren ab, dass die Digitalisierung, die mit einem enormen Austausch und der Auswertung von Daten einhergeht, es dem Einzelnen immer weiter erschwert, die Bereiche seiner Privatheit aufrechtzuerhalten und ihre Einhaltung zu kontrollieren. In der gemeinsamen Arbeitsgruppe von Leopoldina, Akademienunion und acatech „Privatheit in Zeiten der Digitalisierung“ sind Wissenschaftlerinnen und Wissenschaftler aus dem Bereich der Informatik und Informationstechnik sowie den Rechts-, Geistes-, Politik- und Gesellschaftswissenschaften zusammengekommen, um gemeinsam über ein besonders wichtiges Folgeproblem der Digitalisierung zu reflektieren: die Frage, wie Räume für Privatheit technisch und regulatorisch bewahrt werden können.

Digitalisierung bezeichnet nicht nur die rasante Entwicklung einer Technologie, sondern auch deren zeitgleiche Integration in nahezu alle Lebensfelder. In ihrer ursprünglichen Bedeutung bezeichnete „Digitalisierung“ die Darstellung von Signalen aller Art in computerlesbarer Form. Heute hat sich der Begriff zur Charakterisierung aller Vorgänge der maschinellen Verarbeitung, der automatischen Informationsübermittlung sowie der Wiedergabe von Informationen an Mensch und Maschine durchgesetzt (► Box „Digitalisierung“). Es gibt kaum ein anderes Gebiet, in dem neue Entwicklungen so schnell in die Anwendung gelangen und dabei gleichzeitig so großes ökonomisches Potential entfalten.

Insbesondere „Big Data“ eröffnet viele neue Anwendungsfelder (► Box „Big Data“). Charakteristisch hierfür sind das große Datenvolumen und die Möglichkeiten zur Verknüpfung und Vernetzung unterschiedlicher Daten. Aus massiven Datenmengen werden hier – unter Verwendung von Algorithmen und z. T. auch Hochleistungsrechnern – Zusammenhänge erkennbar, welche weit über das Wahrnehmungs- und Urteilsvermögen des einzelnen Menschen hinausgehen. Durch automatisierte Analyseprozesse können komplexe Zusammenhänge besser modelliert und verstanden werden, was zu verbesserten Vorhersagen, informierten Handlungsempfehlungen, automatischen Entscheidungen und – ultimativ – zu neuem Wissen führen kann.

Digitalisierung im Allgemeinen und Big Data im Besonderen bringen eine Fülle

1 Eintrag „privat“, bereitgestellt durch das Digitale Wörterbuch der deutschen Sprache, abgerufen am 17. *Juli* 2018 von https://www.dwds.de/wb/privat.

neuer, bislang nicht gekannter Möglichkeiten mit sich: Eine digitale Umgebung macht Information zum neuen, nahezu unbegrenzten Rohstoff, virtuelle Welten bieten ein ungekanntes Ausmaß an Erweiterungsmöglichkeiten unserer vertrauten Realität und intelligente, lernfähige Systeme stellen vielfältige Entlastungen im Alltag sowie neue Dienstleistungen und Produktionsprozesse in Aussicht.

Dies gilt insbesondere auch für die Industrie, für deren Entwicklungs-, Produktions- und Wartungsprozesse und auch für die Interaktion mit den Kundinnen und Kunden. Die Digitalisierung, wie sie z. B. im Rahmen von Industrie-4.0-Konzepten auf der Grundlage des Internet of Things (IoT) alle Bereiche von Unternehmen durchdringt,[2] ermöglicht über eine Produktivitätssteigerung hinaus die Entwicklung neuer Geschäftsmodelle. Darüber hinaus ergibt sich ein Marktzugang für neue Unternehmen, die Datenanalysen z. B. mit Methoden der Statistik oder des Maschinellen Lernens als Serviceleistung anbieten.

Die Digitalisierung bringt auch neue Risiken mit sich, insbesondere im Hinblick auf die Grundrechte in einer demokratisch verfassten Zivilgesellschaft, in Bezug auf den Wettbewerb zwischen Wirtschaftsunternehmen und die voranschreitende Transformation der Arbeitswelt sowie durch einen allgemeinen Verlust an Transparenz.

Durch die Digitalisierung sind neue, weltweit agierende Unternehmen entstanden, die mithilfe ihrer Angebote und der Daten ihrer Kundinnen und Kunden enormes ökonomisches Gewicht und die Möglichkeit zur Einflussnahme auf das Verhalten von Menschen gewonnen haben. Dies reicht bis hin zur Beeinflussung politischer Entscheidungen, z. B. bei Wahlen. Dienstleistungen wie die Bereitstellung von Suchmaschinenfunktionen, die soziale Vernetzung im Freundes- und Bekanntenkreis, die vereinfachte Kommunikation und Mobilität sind in der modernen Welt für die meisten Menschen unverzichtbar geworden. Jedoch sind diese Dienste nur scheinbar kostenlos, denn sie werden mit der Preisgabe privater Informationen der Nutzerinnen und Nutzer gegenüber den Unternehmen bezahlt.

Nicht nur Unternehmen, auch staatliche Institutionen nutzen die Vorteile der Digitalisierung. Digitale Verwaltungssysteme (E-Government)[3] können Verwaltungsvorgänge für Behörden wie für Bürgerinnen und Bürger erheblich vereinfachen und dabei helfen, bürokratischen Aufwand und Hürden zu minimieren. Zudem werden digitale Möglichkeiten im Bereich der Sicherheit eingesetzt. Nationale und internationale Behörden vernetzen ihre Datenbanken und nutzen die Möglichkeiten, die ihnen die Auswertung des elektronischen Datenverkehrs, mobiler Kommunikation und anderer digitaler Datenquellen zur Kriminalitätsbekämpfung und Terrorismusabwehr bieten. Als Risiken werden allerdings unerwünschte Eingriffe in die Privatsphäre und unrechtmäßige Beschneidungen der persönlichen Freiheiten der Bürgerinnen und Bürger befürchtet.

2 Siehe dazu: Kagermann, Wahlster & Helbig (2013) sowie Kagermann, Riemensperger, Hoke, Helbig & Stocksmeier (2014).

3 UN (2016).

Begriff der Privatheit

Privatheit wird in vielen Kulturen als ein gesellschaftlich wichtiges Schutzgut angesehen, auch wenn die Definition dessen, was als privat schützenswert ist, kulturell, historisch und kontextbezogen variiert.[4] Was unter dem Privaten zu verstehen ist, wird in der Privatheitsforschung nicht einheitlich definiert.[5] Weitgehend Konsens besteht darin, dass Privatheit bedeutet, dass jede Person grundsätzlich das Recht hat, Bereiche des eigenen Lebens zu definieren, zu denen andere Menschen nicht ohne Weiteres Zugang haben, z. B. die eigene Wohnung, private Aufzeichnungen und persönliche Informationen. Es geht dabei in erster Linie um die Kontrolle, die eine Person darüber haben sollte, wer wann in welchem Maße und in welchem Zusammenhang auf von ihr als privat definierte Bereiche zugreifen kann. Privatheit lässt sich somit nicht nur in lokaler, sondern auch in informationeller und dezisionaler, d. h. Entscheidungen betreffender Hinsicht, verstehen.[6] Ein weiteres Kriterium der Privatheit ist ihre Kontextrelevanz: Eine Person kann selbst entscheiden, welchem Personenkreis sie zu welchem Zeitpunkt Einblick in persönliche Bereiche gewährt.[7]

Das Recht auf Privatheit findet sich z. B. in der „Allgemeinen Erklärung der Menschenrechte“, in der „Charta der Grundrechte der Europäischen Union“ (EU-Grundrechtecharta) und im „Grundgesetz der Bundesrepublik Deutschland“ (GG). Mit dem Recht auf informationelle Selbstbestimmung wurde vom Bundesverfassungsgericht (BVerfG) 1983 die informationelle Privatheit in Deutschland verfassungsrechtlich verankert. Dieses Recht gibt dem Einzelnen die Befugnis, selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen. Im Big-Data-Zeitalter haben sich die Rahmenbedingungen für den Schutz der Privatheit fundamental geändert; niemals zuvor war die potentielle Zugänglichkeit zu privaten Informationen größer.

Zurzeit wächst auch bei Wissenschaftlerinnen und Wissenschaftlern, die dieses Forschungsfeld seit Jahren oder Jahrzehnten prägen, die Sorge vor Fehlentwicklungen, die – bei allem bestehenden und noch zu erwartenden Nutzen – dem Einzelnen und der Gesellschaft Schaden zufügen könnten. Dies hängt auch mit der Geschwindigkeit des Fortschritts sowie der Durchdringungstiefe digitaler Anwendungen zusammen, denn Digitalisierung erfasst und verändert unser gesamtes sozioökonomisches System: Dies beginnt bei veränderten Formen und Foren zwischenmenschlicher Begegnung und gesellschaftlicher Partizipation durch neue Medien, setzt sich fort in einem nie da gewesenen Grad an weltweiter Vernetzung mit großen Auswirkungen auf Märkte und die Interaktionsdynamik ihrer Marktteilnehmer und reicht bis zu der Durchdringung unserer individuellen Lebensräume.

Durch die Komplexität und die Geschwindigkeit dieser Entwicklungen werden die möglichen negativen Aspekte digitaler Entwicklungen von vielen Nutzerinnen und Nutzern, aber auch von politischen Entscheidungsträgern wahrgenommen, als seien sie kaum beherrschbare Naturgewalten: Geschehen sie, ist man ihnen ausgeliefert und kann allenfalls im Nachgang versuchen, entstandene Schäden zu begrenzen. Diese Einschätzung ist jedoch fatal. Vielmehr gibt es zahlreiche Möglichkeiten, in die Gestaltung unserer digitalen Zukunft einzugreifen, Regelungen zu etablieren, Standards und Kontrollverfahren einzusetzen oder auch alternative digitale

4 Vgl. EMC Privacy Index 2014, DELL EMC (2014).
5 Mönig (2017), S. 19–35; Rössler (2001).
6 Rössler (2001).
7 Nissenbaum (2010).

Technologien zu entwickeln. Und statt lediglich auf eine von außen vorgegebene Dynamik zu reagieren, können diese Eingriffe in ihrer Wirkung formend sein: Durch eine entsprechende Rahmensetzung sind Regulierung und Gesetzgebung einerseits so anzupassen, dass die Interessen der Bürgerinnen und Bürger geschützt und nachteilige gesellschaftliche Auswirkungen verhindert, gleichzeitig aber die Potentiale neuer Technologien für Bürgerinnen und Bürger, Unternehmen und Staat weitreichend erschlossen werden können. Ziel muss es dabei sein, das Recht des Einzelnen zu schützen und nachteilige gesellschaftliche Auswirkungen zu verhindern.

Mit der vorliegenden Stellungnahme möchten die Akademien verschiedene Handlungsoptionen auf technischer und regulatorischer Ebene aufzeigen, um auch in Zeiten zunehmender Digitalisierung einen Schutz der Privatsphäre zu realisieren. Dabei ist der Schutz der Rechte von Nutzerinnen und Nutzern sowie ihrer Privatsphäre nicht als Hemmnis für wirtschaftliche Entwicklung und als ein Beschneiden der Möglichkeiten der Digitalisierung zu begreifen. Vielmehr kann – neben dem Schutz von Grundrechten als Wert an sich – die Umsetzung von Nutzerrechten langfristig einen Standortvorteil schaffen, da sie das Vertrauen der Nutzerinnen und Nutzer in private Anbieter ebenso wie in staatliche Institutionen ermöglicht. Ein solches Vertrauen ist eine der Voraussetzungen für die Nachhaltigkeit und langfristige Akzeptanz der Digitalisierung.[8]

Die drei Systemebenen der Digitalisierung

Bei der Nutzung digitaler Angebote interagieren die Verbraucherinnen und Verbraucher mit drei Systemebenen: zum einen der Benutzeroberfläche des von ihnen ausgewählten Dienstes wie z. B. Google, die ihnen die gewünschte Leistung zur Verfügung stellt, in diesem Fall Informationen. Darunter liegt die Ebene der Rechenprozesse und Algorithmen, die für die Umsetzung ihrer Suchanfrage nötig sind. Diese wiederum werden durch physische, technische Systeme als unterste Ebene realisiert. Hierzu zählen die Endgeräte der Verbraucherinnen und Verbraucher, z. B. ihr Smartphone, wie auch die über die ganze Welt verteilten Großrechner und Speicher, in welchen die Rechenprozesse stattfinden.

Auf jeder dieser drei Systemebenen besteht die Möglichkeit, Einstellungen vorzunehmen, die beeinflussen, in welcher Art die für das Gesamtsystem verfügbaren Daten genutzt werden (Datenschutz), wie viel die Nutzerinnen und Nutzer darüber erfahren (Transparenz) und ob die Daten nur für diese geplante Nutzung zugänglich sind (Datensicherheit).

Dabei sind die Dienste oft auch in mehrere Prozessschritte unterteilt, z. B. Anmeldung, Anlegen und Aktualisieren von Accounts, Übertragung und Navigation in Angeboten. Diese Prozessschritte wiederum können hinsichtlich Verschlüsselungs- und Authentifizierungsmechanismen, Gestaltung von Zugriffsrechten, Ausmaß und Speicherung übermittelter Informationen uvm. in vielfältiger Weise gestaltet werden – mit entsprechend weitreichenden Unterschieden in Hinblick auf die damit verbundenen Transparenz-, Sicherheits- und Datenschutzgrade.

Um den Schutz von Privatheit im Zeitalter der Digitalisierung zu etablieren, ist es daher wesentlich, alle Prozessschritte auf den drei Systemebenen und deren jeweilige Verknüpfungen zu berücksichtigen.

8 Zum Stichwort „Vertrauen“ siehe auch acatech (2013).

2 Digitalisierung

Seit den 1970er-Jahren wurde die Integrationsdichte von Halbleiterchips – und damit die Speicherkapazität und Rechenleistung – um mehr als das Millionenfache gesteigert. Ähnliche Steigerungsfaktoren sind auch für den Umfang von Datenströmen im Internet zu verzeichnen. In der Folge wandelt sich nun auch der Charakter nahezu aller Systeme der technisierten Umwelt: Haushaltsgeräte werden zu vernetzten Datenquellen im Internet, bislang passive Maschinen zu wahrnehmungsfähigen Agenten mit wachsenden Fähigkeiten, autonom zu handeln und sogar zu lernen. Neben der vertrauten physikalischen Realität entwickeln sich vielfältige virtuelle „Biotope", zu denen wir erst über technische Hilfsmittel wie z. B. Smartphones oder Virtual-Reality-Brillen Zugang gewinnen.

Eines der grundlegenden Merkmale des digitalen Wandels ist die zunehmende Spiegelung der realen Welt, d. h. der sich im physischen Interaktionsraum abspielenden Lebenswelt, in einer digitalen Welt. Eine Vielzahl von Informationen wird aktiv von den Nutzerinnen und Nutzern in sozialen Netzwerken wie Facebook, Twitter oder Instagram eingestellt, andere Informationen werden wiederum generiert durch die Nutzung digitaler Services wie Kreditkartenzahlung oder E-Tickets für Bus und Bahnen. Weitere Informationen werden täglich durch verschiedene digitale Endgeräte gesammelt: Smartphones z. B. melden ihren momentanen Standort an die Netzbetreiber oder geben ihre GPS-Koordinaten über Apps an Dienstanbieter weiter. Es ist davon auszugehen, dass diese Daten schon derzeit dazu genutzt werden, von nahezu allen Menschen in den Industrienationen und den meisten Schwellenländern ein „digitales Spiegelbild" in der Datenwolke (Cloud) zu erstellen.[9] Dieses Spiegelbild enthält weitreichende Informationen über die Aktivitäten, Vorlieben und das soziale Leben und kann u. a. genutzt werden, um etwa soziale Netzwerke in ihren Funktionen zu erweitern, um Angebote wie Verkehrsleitsysteme, die sich an das Verkehrsaufkommen in Echtzeit anpassen, zu entwickeln und um neue Produkte zu kreieren. Insbesondere aber werden diese Informationen auch verwendet, um Marketing effektiver zu gestalten und Werbeangebote, die oftmals webbasierte Dienstleistungen finanzieren, personalisiert zu platzieren.

Die Überführung der Lebenswelt der Nutzerinnen und Nutzer in die Welt der digitalen Daten macht jedoch das Leben jedes einzelnen Menschen auswertbar. Denn mit der Digitalisierung haben sich nicht nur die Möglichkeiten zur Erfassung und Speicherung von Daten gewandelt. Parallel dazu wurden auch neue Methoden entwickelt, um die erfassten Daten miteinander in Beziehung zu setzen und zu analysieren. Der gesamte Datenanalyseprozess umfasst dabei mehrere Teilschritte. Dies sind in der Regel:

1. Identifikation von Datenquellen,

2. Datenaufbereitung (inklusive Informationsextraktion und Integration heterogener Datenquellen),

3. Analyse und Modellbildung sowie

9 Anschaulich macht dies ein Experiment, das Malte Spitz gemeinsam mit ZEIT ONLINE durchführte, in welchem anhand der Vorratsdaten, die über Spitz 6 Monate lang gespeichert wurden, detaillierte Bewegungsmuster errechnet wurden; Spitz (2009).

4. Anwendung der Modelle und ggf. Rückkopplung der Ergebnisse in die Datenquellen.

Die entsprechenden Datenmanagement-Technologien werden meist unter dem Begriff „Big Data“ zusammengefasst (► Box „Big Data“). Mithilfe der Methoden des Maschinellen Lernens[10] (► Box „Maschinelles Lernen“) sind Computer in der Lage, aus einer Vielzahl von Informationen auf Gemeinsamkeiten zu schließen und aus der Verknüpfung intelligente Schlüsse zu ziehen – Fähigkeiten, die bislang Menschen vorbehalten waren. Dies ermöglicht die Entwicklung zahlreicher innovativer datengetriebener Anwendungen mit enormem Potential: Die sog. Datenwissenschaften (Data Sciences) und insbesondere Big Data Analytics nutzen die Möglichkeit, ungeheure Datenmengen nach Mustern und Regelmäßigkeiten zu durchsuchen, die Menschen bislang aufgrund der Komplexität oder der schieren Menge der Daten verborgen bleiben. Davon profitieren Wissenschaftsfelder wie Meteorologie, Astronomie, Chemie, Physik, Neurowissenschaften, Genetik, Materialwissenschaften, Medizin, aber auch Geisteswissenschaften und Sozialwissenschaften (Digital Humanities). Technologien des Maschinellen Lernens kommen u. a. in der Sprach-, Bild- oder Gesichtserkennung zum Einsatz, in den Ingenieurwissenschaften sind sie inzwischen ebenso etabliert wie etwa in der Finanzwirtschaft oder der Pharmazeutik. In der Wirtschaft werden sie heute u. a. schon zur Optimierung der Logistik, der Nutzerfreundlichkeit sowie von Systemen und Prozessen in der Produktentwicklung und der Produktion genutzt.

Software und Geräte, die auf der Basis Maschinellen Lernens arbeiten, sind immer mehr in der Lage, innerhalb ihrer Funktionsbereiche autonom zu agieren und sinnvoll mit Menschen zu interagieren. Technische Systeme werden als „autonom“ bezeichnet, wenn sie ohne menschliche Eingriffe technische Leistungen erbringen, die komplexe Entscheidungen erfordern (► Box „Autonome technische Systeme“). Dazu müssen autonome Systeme in der Lage sein, die für sie wichtigen Weltausschnitte wahrzunehmen und zu interpretieren. Autonome Webagenten können beispielsweise Postings im Internet beobachten und eigene Texte einbringen, autonome Fahrzeuge können Straßenszenen verfolgen, ein Smart Home kann die Handlungen seiner Bewohner erkennen. Die für solche Kontexte erforderlichen Wahrnehmungs- und Interpretationsfähigkeiten sind für unterschiedliche autonome Systeme typischerweise anwendungsabhängig verschieden, in vielen Fällen – gerade wenn es auf die Interaktion mit Menschen ankommt – aber stark an den menschlichen Wahrnehmungsmodalitäten Sehen und Hören orientiert und meist auf menschliche Handlungsfelder ausgerichtet (Wohnungen, öffentliche Räume, Straßen, Internet). Durch ihre Wahrnehmungsfähigkeiten werden autonome Systeme damit auch zu Beobachtern menschlichen Handelns. Das Zusammentreffen der Fähigkeiten autonomes Beobachten, leistungsfähiges Gedächtnis/Verständnis und Vernetzung macht autonome Systeme zu einer großen Herausforderung für die Privatsphäre aller Menschen in ihrem Umfeld. Die zusätzliche Dimension Beweglichkeit trägt zu einer Verschärfung des Problems bei, da z. B. fliegende Drohnen sehr viel agiler beobachten können, als es beispielsweise ein Mensch könnte.

Der Einsatz von Verfahren des Maschinellen Lernens führt zu verschiedenen Konfliktfeldern. Es kann bei dieser Form der Zusammenführung von Daten zu einer Aufhebung von Anonymität kommen: So lässt sich beispielsweise selbst bei anonymisierten Daten ein Datenpunkt oft eindeutig

10 „Maschinelles Lernen“ („Machine Learning“) wird häufig als ein spezifischer Ansatz innerhalb der künstlichen Intelligenz betrachtet. Im folgenden Text wird der Begriff des Maschinellen Lernens genutzt, wie er in der Box „Maschinelles Lernen“ eingeführt wird.

Big Data

Grundsätzlich befasst sich Datenmanagement mit methodischen, organisatorischen und technischen Maßnahmen und Verfahren zur Verwaltung und Analyse von Daten. Durch Big Data entsteht eine neue Komplexität, sowohl im Hinblick auf die zu verarbeitenden Datenströme als auch auf die durchzuführenden Analysen. Es bestehen gestiegene Anforderungen an Datenvolumen (Volume), Datenrate (Velocity), Datenheterogenität (Variety) und Datenqualität (Veracity), die von traditionellen – relationalen – Datenbanksystemen nicht abgedeckt werden. Durch den Einsatz von komplexen Algorithmen der Datenanalyse (Data Mining) werden aus Daten Modelle abgeleitet, die Einsichten oder Vorhersagen generieren. Dabei kommen insbesondere statistische Verfahren, Maschinelles Lernen, lineare Algebra und Optimierung, Signalverarbeitung sowie Text Mining, Graph Mining oder Video Mining und Datenvisualisierung zur Anwendung.

einem Individuum zuordnen.[11] Darüber hinaus gibt es zunehmend Anwendungen, die es ermöglichen, aus öffentlich zugänglichen individuellen Nutzerdaten tiefgreifende Schlüsse über private Eigenschaften zu ziehen. So gibt es Bemühungen, Dispositionen für psychische Erkrankungen wie z. B. Depressionen bereits anhand der Analysen von Aktivitäten in sozialen Netzwerken wie Instagram,[12] aber auch anhand von Stimmproben festzustellen – selbst wenn sich die Erkrankung noch in einem klinisch unauffälligen Stadium befindet. In der Öffentlichkeit viel diskutiert, in der Fachwelt aber umstritten sind Studien, die versuchen zu zeigen, wie sich anhand der Auswertung von Facebook-Likes detaillierte psychometrische Persönlichkeitsprofile erstellen lassen, die dann wieder zur gezielten Beeinflussung der Nutzerinnen und Nutzer eingesetzt werden könnten.[13] Daneben gibt es auch aus wissenschaftlicher und ethischer Sicht höchst fragwürdige Studien, die darauf abzielen, Techniken des Maschinellen Lernens missbräuchlich einzusetzen, z. B. um vom physiologischen Erscheinungsbild eines Menschen Rückschlüsse auf Eigenschaften wie beispielsweise die sexuelle Orientierung zu ziehen.[14]

Viele Anwendungen, die auf der Basis Maschinellen Lernens funktionieren, gehen inzwischen dazu über, eine Nutzung nur dann zu ermöglichen, wenn der Nutzer einwilligt, dem Anbieter seine gesamten Daten zur Verfügung zu stellen (z. B. Google Home). Dadurch entstehen einerseits immer neue Daten, die zur Weiterentwicklung der jeweiligen Dienstleistung genutzt werden können. Andererseits können und werden solche Daten oft auch für andere Zwecke verwendet bzw. weitergegeben. Ein solches Geschäftsmodell lässt ein datensparsames, auf den Schutz der Privatsphäre der Nutzerinnen und Nutzer gerichtetes Verhalten nicht mehr zu.

Neben einem vorrangig kommerziellen Interesse an der Verwendung von Daten gibt es auch Bereiche, in denen eine Sammlung und Auswertung individueller Daten gesellschaftlichen Interessen dient, beispielsweise die Freigabe der eigenen Gesundheitsdaten für die weitere Forschung. Hier kann die Erschließung einer möglichst großen Zahl solcher Datensätze bedeutend zur Verbesserung diagnostischer oder therapeutischer Verfahren beitragen, was dem Einzelnen wie der Allgemeinheit zugutekommt. Zugleich setzt sich der betreffende Proband aber auch dem Risiko aus, intime Informationen, derer er sich vielleicht nicht einmal bewusst ist, nach außen zu geben.

11 Hofmann & Schölkopf (2015).

12 Reece & Danforth (2017).

13 Kosinski, Stillwell & Graepel (2013).

14 Kosinski & Wang (2017); siehe hierzu auch Matsakis (2017).

Maschinelles Lernen

Maschinelles Lernen (Machine Learning) schließt aus empirischen Beobachtungen auf zugrundeliegende Regelmäßigkeiten. Ein solcher Lernprozess wird durch Algorithmen realisiert und resultiert in komplexen mathematischen Funktionen. Aus diesen lassen sich verallgemeinerbare Schlussfolgerungen über beobachtete Gegenstände, Prozesse oder Eigenschaften ziehen oder Voraussagen ableiten, insbesondere auch über private Bereiche der Nutzerinnen und Nutzer. Diese Voraussagefähigkeit, genannt Prädiktivität, ist wesentliches Merkmal der Methoden des modernen Maschinellen Lernens. Sie ist auch dort möglich, wo die untersuchten Zusammenhänge aufgrund ihrer Komplexität menschliche kognitive Kapazitäten überschreiten.

Komplexe prädiktive Modelle sind datengetrieben und entsprechend datenhungrig. Die Größe einer Datenmenge wird dabei durch die Anzahl der Beobachtungen (Kardinalität) und die Anzahl der dabei berücksichtigten Merkmale (Dimensionalität) charakterisiert. Um aus hochdimensionalen Daten lernen zu können, muss man die Komplexität oder Kapazität der Modelle an die Menge der vorhandenen Fallbeispiele (Trainingsdaten) anpassen und ggf. bereits vorhandenes Wissen (A-priori-Wissen) ausnutzen, z. B. dass ein Objekterkennungssystem unempfindlich gegenüber Änderungen in der Perspektive und Beleuchtung sein sollte.

Existierende Lernverfahren unterscheiden sich darin, in welcher Form A-priori-Wissen verwendet wird, auf welche Weise die Kapazität der Modelle kontrolliert wird und wie Gesetzmäßigkeiten algorithmisch erschlossen werden. Zu den gängigsten Verfahren zählen neuronale Netze (Deep Learning), Kernmethoden (z. B. Support-Vektor-Maschinen) und Bayes'sche Verfahren.

A Beispiel: Allgegenwart von Vernetzung – Smart Environment

Digitale Dienstleistungen bieten für die Nutzerinnen und Nutzer sehr viele Vorteile. Sie sind inzwischen nicht einmal mehr an bestimmte mobile Endgeräte wie Smartphones oder Netbooks gebunden, sondern über eine Vielzahl von Alltagsgegenständen verfügbar, beispielsweise Fernsehgeräte, Barbiepuppen, Fitnessarmbänder oder Kameras. Oftmals werden die von diesen Alltagsgegenständen gebotenen Dienstleistungen wie virtuelle Kontrolle der Haustechnik, Musikauswahl oder die Erstellung von Reiserouten von Nutzerinnen und Nutzern gar nicht mehr bewusst mit dem Internet in Verbindung gebracht. Doch ihnen allen ist gemeinsam, dass sie für die Bereitstellung bestimmter Dienste Informationen der Nutzerinnen und Nutzer sammeln und diese ins Internet, z. B. in eine Cloud, laden, um die zur Verfügung stehenden Rechen- und Speicherkapazitäten zu nutzen und auf dort bereits eingestellte Daten zurückzugreifen. Nur durch diese Verbindung ist es möglich, die gewünschten Dienste in der gewünschten Qualität anzubieten. Auf diese Weise werden komfortable personalisierte Dienstleistungen angeboten, die es den Nutzerinnen und Nutzern z. B. erlauben, den Energieverbrauch der Wohnung zu optimieren, jederzeit über Informationen und Dienste aus dem Internet zu verfügen oder die Freizeitgestaltung mit interaktiven Angeboten anzureichern (▸ Box „Smart Homes“).

Autonome technische Systeme

Gemessen am Menschen sind die Wahrnehmungsfähigkeiten autonomer technischer Systeme meist noch rudimentär, jedoch hat die Verbindung aus Sensorik, Big Data und Maschinellem Lernen in den letzten Jahren beträchtliche Fortschritte im Bereich der Maschinellen Wahrnehmung ermöglicht. Bei der visuellen Erkennung von Objekten in Bildern etwa erreichen Computer mit Menschen vergleichbare Genauigkeiten bei wesentlich höherem Datendurchsatz. Für komplexere Herausforderungen, etwa die Erkennung und Interpretation von menschlichen Handlungen, ist Ähnliches innerhalb eines Jahrzehnts zu erwarten. Auch im Bereich der akustischen Signalanalyse, insbesondere der Spracherkennung, haben neuerliche Fortschritte kommerziell einsetzbare Systeme ermöglicht (Beispiel: Siri, Alexa etc.).

Ihre Wahrnehmungs- und Verarbeitungsfähigkeiten machen autonome Systeme zu intelligenten Beobachtern. Die technische Entwicklung gibt ihnen dabei zunehmend mehr Möglichkeiten, das Beobachtete auch immer weitergehender zu interpretieren. Anders als Menschen können sie ihre Beobachtungen mit einer lückenlosen Gedächtnisfähigkeit verbinden. Schließlich – und wiederum im Gegensatz zum Menschen – können technische autonome Systeme ihre Beobachtungen mit Datenbeständen im Internet abgleichen und bei Bedarf in große, globale Datenbasen integrieren. Gerade Letzteres ist beim heutigen Stand der Technik wichtig, um kollektives und kooperatives Roboterlernen zu ermöglichen. Ähnliche Vorgehensweisen sind für autonome Fahrzeuge zu erwarten.

Die mit diesen Dienstleistungen einhergehende Datenerfassung bleibt jedoch für Nutzerinnen und Nutzer oftmals schwer durchschaubar. So ist gerade bei sprachgesteuerten Geräten oft nicht auf den ersten Blick erkennbar, ob und wann sie Sprachsignale aufnehmen, weiterleiten und speichern. Während manche Geräte, wie Lautsprecherboxen von Google oder Amazon, sich nur auf ein bestimmtes Stichwort hin anschalten, können andere Geräte wie Smartphones, Fernseher oder Kinderpuppen in der Standardeinstellung Gesprächsdaten kontinuierlich übertragen. Ebenso ist nur wenigen Nutzerinnen und Nutzern bewusst, dass viele Smartphones in kurzen zeitlichen Abständen ihre aktuellen Ortsdaten an den Betreiber des Betriebssystems senden und damit ein detailliertes Bewegungsprofil erstellen, das mit weiteren Nutzungsdaten verknüpft werden kann. Ohne geeignete Schutzmaßnahmen führen solche Systeme damit zu einer sehr weitgehenden Öffnung der Privatsphäre. Dies stellt auch ein erhebliches Risiko im Hinblick auf eine mögliche missbräuchliche Verwendung der technischen Mittel dar, etwa infolge von Sicherheitslücken, die eine „Übernahme“ der Geräte und Funktionen durch Dritte ermöglichen. Eindrückliche Beispiele hierfür waren in jüngerer Vergangenheit das Abschalten von Wohnblock-Heizungen durch Hacking der lokalen Steuerungsgeräte[15] oder auch die vernetzten Spielzeuge, die von der Bundesnetzagentur als „verbotene Sendeanlagen“ eingeordnet und daher aus dem Verkehr gezogen wurden. Letztere ermöglichen nicht nur das Ausspionieren fremder Wohnungen, sondern auch das unkontrollierbare Ansprechen, Ängstigen oder Bedrohen von Personen und hier insbesondere Kindern.[16]

Die Vernetzung beschränkt sich jedoch nicht allein auf individuelle Dienste.

15 Eikenberg (2013).

16 Bundesnetzagentur (2017); Krempl (2017); Bundesnetzagentur (2018).

Beispiel Smart Homes

Anwendungen im Bereich Smart Homes können potentiell sehr viele verschiedene Ebenen der Datenerfassung betreffen. Bei der Erfassung von Verbräuchen (Energie, Wasser) werden herkömmliche Messinstrumente zunehmend durch fernauslesbare digitale Messinstrumente ersetzt (Smart Metering). Aus diesen Daten können wertvolle Steuerungsinformationen für die Optimierung von Verbrauchsgeräten, wie etwa Heizungen, abgeleitet werden. Übertragen auf die Erfassung geeigneter anderer Sensordaten können ähnliche Systeme Bedrohungen durch Schadensereignisse oder Eindringlinge frühzeitig erkennen und beispielsweise Warn- oder Sicherheitsmaßnahmen auslösen. Im Wohnbereich können Sensorsysteme zahlreiche weitere Aufgaben erfüllen. Bereits kommerziell erhältliche Produkte (Amazon Echo, Google Home) können sprachgesteuert Dienstleistungen wie z. B. die Beantwortung von Anfragen, Bestellung von Waren oder Ausführung einfacher Kommandos erbringen. In Fußböden, Wänden und Möbeln installierte Sensorik kann zusätzliche Funktionalitäten ermöglichen, z. B. die Verfolgung von Personen, Detektion von Stürzen, oder Komfortfunktionen durch „situativ mitdenkende“ Möbel, die z. B. unterstützend oder präventiv auf Bewegungen von Personen reagieren. Bilderfassende Sensoren in Verbindung mit Techniken der virtuellen bzw. erweiterten Realität (Virtual/Augmented Reality) besitzen dabei die weitreichendsten Potentiale für innovative Anwendungen wie etwa videogekoppelte Wohnungen, die Möglichkeit einer immersiven Verbindung zum Arbeitsplatz oder die Erweiterung des Wohnraums durch virtuell begehbare Architektur oder Landschaften. Serviceroboter sowie die Digitalisierung und Vernetzung einer zunehmenden Anzahl von Haushaltsgegenständen ermöglichen weitere Innovationen bezüglich Funktionalität und Dienstleistungen, wiederum gekoppelt mit der Schaffung einer Vielfalt neuer Datenströme zwischen Wohnung und Internet. Zudem wird es in der Natur vieler angebotener Dienstleistungen liegen, dass die erfassende Sensorik mobil und z. T. sogar mit physischem Handlungsvermögen (Aktorik) verbunden ist.

Auch im öffentlichen Raum ist eine zunehmende Aufnahme, Speicherung und Auswertung von Daten zu erkennen. Bereits erprobt werden hier Gesichtserkennungssysteme, die in Menschenmengen, z. B. in Bahnhöfen[17] oder Fußballstadien[18], Kameraaufnahmen in Echtzeit auswerten, um verdächtige Personen und auffällige Handlungen identifizieren zu können. Noch in Entwicklung befinden sich Systeme für intelligente Kreuzungen, die mit Sensoren von Autos und Smartphones von Fußgängern interagieren, um zum einen die Ampelschaltung verkehrsangepasst zu regeln und zum anderen Verkehrsteilnehmer auf eventuelle Risikosituationen aufmerksam machen zu können.[19] Für die Funktion solcher Systeme werden Bewegungs- und Bilddaten aus dem öffentlichen Raum aufgezeichnet und ausgewertet und z. T. direkt mit den mobilen Systemen einzelner Nutzerinnen und Nutzer verknüpft. Neben den erkennbaren Vorteilen bleibt auch hier zu fragen, inwieweit sich in einer solchen Umgebung noch unbeobachtete Rückzugsräume für den Einzelnen erhalten lassen und welche Maßnahmen zu etablieren sind, um einen Schutz vor kriminellem, aber ggf. auch staatlichem Missbrauch gewährleisten zu können.

17 Bundespolizei (2017).

18 BMBF (2015).

19 DLR (2017).

B Beispiel: Datengetriebene Dienstleistungen

Durch die Allgegenwart der Vernetzung ist es möglich, in nahezu allen Kontexten Daten zu sammeln und mithilfe von Big Data zu analysieren, um neue Dienstleistungen anzubieten. Dabei werden oftmals Dienste finanziell kostenlos angeboten, sofern der Nutzer dafür bestimmte persönliche Daten preisgibt und in die Verwendung dieser Daten einwilligt. Der Kunde „bezahlt" also den Dienst mit seinen persönlichen Daten. Im Unterschied zu klassischem Bargeld ist diese Gegenleistung nicht mehr anonym, sondern mit der Identität des Nutzers und mit seinen Nutzungsdaten verknüpft bzw. verknüpfbar. Die Verknüpfung und Auswertung von Daten aus unterschiedlichen Quellen ermöglicht es, Benutzerprofile zu erstellen und so ein genaues Gesamtbild von der individuellen Persönlichkeit und ihres Verhaltens zu gewinnen. Diese Daten können dann als Grundlage genutzt werden, um beispielsweise den Nutzerinnen und Nutzern personalisierte Werbung zur Finanzierung des ursprünglichen Dienstes zu präsentieren. Oftmals ist es diese „sekundäre Nutzung", die den eigentlichen Zweck des angebotenen Dienstes ausmacht.

Darüber hinaus gehen insbesondere die großen Anbieter dazu über, mehrere miteinander verknüpfte Dienstleistungen anzubieten, die z. T. von Dritten entwickelt, etabliert und dann – inklusive der bereits vorhandenen Kundendaten – aufgekauft werden. So bietet Google beispielsweise schon lange nicht mehr nur die Dienste einer Suchmaschine an, sondern darüber hinaus auch ein Betriebssystem für Smartphones, einen E-Mail-Dienst, einen Kartendienst, einen Videokanal und vieles andere mehr. Microsoft bietet neben Betriebssystem und Software u. a. die Möglichkeit der Kommunikation über E-Mail und Skype und der Speicherung von Daten in der Cloud. Facebook vernetzt seine Nutzerinnen und Nutzer nicht mehr nur als Anbieter eines sozialen Netzwerks, sondern stellt zudem auch WhatsApp als Messenger für die Kommunikation zur Verfügung.

Damit sind die Unternehmen in der Lage, auf Kundendaten aus verschiedenen Nutzungsbereichen zurückzugreifen, was zum einen die Entwicklung von attraktiven und komfortablen Dienstleistungsangeboten ermöglicht. Zum anderen können Nutzerinnen und Nutzer dieser Dienstleistungen aber kaum mehr nachvollziehen, welche Daten zu welchem Zeitpunkt erfasst und von den Betreibern der Dienste verwendet werden.[20] Hierbei kommt hinzu, dass die Unternehmen nicht nur Daten speichern und auswerten, die der Nutzer aktiv geteilt hat, sondern auch solche, die sich aus dessen Aktivitäten auf bestimmten Webseiten und anderen Hintergrundinformationen ergeben. Solche Informationen werden meist automatisch, in großem Umfang und für den Nutzer nicht ohne Weiteres erkennbar abgegriffen. Dabei werden vielfach auch Informationen erfasst, die aus der Interaktion des Nutzers mit Dritten stammen und daher Dritte betreffen, ohne dass diese davon erfahren oder gar einwilligen. Weder die Nutzerinnen und Nutzer noch betroffene Dritte können nachvollziehen, was genau mit den Daten passiert, an wen sie evtl. weitergegeben und wie sie weiterverwendet werden (▸ Box „Beispiel Mobilfunk").

C Beispiel: Wissenschaft und Medizin

In weiten Teilen der Wissenschaften haben Technologieentwicklungen in den letzten beiden Jahrzehnten dazu geführt, dass die Menge der Forschungsdaten

20 Mittlerweile bieten einige Anbieter Apps zur Einsichtnahme in die Datenspeicherung an. Während dies z. B. bei Google Dashboard in erster Linie ein Informationsangebot ist, gehen andere Anbieter weiter und ermöglichen auch das gezielte Löschen gespeicherter Daten, so z. B. Amazon für seine Sprachsteuerung Alexa.

Beispiel Mobilfunk

In Mobilfunksystemen findet ein ständiger Datenaustausch zwischen einem eingeschalteten Endgerät und dem Netz statt, unabhängig davon, ob eine Verbindung aktiv genutzt wird. Diese sog. Signalisierung gewährleistet nahezu weltweit die Kommunikationsbereitschaft der Handys und begründet über die fast vollständige Überall-Erreichbarkeit die Attraktivität des Mobilfunks. Bei dem hierfür notwendigen Austausch von Signalen werden sowohl Positionsdaten als auch administrative Daten, z. B. Berechtigungen und Identifikation der Gesprächsteilnehmer, an den Netzbetreiber übermittelt und in einer Echtzeit-Datenbank gespeichert; der Teilnehmer wird so „verfolgt". Diese Daten werden aufgrund gesetzlicher Ermächtigung oder Verpflichtung über längere Zeit gespeichert, etwa zum Zwecke der Abrechnung. Aufgrund des Kommunikationskomforts haben die Nutzerinnen und Nutzer von Anfang an die Preisgabe ihrer Aufenthaltsdaten hingenommen. Vertrauensbildend hat hier auch die gesetzlich verankerte Pflicht des Mobilfunkbetreibers gewirkt, diese Daten vertraulich zu behandeln. Die Einführung neuartiger mobiler Dienste und Anwendungen im mobilen Internet sowie die Integration der GPS-basierten Navigationssysteme in die Mobilkommunikation haben allerdings neue Anreize gesetzt, persönliche Daten preiszugeben. Viele Diensteanbieter nutzen die erhobenen Positionsdaten nun auch für zusätzliche kommerzielle Dienste, etwa um Nutzerinnen und Nutzern ortsabhängige Informations- und Kaufangebote zu machen. Eine Weitergabe der Mobilitätsdaten an Dritte ist dabei nicht ausgeschlossen.

sprunghaft anstieg. Fortschritte in Bereichen wie der Satellitentechnik, der Mikroskopie und Teleskopie oder den sog. Hochdurchsatzverfahren in der Biologie (Omics-Technologien) ermöglichen es, in kürzester Zeit eine so enorme Menge an Beobachtungs- und Messdaten zu gewinnen, dass deren Zusammenführung und Auswertung durch Menschen allein nicht mehr möglich ist. Aber auch in den Geistes- und Sozialwissenschaften werden zunehmend neue und umfassende Datenquellen wie Satellitendaten, Sprach- und Textkorpora oder Daten der Mediennutzung erschlossen. Da diese Daten in der Regel in digitaler bzw. leicht digitalisierbarer Form vorliegen, nehmen Informationstechnologien zur Datenanalyse einen immer größeren Stellenwert im Prozess der Wissensgewinnung ein. Sie erlauben es, große Datenmengen zu vergleichen und unterschiedliche Datentypen miteinander zu verknüpfen, um nach Mustern und Korrelationen zu suchen, die dazu beitragen können, bislang unerkannte Zusammenhänge zu erkennen. Im Zuge der Weiterentwicklung der Analysetechniken des interpretierbaren Maschinellen Lernens[21] ist inzwischen sogar absehbar, auf der Grundlage neuer Lernprozesse nicht mehr nur auf Korrelationen basierende Voraussagen zu tätigen, sondern sogar zu neuen grundlegenden naturwissenschaftlichen Erkenntnissen zu gelangen.[22] Dabei besteht eine generelle Gefahr darin, dass gleichzeitig auftretende Ereignisse (Korrelationen) fälschlich als ursächlich miteinander zusammenhängend (Kausalitäten) gedeutet werden. Daher ist es eine der größten derzeitigen wissenschaftlichen Herausforderungen, Methoden zu entwickeln, die innerhalb von festgestellten Korrelationen Kausalzusammenhänge identifizieren können.

Zu den ersten großen Erfolgen dieses Zusammenspiels von Technologieentwicklung, Informationstechnik und fachspezi-

21 Bach et al. (2015); Montavon, Samek & Müller (2018).

22 Schütt, Arbabzadah, Chmiela, Müller & Tkatchenko (2017).

fischer Forschung zählten in der Biologie die Genomprojekte, in denen in immer kürzerer Zeit und mit stark sinkenden Kosten die Genome von immer mehr Organismen sequenziert werden konnten. Diese Entwicklung wirkte sich auch auf verschiedene Anwendungsfelder der Medizin aus, so z. B. in der Präimplantationsdiagnostik, der Krebsbehandlung oder der Entwicklung von Impfstoffen und pharmazeutischen Wirkstoffen. In der Medizin verspricht man sich darüber hinaus beispielsweise durch eine weitergehende Nutzung von Behandlungsdaten Erkenntnisse zur Verbesserung des Versorgungssystems und der Etablierung einer Präzisionsmedizin. Eine solche Nutzung würde allerdings voraussetzen, dass wirkungsvolle Schutzmechanismen zur Wahrung der Privatsphäre und des Vertrauensverhältnisses zwischen Patientin oder Patient und behandelnder/m Ärztin/Arzt etabliert werden.

Ähnliche bahnbrechende Erkenntniszugewinne sind in weiten Teilen der Wissenschaft, von der Astronomie über die Ökologie bis zur Archäologie, zu verzeichnen. Die zunehmende Nutzung digitaler Anwendungen in der Forschung führt dabei auch zu Änderungen in der Wissenschaftslandschaft. Neue Infrastrukturen werden benötigt, um den Austausch der Forschungsdaten über Institutionen hinweg weiter zu befördern (Open Data).[23] Zu diesem Zweck müssen die Daten in einer Weise vorgehalten und standardisiert werden, dass

1. ihre Auffindbarkeit gewährleistet ist,

2. ihre Auswertbarkeit auch für Dritte möglich ist und

3. die zur wissenschaftlichen Überprüfbarkeit notwendigen Kontextinformationen (Metadaten), z. B. über die Versuchsanordnung, die Art der Probennahme etc., ebenfalls verfügbar sind.

In manchen Forschungsfeldern wie z. B. der pharmazeutischen Forschung oder auch der Informatik erfolgt ein großer Teil der Forschungsaktivität in industriellem bzw. kommerziellem Kontext. Deshalb ergeben sich in Bereichen, in denen Daten und Forschungsergebnisse als Geschäftsgeheimnisse behandelt werden, besondere Herausforderungen, möchte man auf diese auch zum öffentlichen Nutzen zugreifen. Aus diesem Grund wird hier zurzeit daran geforscht, wie Firmeninteressen mittels Anonymisierung gewahrt bleiben könnten.

23 Auf europäischer Ebene soll die Etablierung einer European Open Science Cloud EOSC zur Verbesserung des Datenaustausches auf internationaler Ebene beitragen, EC (2018). Auch in Deutschland gibt es erste Schritte zum Aufbau einer Nationalen Forschungsdateninfrastruktur NFDI, BMBF (2016).

3 Big Data als Herausforderung für das Rechtssystem

Die digitale Transformation der Gesellschaft und besonders die Einsatzmöglichkeiten von Big Data bringen Herausforderungen für die Rechtsordnung mit sich. Dabei betrifft die Digitalisierung rechtliche Regelungen in grundsätzlich allen Rechtsgebieten, also im nationalen öffentlichen Recht, Zivilrecht und Strafrecht einschließlich der vielen Sondergebiete wie z. B. Medizinrecht oder Finanzmarktrecht und natürlich auch im Europa- und Völkerrecht.

Die Veränderungen machen es erforderlich, zu überprüfen, ob und inwieweit die vorhandenen rechtlichen Regeln noch dazu in der Lage sind, den in der Rechts- und Gesellschaftsordnung, insbesondere in den Grundrechten geschützten Bereich der Privatheit weiterhin aufrechtzuerhalten. Der Schutz der Privatheit berührt dabei auch Gemeinwohlziele wie individuelle und kollektive Selbstbestimmung, Persönlichkeitsschutz, Chancengerechtigkeit, Folgenverantwortung, Sicherheit, Schutz vor Manipulation und vor Diskriminierung. Lassen sich diese auch angesichts des Epochenwandels, der mit Big Data einhergeht, weiterhin gewährleisten? Welche Möglichkeiten für Verbesserungen im Recht sind verfügbar? Lassen sich Risiken absehen und wieweit können sie mithilfe des bestehenden Rechts vermieden oder zumindest minimiert werden? Wieweit bedarf es veränderter oder gar grundsätzlich neuer Instrumente rechtlicher Regulierung? Angesichts der Vielzahl an betroffenen Rechtsgebieten ist es ausgeschlossen, auf alle in dieser Stellungnahme angesprochenen Problemfelder aus rechtlicher Perspektive einzugehen. Stattdessen sollen – in Ergänzung zu den noch folgenden Teilaussagen in konkreten Problemfeldern – übergreifende Fragen zu rechtlichen Aspekten aufgeworfen und exemplarisch Lösungsmöglichkeiten anhand einzelner Themen angedeutet werden. Details müssen ausgeklammert bleiben. Verwiesen sei stattdessen auf die beispielhafte Behandlung einzelner Problemfelder in einer gesonderten Publikation, die im Rahmen der Erarbeitung dieser Stellungnahme entstand.[24]

Grundrechtsschutz

Von besonderer Bedeutung sind die Freiheitsrechte, die im Grundgesetz, aber auch in der EU-Grundrechtecharta und der Europäischen Menschenrechtskonvention sowie in völkerrechtlichen Abkommen wie den Menschenrechtspakten der United Nations (UN) normiert sind. Sie sind selbstverständlich maßgebend für jede Form von Kommunikation, also auch die digitale Kommunikation, und daher auch für die Generierung, Analyse und Nutzung von Big Data. Die Freiheitsrechte sind ebenso Maßstab für die rechtliche Beurteilung speziell des Umgangs mit der algorithmischen Selektion und Steuerung von Verhalten oder der im IT-Bereich eingesetzten Geschäftsmodelle. Der Schutz der Menschenwürde, der Gleichheitssatz, die Kommunikationsfreiheit, der Persönlichkeitsschutz, die Berufsfreiheit, die Religionsfreiheit oder die Gewährleistung des Eigentums gelten übergreifend und sind nicht etwa auf den Einsatz bestimmter Technologien begrenzt (▸ Box „Grundrechtsfrage“).

24 Hoffmann-Riem (2018).

Grundrechtsfrage

Grundrechte sind historisch gesehen als Abwehrrechte der von hoheitlichen Eingriffen Betroffenen gegen den Staat entwickelt worden, und zwar als sog. subjektive Rechte. Im Laufe der Entwicklung der Grundrechtstheorie und der Grundrechtsjudikatur, insbesondere des BVerfG, ist jedoch eine weitere Dimension herausgearbeitet worden: Der in ihnen enthaltene Auftrag richtet sich an alle Träger von Hoheitsgewalt, im Rahmen ihrer jeweiligen Aufgabenfelder die Verwirklichung des Freiheitsschutzes in der gesamten Rechtsordnung zu gewährleisten, also auch im Verhältnis Privater untereinander, darunter insbesondere zum Schutz von Freiheitsrechten gegen private Machtträger. Solche Gestaltungs- und Schutzaufträge sowie -pflichten sind keine Besonderheit deutschen Rechts, sondern sind auch für andere Rechtsgrundlagen, so für die EU-Grundrechtecharta und die Europäischen Menschenrechtskonvention, anerkannt.

Aus rechtlicher Sicht besteht daher kein Bedarf, alle Normierungen des Freiheitsrechtsschutzes um die Formel zu erweitern, dass sie auch digitale Kommunikation, die Nutzung digitaler Infrastrukturen und von Big Data oder den Einsatz von Instrumenten digitaler Verhaltenssteuerung erfassen. Auch bedarf es keiner besonderen Anordnung, dass auch die Ermächtigungen zu Beschränkungen von Freiheitsrechten, die im Grundgesetz, in den europäischen Grundrechtsverbürgungen und in völkerrechtlichen Abkommen enthalten sind, genutzt werden können und müssen, um Risiken abzuwehren, die mit der digitalen Transformation verbunden sind. Dabei erweist es sich als hilfreich, dass Normen – und zwar auch Grundrechtsnormen – seit jeher dynamisch ausgelegt werden.[25]

So ist beispielsweise der Grundrechtsschutz in Deutschland im maßgebenden Feld bereits z. T. durch grundrechtliche Innovationen ergänzt worden. Beispiele hierfür sind das schon erwähnte „Grundrecht auf informationelle Selbstbestimmung“[26], entwickelt vom Bundesverfassungsgericht (BVerfG) und gerichtet auf den weiterhin wichtigen Schutz personenbezogener Kommunikation, sowie das „Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit eigener informationstechnischer Systeme“ (sog. IT-Grundrecht).[27] Das BVerfG hat in seiner zweiten Entscheidung zu diesem Grundrecht[28] festgestellt, dass zu den informationstechnischen Systemen nicht nur private, von den Betroffenen eigengenutzte Computer zählen, sondern auch ihre Vernetzung mit fremden Computern, etwa bei der Ablegung von Daten in der Cloud.[29] Es hat zugleich betont, dass Daten, die auf externen Servern in der berechtigten Erwartung auf Vertraulichkeit ausgelagert sind, vom Schutz erfasst sind. Gleichermaßen wird Schutz gewährt, wenn Bewegungen der Betroffenen im Netz verfolgt werden. Das Gericht betont ferner, dass aufgrund der Möglichkeiten der Verknüpfung von Daten ein Eingriff in dieses Grundrecht von besonderer Intensität insbesondere für den Persönlichkeitsschutz sein kann.

Diese Verbürgungen finden sich zwar nicht im Wortlaut des Grundgesetzes, wurden aber vom BVerfG als Konkretisierung und zugleich Weiterentwicklungen des Grundrechtsschutzes im Hinblick auf die Garantie der Menschenwürde (Art. 1

25 Dies führt auch in den Bereich von Innovationen im Recht, dazu siehe etwa Hornung (2015); Hoffmann-Riem (2016a), Abschn. §§ 34, 35.

26 BVerfG (1983).

27 BVerfG (2008b).

28 BVerfG (2016).

29 BVerfG (2016), Rn. 209 f.

Abs. 1 GG) und des Persönlichkeitsrechts (Art. 2 Abs. 1 GG) entwickelt. Vergleichbares gilt für das vom Europäischen Gerichtshof entwickelte Grundrecht auf Vergessenwerden – dort als Ausprägung von Art. 8 der EU-Grundrechtecharta.

Darüber hinaus ist zu fragen, ob die digitale Transformation, soweit sie zu neuen Risiken führt, mit den herkömmlichen rechtlichen Instrumenten des Freiheitsschutzes selbst bei dynamischer Auslegung angemessen bewältigt werden kann. Anlass für solche Fragen bieten beispielsweise der Einsatz künstlicher Intelligenz, automatisierte Verfahren für Eingriffe in Rechtsgüter, die Robotik und die Verschmelzung der physischen und virtuellen Welt (Onlife).[30] Als Kandidaten für normative Neubestimmungen kämen insbesondere die Reichweite des Schutzes von Privatheit bei verstärkter Berücksichtigung des übergreifenden Schutzes von individueller und kollektiver Autonomie in Betracht sowie der Schutz vor Verhaltensmanipulation.[31]

Zu beachten ist hierbei auch, dass die digitale Transformation mit ihren weitreichenden Möglichkeiten wie etwa der Überwachung menschlichen Verhaltens[32] wesentlich durch Privatunternehmen erfolgt – darunter sehr machtvollen, die erheblichen Einfluss auf die Freiheitsräume anderer Privater ausüben. Wird hier nicht ausreichend für Schutzmöglichkeiten der Bürgerinnen und Bürger auch gegenüber den Unternehmen gesorgt, besteht die Gefahr, dass die Rechte und Freiheiten der Bürgerinnen und Bürger durch die Einrichtung bzw. Nutzung von transnationalen digitalisierten Infrastrukturen, durch die Ausgestaltung der Geschäftsmodelle und dabei insbesondere durch die Erhebung und Verwendung von Daten verletzt oder eingeschränkt werden. Daher ist die Ausgestaltung des Freiheitsschutzes auch gegenüber einer Gefährdung durch Private wichtig.

Eine entsprechende Aufgabe zur näheren gesetzlichen Ausgestaltung von Freiheitsschutz auch gegenüber Gefährdungen durch Private ergibt sich aus den objektivrechtlichen Gehalten von Grundrechten, die Aufträge zum Schutz der grundrechtlichen Wertvorgaben auch im Verhältnis von Privaten untereinander enthalten. Beispiele für ein solches Gewährleistungsrecht sind die Datenschutzgesetze sowie die EU-Datenschutz-Grundverordnung (EU-DSGVO), die auch Privaten Fesseln gegenüber der Verletzung von Persönlichkeitsrechten anlegen, aber schon für die Bewältigung der Probleme der Gegenwart nicht ausreichen. So werden die datenschutzrechtlichen Normen noch näher auf die neuen Potentiale der Nutzung von Big Data und die durch Big Data ermöglichten Gefährdungen von Rechtsgütern abzustimmen sein.

Objektiv-rechtliche Gehalte von Grundrechten finden sich nicht nur in den deutschen Grundrechtsnormen, sondern werden zunehmend auch im Bereich der EU-Grundrechtecharta sowie der Europäischen Menschenrechtskonvention, aber auch in einzelnen völkerrechtlichen Abkommen anerkannt.[33] Ihre Umsetzung in die jeweiligen Rechtsordnungen steht allerdings noch weitgehend aus.

Im Bereich der durch die digitale Transformation bedingten Gefährdungen dürfte zukünftig das schon erwähnte Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme[34] besondere Bedeutung gewinnen. Dieses Grundrecht ist im konkreten

30 Hildebrandt (2016), S. 41 ff.

31 Dazu und zu weiteren Anregungen in Form ausformulierter Grundsätze siehe die vom italienischen Parlament im Juli 2015 verabschiedete „Declaration of Internet Rights“, Camera dei deputati (2015).

32 Zur Praxis siehe statt vieler Christl (2014).

33 Siehe dazu Marauhn (2015); Fischer-Lescano (2014); Schliesky, Hoffmann, Luch, Schulz & Borchers (2014).

34 BVerfG (2008a).

Ausgangsfall zwar im Rahmen des subjektiv-rechtlichen Grundrechtsschutzes entwickelt worden. Da es aber auf Art. 1 Abs. 1 und Art. 2 Abs. 1 GG fußt, die ihrerseits objektiv-rechtliche Schutzgehalte normieren, ist es ebenfalls objektiv-rechtlich geprägt.[35]

Indem das BVerfG die Notwendigkeit von Systemschutz betont, werden Impulse dafür gesetzt, auch in anderen Hinsichten in Grundrechten Aufträge zur Gewährleistung von Systemschutz zu erkennen, soweit dieser effektiven Grundrechtsschutz ermöglicht. Angesichts der Intransparenz vieler digitalisierter Vorgänge und damit der Erschwernis bis Unmöglichkeit subjektiv-rechtlichen Rechtsschutzes ist es besonders wichtig, Schutzvorkehrungen in die informationstechnischen Systeme zu integrieren und damit Schutz systemisch abzusichern. Schon im traditionellen Datenschutzrecht ist der Systemschutz als wichtig anerkannt, und in der EU-DSGVO ist er weiter ausgebaut worden. Datenschutz durch Design und Datenschutz durch Voreinstellung (Default) sind Beispiele für systemischen Rechtsgüterschutz.

Die Notwendigkeit, das Recht auf seine fortwährende Tauglichkeit zu überprüfen, ist nicht auf die technologischen Aspekte der digitalen Transformation begrenzt. Denn diese verändert auch die soziale Ordnung und damit die Bedingungen für das individuelle und gesellschaftliche Leben.[36] So kann der Einsatz von digitalen Algorithmen und Big-Data-Anwendungen die Wahrnehmung von Realgeschehen filtern und verändern, Einstellungen und Werte beeinflussen, zur Erfassung von Entwicklungen und Trends und deren politischer oder gewerblicher Nutzung eingesetzt werden, die Basis neuer, auch gesellschaftlich wichtiger Geschäftsmodelle bilden usw. Dies ist mit Möglichkeiten der Verhaltenssteuerung verknüpft, ohne dass dies den Betroffenen stets bewusst wird.[37] Bedeutsam sind auch neue Formen der Mobilität (etwa Smartphone, selbstfahrende Automobile, Mobilitätsunterstützung durch Cloud Computing), neue Arten medizinischer Diagnostik, aber auch veränderte Möglichkeiten der Überwachung, Spionage und Sabotage. Sollen angesichts solcher Entwicklungen die normativen Zielwerte einer rechts- und sozialstaatlichen Demokratie bewahrt werden, bedarf es auch bereichsbezogener Rechtsanpassungen und ggf. neuartiger Normierungen.

Entgrenzungen

Erschwert wird der Einsatz von Recht für die Bewältigung solcher Probleme, insbesondere für den Schutz von Autonomie, allerdings dadurch, dass die neuen Technologien in vielerlei Hinsicht Entgrenzungen mit sich bringen und damit das Recht, das meist mithilfe von Grenzziehungen arbeitet, vor besondere Herausforderungen stellen oder es gar ins Leere laufen lassen. So sind die digitalen Technologien und deren Infrastrukturen sowie die eingesetzten Geschäftsmodelle nicht oder nur ausnahmsweise regional, etwa national, begrenzt. Vielmehr sind sie häufig transnational oder auch global verfügbar. Gleiches gilt für die mit digitalisierter Technik erbrachten Dienste. Auch verschwimmen im IT-Bereich die Grenzen zwischen Hardware und Software und zwischen Dienstleistungen und den genutzten IT-Infrastrukturen als ihrem Medium. Private und öffentliche Kommunikation werden verstärkt miteinander vermengt. Herkömmliche Vorstellungen über Privatheit und Öffentlichkeit erodieren. Ein besonderes Problem auch mit Blick auf die rechtlichen Folgen entsteht, wenn lernende algorithmische Sys-

35 Siehe etwa Wehage (2013), S. 155 ff.; Hauser (2015), S. 290 ff. sowie weitere Nachweise dort in Fn. 4.

36 Grundlegend, auch unter Einordnung in die historische Entwicklung, siehe dazu Stalder (2016).

37 Dies ist vielfach beschrieben worden. Als ein Beispiel unter mehreren sei verwiesen auf Latzer, Hollnbuchner, Just & Saurwein (2016); Hoffmann-Riem (2017).

teme sich neuen Problemen eigenständig anpassen oder in der Lage sind, sich unabhängig von der menschlichen Programmierung zu entwickeln (Machine Learning und Deep Learning). Soweit – insbesondere durch entsprechende Rechtspflichten – nicht für die Erkennbarkeit solcher Veränderungen der lernenden Algorithmen gesorgt wird, lassen sich mögliche problematische Folgen nicht wirksam kontrollieren oder korrigieren.

Erscheinungen der Entgrenzung, insbesondere die der Entterritorialisierung, führen zu weit offenen Flanken im Rechtsschutz, soweit das Recht an Grenzsetzungen anknüpft, etwa regional (sei es national oder etwa EU-weit), und soweit es zudem gegenständlich begrenzt ist.[38] Verfügbar ist zwar auch transnational oder global geltendes Recht wie z. B. Völkerrecht. Dessen räumlicher Anwendungsbereich mag weit sein, er ist aber gegenständlich nur auf einzelne Sektoren wie insbesondere das Welthandelsrecht oder Teilprobleme des Urheberrechts bezogen[39] und erfasst damit keinesfalls alle hier maßgeblichen Herausforderungen.

Territoriale, darunter auch nationale Anknüpfungspunkte rechtlicher Regulierung sind zwar auch gegenüber transnationalen oder globalen Aktivitäten von IT-Unternehmen nicht ausgeschlossen – etwa, wenn diese ihren Sitz und/oder ihr Betätigungsfeld in den jeweiligen Regionen haben (s. dazu Art. 3 EU-DSGVO, § 1 BDSG [neu]). Den bisher eingesetzten Instrumenten mangelt es aber häufig an Effektivität. Insbesondere stößt hoheitliche Regulierung meist auf erheblichen Widerstand der IT-Unternehmen, die versuchen, diese zu verhindern oder zu verwässern, und die viele Möglichkeiten haben, ihr auszuweichen: z. B. durch Verlegung des Unternehmenssitzes oder Verlagerung von Tätigkeitsschwerpunkten auf andere Unternehmensteile eines Konzerns. Zu den Strategien gehört auch das Abstellen auf Selbstgestaltung und Selbstregulierung, soweit sie Transparenz möglichst vermeiden, einer rechtsstaatlichen Umhegung ausweichen und effektive Kontrolle ausschließen.

Machtkonzentration

Die grenzüberschreitenden Möglichkeiten der digitalen Transformation haben, wie schon erwähnt, den Aufbau globaler Machtpositionen und deren Konzentration bei einigen wenigen Konzernen erleichtert. Diese haben es geschafft, in wichtigen Teilmärkten globale Oligopole zu bilden und weitere Marktsegmente zu besetzen. Erklärungen für den Erfolg solcher Bemühungen finden sich u. a. in der Netzwerk- und Internetökonomie.[40] Hinzu kommt die Mehrseitigkeit der Märkte, auf die in Kapitel 4A näher eingegangen wird. Derartige Konglomerateffekte können zu Marktverschließungen, also zur Unterbindung von Wettbewerb, genutzt werden.

Das grundsätzlich einschlägige Kartellrecht als Machtbegrenzungsrecht ist zur Gegensteuerung nur begrenzt einsetzbar. Insofern ist auch darauf zu verweisen, dass Kartellrecht seinem Grundanspruch nach ein Recht zur Sicherung der Funktionsfähigkeit von Märkten und insbesondere zur Begrenzung ökonomischen Machteinsatzes ist. Die Durchsetzung von Gemeinwohlzielen wie Persönlichkeitsschutz, Manipulationsfreiheit, Zugangschancengerechtigkeit oder Verhinderung von Diskriminierung sind nicht spezielle Ziele von traditionellem Kartellrecht und ihre Erreichung ist auch nicht automatisch über kartellrechtliche Vorkehrungen

38 Zu den Problemen der Entterritorialisierung und des Umgangs des vor allem öffentlichen Rechts damit siehe Cornils (2017).

39 Siehe dazu statt vieler Drexl (2016).

40 Zur Internetökonomie statt vieler Peters (2010); Clement & Schreiber (2016).

9. Novelle des Gesetzes gegen Wettbewerbsbeschränkung (GWB)

Damit der Zusammenschluss von Unternehmen durch die deutsche Fusionskontrolle überprüft werden kann, müssen bestimmte Mindestanforderungen gegeben sein. Ausschlaggebend ist hierbei insbesondere die wirtschaftliche Bedeutung der beteiligten Unternehmen (Aufgreifschwelle): Die fusionierenden Unternehmen müssen im letzten abgeschlossenen Geschäftsjahr insgesamt einen weltweiten Umsatz von mehr als 500 Millionen Euro erzielt haben, und mindestens 2 Unternehmen einen bestimmten Inlandsumsatz erzielt haben. Dieser muss bei einem Unternehmen über 25 Millionen Euro und bei dem anderen Unternehmen über 5 Millionen Euro liegen (Inlandsumsatzschwelle). Der Erwerb von WhatsApp durch Facebook unterlag trotz des Kaufpreises von 19 Milliarden US-Dollar keiner Anmeldepflicht in Deutschland, da WhatsApp nur geringe Umsätze aufwies und somit die Aufgreifschwelle der deutschen Fusionskontrolle nicht berührt war. Am 9. Juni 2017 ist eine Neufassung des Gesetzes gegen Wettbewerbsbeschränkungen, die 9. GWB-Novelle, in Kraft getreten, die eine zusätzliche transaktionswertbezogene Aufgreifschwelle einführt. Mit dieser Neuerung soll neben der Umsetzung der EU-Richtlinie zum Kartellschadenersatz in nationales Recht u. a. eine wirksame Fusionskontrolle vor allem im Hinblick auf die zunehmende Digitalisierung der Wirtschaft sichergestellt werden. Danach besteht künftig eine Anmeldepflicht, wenn die Umsatzschwellen der früheren Regelung erreicht sind oder der Wert der Gegenleistung für den Zusammenschluss mehr als 400 Millionen Euro beträgt und das zu erwerbende Unternehmen in erheblichem Umfang im Inland tätig ist. Der Begriff der Gegenleistung umfasst alle Vermögensgegenstände und sonstigen geldwerten Leistungen (Kaufpreis) sowie übernommene Verbindlichkeiten. Zudem wurde eine Änderung der Bußgeldregelungen durchgesetzt, wonach Bußgelder nunmehr nicht nur gegen eine handelnde Tochtergesellschaft, sondern auch gegen die lenkende Konzernmutter oder gegen rechtliche wie wirtschaftliche Nachfolger von Unternehmen verhängt werden können. Dieser Aspekt der Novelle wurde von Industrieverbänden kritisiert, erscheint jedoch angesichts der immer wieder vorkommenden Umgehung von Geldbußen sinnvoll.

gesichert.[41] Allerdings kann ein funktionsfähiger Markt zu ihrer Verwirklichung mit beitragen. Ergänzend sind aber weitergehende, nicht marktbezogene Regelungen erforderlich (▸ Box „Novelle GWB“).

Transparenzdefizite

Ein mit der digitalen Transformation in ihrer bisherigen Gestalt verbundenes Problem ist der erhebliche Mangel an Transparenz beim Einsatz digitaler Techniken und bei der Handhabung der Geschäftsmodelle.[42] Die Setzung und Anwendung von Recht, aber auch die Möglichkeiten der Kontrolle sind auf zuverlässige Informationen über Realgeschehen angewiesen, wenn sie effektiv sein sollen. Die digitale Transformation hat zwar neue Räume zur Generierung, Erfassung und Verwertung von Informationen geschaffen; zugleich aber wurden Zugänge zu den dabei genutzten Vorgehensweisen und den erarbeiteten Ergebnissen von den Akteuren meist versperrt. Sowohl für die Nutzerinnen und Nutzer als auch für Aufsichtsinstanzen sowie für die allgemeine Öffentlichkeit als Träger demokratischer Mitverantwortung kann es aber wichtig

41 An dieser Beschränkung des Kartellrechts ändert auch die 9. Novelle des Gesetzes gegen Wettbewerbsbeschränkungen (GWB) vom 01.06.2017 nichts.

42 Wischmeyer (2018).

sein, dass der Umgang mit Daten, auch ihr Einsatz im Rahmen von Big-Data-Analytik, nachvollziehbar und kontrollierbar ist, soweit davon individuelle oder kollektive Rechtsgüter nachteilig betroffen werden können. Aber auch für den Schutz kollektiver Rechtsgüter, die von Big-Data-Anwendungen gefährdet werden können, ist Transparenz wichtig. Zu den Schutzgütern gehören neben anderen die plurale Offenheit der öffentlichen Meinungsbildung und manipulationsfreie politische Wahlen. Transparenz ist ferner eine Voraussetzung für die Sicherung auch von Verantwortlichkeit (Accountability). Besondere Probleme von Intransparenz sind mit dem Einsatz lernender algorithmenbasierter Systeme verbunden.

Die EU-DSGVO hat die Möglichkeiten für Informationen über die Art der Datenverarbeitung verbessert. Abschnitt 2 der EU-DSGVO und §§ 32 ff. BDSG (neu)[43] sehen gewisse, z. T. sehr detaillierte Pflichten der Datenverwender zur Information von (individuell) betroffenen Personen und Auskunftsrechte für diese vor. Das betrifft die Erhebung, Verarbeitung – auch die Verarbeitung zu anderen Zwecken als bei der Erhebung vorgesehen – und die Übermittlung personenbezogener Daten (s. Art. 13–15 EU-DSGVO i.V.m. Nrn. 60 ff. der Erwägungsgründe). Erfasst sind allerdings nur Informationen über gezielt gewonnene personenbezogene Daten, nicht aber etwa Informationen über alle Daten, die bei der Nutzung von Informationstechnologien oder durch Big-Data-Analytik anfallen und verwendet oder durch sie neu generiert werden. Ein Schutzdefizit besteht auch darin, dass die Informations- und Auskunftspflichten sich nicht auf die Offenlegung der konkreten Empfänger der Daten oder auf die Zwecke erstrecken, für die diese die Daten konkret verwenden.

Transparenzbedarf besteht auch speziell für den Einsatz von Algorithmen: Nach welchen Maximen erfolgt die Programmierung, welche Kriterien werden zugrunde gelegt? Gleiches gilt für die Frage, welche Informationen als Input eingegeben werden, wenn die Algorithmen zur Selektion und Steuerung in konkreten Fällen, etwa beim Targeting, Profiling oder Scoring, eingesetzt werden.

Immerhin fordern Art. 13 Abs. 2f, 14 Abs. 2g EU-DSGVO als Teil des Auskunftsrechts an die betroffenen Personen gerichtete „aussagekräftige Informationen über die involvierte Logik,[44] ferner über die Tragweite und die angestrebten Wirkungen einer derartigen Verarbeitung“ – aber ausdrücklich nur für einen Teilbereich, nämlich eine automatisierte Entscheidungsfindung einschließlich Profiling (allerdings mit dem Zusatz „zumindest in diesen Fällen“)[45]. Soweit lernende Algorithmen eingesetzt werden,[46] müssen zur „involvierten Logik“ auch Informationen mit Bezug auf die Trainingsprogramme gehören, die in solche algorithmischen Systeme eingebettet sind.[47] Was mit der „involvierten Logik“ konkret erfasst wird, bleibt allerdings offen. In der Literatur wird dies im Sinne der „Methoden und Kriterien“ umschrieben,[48] ohne dies aber näher zu spezifizieren.

In der EU-DSGVO fehlen bereichsspezifische Eingrenzungen, beispielsweise hinsichtlich der Kategorien von Daten, die für besondere Anwendungen wie Scoring

43 Siehe auch §§ 55 ff. Bundestag (2018) – in Umsetzung der Richtlinie EU 2016/680 Europarl & European Council (2016a).

44 Nach Paal, Pauly & Ernst (2018) Rn. 31 zu Art. 13 müssen nur die Grundannahmen der Algorithmus-Logik mitgeteilt werden, nicht etwa die Algorithmen selbst.

45 Dies deutet darauf hin, dass die Regelung nur einen Mindeststandard schützt.

46 In der EU-DSGVO unter Einschluss der Erwägungsgründe werden die besonderen, mit lernenden Algorithmen verbundenen Probleme leider nicht thematisiert.

47 Dabei kann es nicht reichen, Informationen über den Ausgangsalgorithmus zu erhalten, da dieser sich durch die Lernprozesse laufend verändert – mit der weiteren Folge, dass nicht einmal den Programmierern bekannt sein kann, wie er sich im Laufe der Zeit durch Selbstprogrammierung verändert hat. Hier besteht noch erheblicher Forschungsbedarf.

48 So Bäcker in Kühling et al. (2018), Rn. 27 zu Art. 15.

verwendet werden dürfen. So käme eine Beschränkung der Daten auf die bisherige Kreditgeschichte der betroffenen Person in Betracht und es könnte – in Analogie zum Recht auf Vergessenwerden – für Fristen bei der Verwendung bestimmter Daten gesorgt werden. Nur angemerkt sei, dass entsprechende Restriktionen auch in bestimmten Feldern des Profiling hilfreich wären, so etwa eine Begrenzung der Datenkategorien für Profiling im Bereich von Bewerbungsverfahren, aber auch bei der kommerziellen Kommunikation.

Um die Beachtung solcher besonderen, noch zu schaffenden Anforderungen an die Transparenz beim Einsatz von besonders wichtigen Algorithmen kontrollierbar zu machen, sind Verfahren der Zertifizierung durch akkreditierte Stellen und Vorkehrungen zum Monitoring in Betracht zu ziehen.

Eine weitere Transparenzfrage betrifft die Nachvollziehbarkeit von Prozessen und Entscheidungen, die auf Algorithmen basieren. Hier besteht eine Vielfalt von Problemen insbesondere bei lernenden Algorithmen.[49] Werden solche Algorithmen rechtlich als Geschäftsgeheimnisse behandelt, was der Bundesgerichtshof für die Scoring-Programme der Schufa ausdrücklich bejaht hat,[50] entfällt die Möglichkeit, diese zu überprüfen, womit auch ein Rechtsschutz für Nutzerinnen und Nutzer vereitelt wird. Allerdings ist der Schutz von Geschäftsgeheimnissen nicht absolut. Im Interesse des Schutzes gegenläufiger Rechtsgüter können Geschäftsgeheimnisse im Rahmen der Verhältnismäßigkeit gesetzlich ausgeschlossen oder beschränkt werden. Davon sollte Gebrauch gemacht werden. Soweit im Rahmen von Rechtsstreitigkeiten eine gerichtliche Überprüfung von Algorithmen, die gleichwohl als Geschäftsgeheimnis eingestuft werden, erforderlich ist, wäre es empfehlenswert, sog. In-Camera-Verfahren zu ermöglichen.[51]

Nach bisherigem Recht ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten an bestimmte Voraussetzungen gebunden. Sie ist nur zulässig, wenn das Gesetz oder eine andere Rechtsvorschrift diese Tätigkeiten erlaubt oder der Betroffene eingewilligt hat. Diese doppelte Möglichkeit der Rechtmäßigkeit hat auch Art. 6 EU-DSGVO übernommen, aber noch eine weitere Möglichkeit hinzugefügt: Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nun ebenfalls zulässig, wenn sie für die Erfüllung eines Vertrages notwendig ist, dessen Vertragspartei die betroffene Person ist, oder sie zur Durchführung vorvertraglicher Maßnahmen erforderlich ist, die auf Anfrage der betroffenen Person erfolgen (Art. 6 Abs. 1 EU-DSGVO).

Risiken hoheitlicher Überwachung

Defizite rechtlicher Regelung bestehen nicht nur im Hinblick auf die private, insbesondere privatwirtschaftliche Nutzung von Big Data, sondern auch hinsichtlich ihres Einsatzes bei der Erfüllung öffentlicher Aufgaben. Erwähnt seien vor allem die Generierung und Nutzung von Big Data für Zwecke hoheitlicher Überwachung, für Predictive Policing oder für die Erfassung gesellschaftlicher Trends und deren Nutzung zur Verhaltensbeeinflussung. Solche Verwendungen können mit dem Schutz der Rechtsgüter der Bürgerinnen und Bürger kollidieren. Um dieses Risiko zu begrenzen, gibt es bereits die „Richtlinie zum Schutz natürlicher

49 Zu lernenden Algorithmen, insbesondere zur Transparenzproblematik, siehe Wischmeyer (2018), S. 1, 18–65.

50 BGH (2014). Es ist allerdings fraglich, ob diese Entscheidung nach Inkrafttreten der EU-DSGVO Bestand haben wird.

51 In solchen Verfahren werden die beklagten Unternehmen gegenüber dem Gericht zur Offenlegung – etwa von freiheitsgefährdend einsetzbaren Algorithmen oder nur der ihnen zugrundeliegenden Maximen und Kriterien – verpflichtet, ohne dass diese vom Gericht weiteren Personen unter Einschluss der Gegenpartei zugänglich gemacht werden, mit Ausnahme von eingeschalteten neutralen Sachverständigen.

Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates“[52], die im zweiten Teil des BDSG (neu) in den §§ 45 ff. umgesetzt worden ist. Diese gilt allerdings dem traditionellen Datenschutz und ist nicht abgestimmt auf die durch Big Data bedingten Risiken hoheitlicher Überwachung. Gesetze zum Schutz der öffentlichen Sicherheit wie das Bundeskriminalamtgesetz oder das Gesetz über den Bundesnachrichtendienst sollten daher so modifiziert werden, dass sie hinreichenden Schutz auch gegenüber den spezifischen Einsatzmöglichkeiten von Big Data geben, ohne die Schutzaufgabe als solche vernachlässigen zu müssen.

In grundrechtlicher Hinsicht ist auf den Schutz durch das Brief-, Post- und Fernmeldegeheimnis, auf das Grundrecht auf informationelle Selbstbestimmung und das Grundrecht der Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme zu verweisen, aber auch auf das Grundrecht der Unverletzlichkeit der Wohnung. Diese Grundrechte enthalten allerdings auch Schranken des Freiheitsschutzes im Interesse effektiver Erfüllung öffentlicher Aufgaben.

Soweit Grund- und Menschenrechte Hoheitsträgern Eingriffe in Rechte anderer ermöglichen oder beschränken, sollte die Anwendbarkeit rechtsstaatlicher Maßstäbe nicht auf Akte der deutschen Hoheitsträger im deutschen Hoheitsgebiet oder im EU-Gebiet begrenzt, sondern auch auf deren Handeln in ausländischen Rechtsordnungen erstreckt werden. Ebenfalls sollte gesichert werden, dass Hoheitsträger anderer Staaten bei Grundrechtseingriffen im deutschen Hoheitsgebiet an die Standards des EU-Rechts sowie des nationalen Datenschutzrechts gebunden werden.

52 EC (2016a).

4 Big Data und Privatheit – Problemanalyse und Handlungsoptionen

A Ökonomische Auswirkungen

Für eine Diskussion möglicher Gefahren der Digitalisierung für die Privatheit der Bürgerinnen und Bürger ist es wichtig, die Anreize der „Datensammler“ und die ökonomischen Mechanismen hinter der Datenwirtschaft zu verstehen. Für die Abwägung politischer Maßnahmen zum Schutz der Privatheit ist ein solches Verständnis zentral, um etwaige Regulierungsansätze effektiv planen und umsetzen zu können.

Digitale Technologien haben seit den 1970er-Jahren in nahezu allen Bereichen der Wirtschaft Einzug gehalten und dort dazu beigetragen, Prozesse effizienter und damit kostengünstiger zu gestalten. Lange Zeit kamen die Treiber dieser Entwicklung aus Unternehmen der klassischen Informations- und Kommunikationstechnologie. Doch inzwischen hat hier ein grundsätzlicher Wandel hin zu software- und cloudbasierten Technologien stattgefunden, die sich mit der Speicherung, dem Transport, der Verknüpfung und Verarbeitung von Daten befassen. Damit einhergehend sind völlig neue Unternehmen erfolgreich in den Markt eingetreten. Vor allem der Einsatz von Verfahren des Maschinellen Lernens hat dazu beigetragen, die Geschwindigkeit zu erhöhen, mit der Daten in ökonomisch wertvolle Information umgesetzt werden können. Diese Dienstleistungen der entsprechenden Unternehmen werden von zahlreichen Menschen oftmals ohne große finanzielle Aufwendungen genutzt – dennoch sind sie in wirtschaftlicher Hinsicht sehr erfolgreich: Hier werden die Daten selbst zu ökonomisch relevanten Wertquellen.[53] So konnten sich Unternehmen der Internetwirtschaft wie Facebook und Alphabet (Mutterkonzern von Google) in den vergangenen Jahren zu den weltweit größten börsennotierten Unternehmen nach Marktkapitalisierung entwickeln.[54]

Allerdings bringen diese Unternehmensmodelle auch Nachteile mit sich: So können Bürgerinnen und Bürger nicht mehr auf Anonymität in Freizeit und Arbeitsleben vertrauen. Ihre Identität, aber auch frühere Kaufentscheidungen, Kaufkontexte, politische Präferenzen und persönliche Verbindungen zu anderen Nutzerinnen und Nutzern des Internets sind den Anbietern von Dienstleistungen, Waren und Informationen immer öfter bekannt. Den Dienstleistern stehen dadurch so viele Daten und damit auch potentielle Informationen über die Nutzerinnen und Nutzer zur Verfügung, dass sie neben ihrer ökonomischen Bedeutung auch über eine erhebliche Informations- und damit auch Steuerungsmacht verfügen. Das gibt ihnen wiederum neue Möglichkeiten für Versuche der Einflussnahme auf einzelne Nutzerinnen und Nutzer sowie auf Nutzergruppen. Dies lässt sich im ökonomischen Bereich für Zwecke der Werbung, aber auch zur Einflussnahme z. B. im politischen Bereich nutzen. Die missbräuchliche Nutzung von Daten durch Cambridge Analytica und die damit verbundene Diskussion zeigen ungeachtet der Frage der Wirksamkeit der Manipulationsversuche auf, in welchem Umfang persönliche Daten genutzt werden können, um in poli-

53 EFI (2016), S. 62.
54 EFI (2017), S. 100.

tischen Diskussionen und Wahlen gezielt Einfluss auf wahlentscheidende Gruppen zu nehmen.[55]

Für politische Akteure in Europa (und in anderen Regionen) erwächst vor diesem Hintergrund eine problematische Entscheidungslage: Geben sie der von vielen Akteuren der Wirtschaft aufgestellten Forderung nach Senkung der Vorgaben zum Schutz der Privatheit nach, fördern sie die Entwicklung der eigenen nationalen und der europäischen Internetwirtschaft sowie die Entstehung neuer Wertschöpfungsquellen. Dem stehen aber u. U. hohe gesellschaftliche Kosten, so die des teilweisen Verlusts von Privatheit und der Einschränkung des Datenschutzes, gegenüber. Geschäftsmodelle, die einen restriktiven Umgang mit Daten als besonderen Kundennutzen vermarkten, waren bisher nur in Nischenbereichen erfolgreich.

Aus ökonomischer Sicht führen die neuen Möglichkeiten von Big Data in den folgenden Bereichen zu relevanten Veränderungen, die auch Implikationen für den Umgang mit privaten Daten in der digitalen Welt haben:

Die Dynamik des Anbietermarktes

Die Internetwirtschaft und die auf Big Data basierenden Dienstleistungen werden weltweit von nur wenigen großen Unternehmen dominiert, die Monopolcharakter besitzen. Der Theorie des Schumpeter'schen Innovationswettbewerbs zufolge sind Monopole häufig nur temporär, weil neue Unternehmen versuchen werden, Monopolisten in profitablen Marktpositionen zu überflügeln. Die Monopolisten, so diese Logik, lösen sich gegenseitig ab.

In diesem Kontext werden Start-ups generell als positiv angesehen, da sie als Garanten für den Innovationswettbewerb gelten, selbst wenn marktmächtige Unternehmen bereits tätig sind. Allerdings führt im Bereich der digitalen Technologien der Markteintritt durch junge Unternehmen nicht automatisch zu einem solchen Innovationswettbewerb. Oftmals wirkt es sich als wettbewerbshemmend aus, dass diese in ihrer Frühphase noch nicht über ausreichend große Datenmengen verfügen können. Darüber hinaus ist eine Übernahme durch ein existierendes Unternehmen für viele Start-ups derzeit oft attraktiver als ein Börsengang und der Aufbau einer eigenständigen Marktpräsenz. Start-ups werden dann zu Quellen neuer Technologien für große und am Markt etablierte Unternehmen. Anstatt der Bildung dominanter Positionen entgegenzuwirken, unterstützen Start-ups somit die Verfestigung solcher Positionen. Die zahlreichen Übernahmen erfolgreicher Start-ups durch etablierte Unternehmen nähren Zweifel daran, dass der Markteintritt junger Unternehmen im Bereich der datenbasierten Wirtschaft den Wettbewerb in jedem Fall stärkt.[56]

Überführung von Daten in ökonomischen Nutzen

Big-Data- und verwandte datenbasierte Unternehmensmodelle haben zunächst kostensenkende Wirkungen bezüglich der Ermittlung wichtiger Nachfrage- und Kundenparameter.[57] So ist es für die Unternehmen z. B. erheblich einfacher, Kundenpräferenzen und andere relevante Informationen zu erheben und auszuwerten. Daraus ergeben sich u. a. folgende Nutzungsmöglichkeiten:

I) Unternehmen können nicht nur ihre Werbung und ihre Produkte mit Blick auf ihre Kundschaft gezielt platzie-

55 Siehe z.B. Kühl (2018).

56 Vgl. auch EFI (2016), Kapitel B3, insbes. Tab. B3-9. Die 9. Novelle des GWB ist auch vor diesem Hintergrund zu sehen (▸ Box „Novelle GWB").

57 Übersichtsdarstellungen der grundlegenden ökonomischen Effekte finden sich u. a. in EFI (2015), Goldfarb & Tucker (2017), Goldfarb, Greenstein, Tucker & National Bureau of Economic Research (2015), Levin (2011), Peitz & Waldfogel (2012).

ren, sondern darüber hinaus durch die Kenntnis der Zahlungsbereitschaft und fähigkeit potentieller Kundinnen und Kunden diese auch über differenzierte Preise ansprechen. Dadurch kommt es zu einer Auflösung des Marktmachtparadoxons: Anbieter müssen, um einen angestrebten Gewinn zu erzielen, nicht länger einen hohen, einheitlichen Preis für ein Produkt ansetzen, der einen Teil ihrer potentiellen Kundschaft ausschließt. Der von einigen weniger solventen Kundinnen und Kunden gezahlte geringere Preis kann durch einen entsprechend höheren Preis bei entsprechend zahlungsfähigen Kundinnen und Kunden ausgeglichen werden. Auf diese Weise können Anbieter durch entsprechende Angebote Transaktionen ermöglichen, die bei einem homogenen Preis zahlreiche Konsumentinnen und Konsumenten von einem Kauf ausschließen würden, so kommen nun auch Konsumenten in den Genuss der Dienstleistung, denen zuvor der Konsum nicht möglich war.

II) Es werden digitale Transaktionen möglich, die in anderer Form nicht umsetzbar sind. Ein Beispiel sind die sog. Programmatischen Marktplätze wie z. B. „Ad Exchanges“ zum Handel mit Platzierungen von digitaler Werbung auf Internetseiten. Dabei kann auf den jeweiligen Nutzer zugeschnittene Werbung in dem Moment, in dem er eine bestimmte Internetseite öffnet, platziert werden.

III) Die Neuentwicklung und Vermarktung differenzierter Produkte und Dienstleistungen, die den Präferenzen der Konsumenten bzw. dem Nachfragekontext entsprechen, werden gefördert. Somit erhalten Kundinnen und Kunden auf ihre individuellen Vorlieben und Bedürfnisse zugeschnittene Angebote, während Unternehmen z. B. in der Planung, der Produktion und der Lagerung Kosten sparen können.

Insofern ist es möglich, dass einerseits mit verbesserten Informationen über Kundinnen und Kunden, wie sie sich im Zuge des Einsatzes von Big-Data-Ansätzen ergeben, Nutzengewinne für die Käuferinnen und Käufer entstehen. Andererseits wird dieser Nutzen erkauft durch die Preisgabe persönlicher Informationen, ohne dass die Bürgerinnen und Bürger, deren Daten gesammelt, ausgewertet und z. T. weitergegeben werden, hierzu speziell zugestimmt hätten. Zudem ist zu berücksichtigen, dass bei der Umsetzung von Big-Data-Ansätzen Entscheidungen unter dem Einsatz von Verfahren des Maschinellen Lernens algorithmisch umgesetzt werden. Dabei kann es dazu kommen, dass Daten, die dem maschinellen Lernprozess zugrunde gelegt wurden, bereits Verzerrungen enthalten, die dann in Entscheidungsregeln übertragen werden. Dies kann bereits bestehende diskriminierende Effekte verstärken oder sogar zementieren.[58]

Die Nutzung mehrseitiger Märkte in der digitalisierten Welt

Internetbasierte Leistungen werden zunehmend auf mehrseitigen Märkten angeboten, d. h., es wird die Möglichkeit genutzt, ökonomisch relevante Aktivitäten unterschiedlicher Akteure intelligent zu verknüpfen. Um für eine möglichst hohe Zahl von Nutzerinnen und Nutzern auf einer der Marktseiten attraktiv zu sein, kann es dabei auch betriebswirtschaftlich sinnvoll sein, eines oder mehrere Angebote zu einem Nullpreis oder sogar subventioniert anzubieten.[59] Auf diese Weise werden Dienstleistungen wie E-Mail-Dienste vermeintlich umsonst zur Verfügung gestellt, um dann mit dem Verkauf von Nutzerdaten oder dem datenbasierten gezielten Platzieren von Werbung Gewinne zu erzielen.

58 Ein besonders wichtiger Anwendungsbereich sind Bewerbungsplattformen, bei denen Verzerrungen gegen Minderheiten auftreten können. Vgl. Cowgill & Tucker (2017).

59 Vgl. hierzu Rochet & Tirole (2003), Rysman (2009) sowie Shy (2011).

Zwar haben mehrseitige Märkte bereits lange vor Schaffung des Internets existiert – wie z. B. Zeitungen, die ihre Nachrichten nicht nur über den Verkauf ihrer Druckexemplare, sondern auch über Werbung finanzieren. Doch Big Data eröffnet in diesem Bereich völlig neue Dimensionen. So werden über die o. g. Programmatischen Marktplätze jährlich Milliarden umgesetzt.

Mehrseitige Märkte entwickeln starke Konzentrationstendenzen. Zudem haben die entsprechend agierenden Unternehmen wie z. B. Google (Alphabet) oder Amazon angesichts hoher Gewinne gute Möglichkeiten, in weitere Marktsegmente vorzudringen und auf diese Weise ihre jeweiligen Marktpositionen zu verstärken. Aus diesem Grund werden sie von den Wettbewerbsbehörden inzwischen intensiv beobachtet. Allerdings stellt hohe Marktmacht bzw. -konzentration per se kein sicheres Indiz für ein Marktversagen dar, da die Bildung von mehrseitigen Plattformen auch mit hohen Effizienzgewinnen einhergehen kann, die ohne eine Konzentration nicht denkbar wären und auch Konsumenten zugutekommen können. Die wettbewerbsökonomische Analyse mehrseitiger Plattformen ist somit komplex und erfordert die Berücksichtigung einer Reihe von Aspekten, um den gesamtwirtschaftlichen Nutzen und die Kosten der Marktmacht von Plattformen abzuwägen.[60]

Datenbasierte Innovationen

Big-Data-basierte Geschäftsmodelle gelten oft als „disruptive Innovationen“. Der Begriff wird in den Wirtschaftswissenschaften unterschiedlich definiert. Die meisten Definitionen gehen jedoch von negativen Auswirkungen auf etablierte Anbieter aus, weil disruptive Innovationen die Wettbewerbsposition etablierter Anbieter angreifen. Der disruptive Effekt von Big-Data-Ansätzen entsteht dabei vor allem durch neue Geschäftsmodelle. So kann ein Geschäftsmodell, in dem Nutzerdaten monetarisiert werden, etablierte Anbieter vor Probleme stellen, da deren Produkte und Dienstleistungen durch Angebote angegriffen werden, die durch Datenmonetarisierung subventioniert sind oder im Extremfall zu einem Nullpreis oder als sog. „Freemium“[61] angeboten werden können. E-Mails beispielsweise stellen ein Konkurrenzprodukt für klassische Postdienstleistungen dar. Darüber hinaus ist es möglich, durch die Vernetzung digitaler Informationen bestimmte Produktions- oder Dienstleistungsschritte zu umgehen und somit einen erheblichen Wettbewerbsvorteil gegenüber herkömmlichen Anbietern zu erzielen. So vermittelt z. B. das Unternehmen Uber den direkten Kontakt zwischen Personen, die einen bestimmten Ort erreichen wollen, und privaten Autofahrerinnen und -fahrern, die sie gegen ein Entgelt dorthin mitnehmen.

Die Bedeutung datengetriebener Dienstleistungsangebote dürfte insgesamt weiter zunehmen. Persönliche Daten von Nutzerinnen und Nutzern digitaler Dienste stellen auf längere Sicht eine wichtige Ressource dar, da sie langfristig den Zugang zum Endkunden sichern.[62] In der Gesamtschau der Entwicklung zeigen sich starke Anreize für Anbieter unterschiedlichen Typs, datenbasierte Geschäftsmodelle zu verfolgen und selbst Daten der Produktnutzerinnen und -nutzer zu sammeln und zu monetarisieren. Dies führt zu einer Zunahme von Unternehmensfusionen und

60 Vgl. hierzu Schmalensee & Evans (2007) sowie Monopolkommission (2015).

61 Der Begriff „Freemium“ ist ein aus den Worten free und premium zusammengesetztes Kunstwort. Unter Freemium wird ein Geschäftsmodell verstanden, bei dem ein Produkt in der Basisversion kostenfrei angeboten wird, die Vollversion oder bestimmte Erweiterungen des Produkts jedoch kostenpflichtig sind. Als Beispiel kann Spotify dienen, ein Online-Musikanbieter, bei dessen Basisprodukt u. a. Einschränkungen bei der Musikwahl und durch Werbung bestehen – Beschränkungen, die das kostenpflichtige Vollprodukt nicht aufweist.

62 Für viele Investoren sind Unternehmen mit hohen Nutzerzahlen daher besonders attraktiv. Zur wachsenden Bedeutung von „Nutzerkapital“ für den Wert internetbasierter Unternehmen vgl. EFI (2016), Kapitel B3, Tab. B3-5.

-übernahmen, da größere Unternehmen bestrebt sind, erfolgreiche kleinere Anbieter aufzukaufen, sobald diese über einen ausreichend vernetzten, datenreichen Kundenstamm verfügen.[63] Den starken ökonomischen Gewinnanreizen des digitalen Marktes stehen bislang nur wenige ökonomisch relevante Anreize zur Entwicklung von Angeboten gegenüber, die Privatheit und Datenschutz gewährleisten (► Box „Übernahme WhatsApp durch Facebook“).

63 In jüngeren Diskussionsbeiträgen wird der Vermutung nachgegangen, dass die Marktkonzentration insgesamt angestiegen ist und dass neue „Super-Star Firms“ auftreten, die besonders kapitalintensiv arbeiten können, aber eine nur relativ geringe Arbeitsnachfrage haben. Damit liefert die Theorie der „Super-Star Firms“ eine Erklärung für den Rückgang des „Labor Share“. Vgl. Autor, Dorn, Katz, Patterson & Van Reenen (2017). Allerdings ist die empirische Fundierung dieser These noch nicht abgeschlossen.

Übernahme von WhatsApp durch Facebook und Klage der Europäischen Union

Das Unternehmen WhatsApp Inc. wurde 2009 in Santa Clara (Kalifornien) gegründet. Über WhatsApp können Textnachrichten, Bild-, Video-, Ton- und andere Dateien zwischen Einzelpersonen oder in Gruppen ausgetauscht werden. Der Zugang zu dieser Kommunikation erfolgt über mobile Anwendungsprogramme (Apps), die für verschiedene Smartphone-Betriebssysteme verfügbar sind. Im Frühjahr 2015 wurde auch erstmals internetbasierte Telefonie über die App ermöglicht. WhatsApp erreichte in kurzer Zeit sehr hohe Nutzerzahlen. So hatte der Dienst im Februar 2014 mehr als 450 Millionen Nutzerinnen und Nutzer.

WhatsApp wurde bereits früh für seine Allgemeinen Geschäftsbedingungen kritisiert, die dem Unternehmen erlauben, Daten der Nutzerinnen und Nutzer zu kommerziellen Zwecken zu verwenden. WhatsApp übermittelt alle Namen und Nummern aus den Telefon-Adressbüchern seiner Nutzerinnen und Nutzer an Server in den USA. Daher hatten die Datenschutzbehörden mehrerer Länder wegen Verletzungen des Datenschutzes Klagen eingereicht.

Am 19. Februar 2014 kaufte das US-Unternehmen Facebook Inc. WhatsApp Inc. für 19 Milliarden US-Dollar. Der Zusammenschluss wurde von der Europäischen Kommission ohne Auflagen genehmigt.[64] Bis April 2015 war die Nutzerzahl auf 800 Millionen Personen gestiegen. Als besonders umstritten erwies sich die Weitergabe der Nutzerdaten an Facebook nach der Übernahme von WhatsApp. Am 25. August 2016 kündigte WhatsApp eine aktualisierte Datenschutzerklärung an. Hierin wurde die Weitergabe der Nutzerdaten an Facebook auch zum Zweck der Optimierung von Werbemaßnahmen festgeschrieben. Viele Datenschutzverantwortliche haben diese Regelung für unzulässig gehalten, da sie früheren Aussagen der fusionierenden Unternehmen widersprach.

Besondere Bedeutung erlangte die Klage der Europäischen Kommission gegen Facebook Inc. Nach Angaben der Europäischen Kommission hatte Facebook im Antrag auf Genehmigung der Fusion im Jahr 2014 in irreführender Weise angegeben, das Unternehmen sei nicht in der Lage, einen automatischen Datenabgleich zwischen Nutzerkonten von WhatsApp und Facebook durchzuführen. Ein solcher Abgleich wurde aber im August 2016 angekündigt. Tatsächlich, so die Europäische Kommission, sei WhatsApp schon 2014 bekannt gewesen, dass diese Möglichkeit besteht. Die Kommission verhängte wegen der Irreführung eine Strafzahlung von 110 Millionen Euro gegen Facebook, blieb damit aber unter der Höchststrafe von 1 Prozent des Jahresumsatzes (248 Millionen Euro).[65]

Allerdings erklärte die Kommission auch, dass eine korrekte Angabe nicht zu einer Veränderung der Positiventscheidung im Jahr 2014 geführt hätte, da die Kommission bereits hypothetisch berücksichtigt habe, dass ein Nutzerabgleich stattfinden könne.

64 EC (2014).

65 Siehe hierzu: http://europa.eu/rapid/press-release_IP-17-1369_de.htm.

Handlungsfelder und Handlungsoptionen

Von der Digitalisierung geht ein enormer wirtschaftlicher Nutzen aus. Damit dieser Nutzen sich im Sinne möglichst vieler gesellschaftlicher Gruppen, z. B. Unternehmen, Wissenschaftlerinnen und Wissenschaftler sowie Verbraucherinnen und Verbraucher, entfalten kann, bedarf es eines ausgewogenen Zusammenspiels verschiedenster Maßnahmen: von der Unterstützung der Entwicklung neuer, innovativer Produkte über Maßnahmen zur Gewährleistung der Sicherheit digitaler Systeme bis hin zu Regulierungsmaßnahmen, um individuelle und kollektive Güter zu schützen. Dabei steht die Politik oftmals vor dem Dilemma, dass ein zu frühes regulatives Eingreifen in ökonomische Dynamiken auf die Entwicklung neuer Wirtschaftszweige, in diesem Fall der Digitalindustrie, innovationsfeindlich und hemmend wirken kann. Ein zu spätes Eingreifen hingegen kann dazu führen, dass sich einmal herausgebildete Marktpositionen verfestigen, zum Nachteil der Verbraucherinnen und Verbraucher ausgenutzt werden und einer innovationsfördernden Marktdynamik entgegenstehen.

▼ Handlungsfeld: Produktentwicklung und -anpassung unterstützen

(1) *Experimentierräume zur Verfügung stellen.* Wie sich Geschäftsmodelle, Unternehmen oder Nutzerverhalten entwickeln, ist gerade im Bereich der digitalen Transformation nicht immer absehbar. Frühe Regulierung kann bei Unsicherheit bezüglich der Auswirkungen schädlich sein. Daher kann es sinnvoll sein, Experimentierräume zu öffnen, in denen sich neue Geschäftsmodelle und Technologien zunächst ohne Eingriffe des Staates entwickeln. So kündigte die Financial Conduct Authority (FCA) im Vereinigten Königreich im November 2015 eine „Regulatory Sandbox“ an, in der Unternehmen aus der Finanzdienstleistung (Fintech-Unternehmen) zunächst von Regularien der Bankenaufsicht ausgenommen sein sollen.[66] Solche Reallabore wurden inzwischen auch in der Schweiz, Singapur, Australien und Malaysia eingerichtet.[67] Die darin realisierte Kooperation zwischen Regulierern und Unternehmen stellt alle Beteiligten vor eine schwierige Aufgabe. Gleichzeitig sind Reallabore u. U. eine ausgewogene Antwort auf das Problem der optimalen zeitlichen Gestaltung neuer Branchen und Technologien. Voraussetzung hierfür ist, dass der Schutz von Gemeinwohlgütern stets gewährleistet bleibt.

▼ Handlungsfeld: Systemsicherheit als relevanten Wirtschaftsfaktor erkennen und Standards etablieren

Den Schutz aller Nutzerinnen und Nutzer – der privaten, kommerziellen und staatlichen – zu gewährleisten, stellt eine der wesentlichen Herausforderungen der Digitalisierung dar. (► Box „Risiken für Cybersicherheit“).[68] Mit der Vielzahl neuer, vernetzter Geräte hat sich die potentielle Angriffsfläche für Cyberkriminalität massiv erhöht, wie die vielen inzwischen bekannt gewordenen gravierenden Fälle von Datendiebstahl belegen (► Box „Kriminalität und Big Data“). Dies stellt ein großes Risiko für betroffene Personen und für Unternehmen, aber auch für die gesamte Gesellschaft dar und kann langfristig einen Vertrauensverlust in digitale Technologien nach sich ziehen. Daher bedürfen Datenbestände und datengetriebene Anwendungen in besonderem Maße technischer Schutzmaßnahmen und -garantien. Der mit marktüblichen Geräten und Systemen einhergehende Schutz ist bisher unzureichend, insbesondere relativ zu dem monetären und gesellschaftlichen Wert solcher Anwendungen. Zugleich entwickeln sich die Möglichkeiten der Angreifer stetig weiter. Waren

66 Vgl. FCA (2015).
67 Vgl. Der Bundesrat (2016) für die Schweiz und MAS (2016) für Singapur.
68 Wischmeyer (2016).

für Angriffe früher ausgeprägte Hackerkenntnisse erforderlich, gibt es zunehmend vorgefertigte Angriffswerkzeuge. Malware und Angriffsinfrastrukturen wie Botnetze können von technisch wenig versierten Angreifern als „Crime as a Service" im Darknet gemietet werden. Darüber hinaus werden sich Angreifer der Zukunft durch einen immer höheren Organisationsgrad auszeichnen. Immer häufiger treten dabei auch staatliche Akteure in Erscheinung.

(1) *Sicherheitsstandards.* Kurz- und mittelfristig ist es dringend notwendig, adäquate Mindeststandards für System- und Datensicherheit sowie Privatsphärenschutz über alle Branchen hinweg zu etablieren und umzusetzen. Solche Standards sollten für Prävention, Abwehr und Analyse von Angriffen sowie für andere Risiken wie Datenverlust, Datenkorruption oder die kriminelle Energie von Mitarbeiterinnen und Mitarbeitern sowie Angestellten entwickelt werden.

(2) *Präventives Design.* Für die Systemsicherheit ist es wesentlich, kritische Systeme und Dienste von Beginn der Produktentwicklung an auch unter dem Gesichtspunkt der Produktsicherheit zu entwickeln (Security by Design). Dabei sollte nur Software zum Einsatz kommen, die für den Betrieb des Systems unverzichtbar ist und deren Korrektheit garantiert werden kann. Dies ist durch Testverfahren, Zertifizierung oder andere Verifikationsmaßnahmen nachzuweisen. Nicht vertrauenswürdige Software darf nur in geschützten Umgebungen ausgeführt werden. Zugangs- sowie Rollen- und Rechtemanagement für Nutzerinnen und Nutzer sowie Systemkomponenten sollten restriktiv gehandhabt werden. Ein Information Security Management System (ISMS) kann den Betreiber dabei unterstützen, Risiken und Sicherheit umfassend zu bewerten. Ebenso können anerkannte Zertifizierungen und regelmäßige Audits zu einem besseren Informationssicherheitsstandard beitragen. Gilt es, besonders sensible Daten zu schützen, sind dezentrale, in sich geschlossene Netze einer globalen Vernetzung vorzuziehen. Dabei kann sich auch der Ausbau lokaler Datenerfassung, -auswertung, -aggregation und -verwendung empfehlen.

(3) *Angriffsdetektion und -abwehr.* Systeme und Infrastrukturen müssen nach Stand der Technik bestmöglich nach außen abgesichert werden. Dies umfasst zum einen eine Reihe von etablierten Maßnahmen (Firewalls, verschlüsselte/authentifizierte Kommunikation, Intrusion Detection/Prevention u.Ä.), die verstärkt als Standards und Best Practices umgesetzt werden sollten. Darüber hinaus wird empfohlen, die Angriffsabwehr durch Forschung weiter zu stärken, etwa durch intensiveren Einsatz von Maschinellem Lernen bei der Früherkennung von Angriffen.

(4) *Nachvollziehbarkeit*. Systeme sollten so gestaltet werden, dass sie die Nachvollziehbarkeit und Zuordnung von Angriffen ermöglichen. Nur so können neue Angriffsmuster erkannt und analysiert werden. Dies ist sowohl zur Verbesserung der Systeme als auch für die Strafverfolgung relevant. Regulatorisch ist zu prüfen, ob Anreize zum Austausch über Angriffe geschaffen werden sollten, die über die gesetzlichen Vorgaben für Betreiber kritischer Infrastrukturen hinausgehen. Generell gilt es, die Durchführung von systematischen Schwachstellenanalysen zur Verhinderung möglicher Angriffe zu unterstützen.

(5) *Beschaffungs- und Haftungsregelungen*. Das Sicherheitsniveau von Produkten und Diensten kann mittelfristig durch entsprechend angepasste Beschaffungs- und Haftungsregelungen deutlich erhöht werden. Schon für die Beschaffung von IT ist es – im öffentlichen wie privaten Sektor – notwendig, Sicherheitsmechanismen zu etablieren. In kritischen Anwendungsbereichen sollten zudem Sicherheitstests oder Zertifikate nachgewiesen und deren Wirksamkeit durch Haftungsregeln gestärkt werden. Dafür sind Standards für praxisrelevante und branchenspezifische Tests zu entwickeln.

Hierbei sind zudem Möglichkeiten zur Weiterentwicklung von Software, Hardware und Diensten zu berücksichtigen, so dass folgende Fragen geklärt werden können: Ab wann sind neue Tests erforderlich? Bis wann sind partielle Tests hinsichtlich veränderter Teile möglich? Ab wann muss ein komplettes Produkt erneut getestet werden? Die Entwicklung solcher Standards sollte Gegenstand verstärkter Forschungsbemühung sein, während deren Etablierung, möglichst im internationalen Raum, der politischen Unterstützung bedarf.

Diese Maßnahmen sollten durch die Pflicht ergänzt werden, Sicherheitsupdates für bekannt gewordene Sicherheitslücken innerhalb der Gewährleistungsfrist bereitzustellen.[69]

(6) *Sicherer Datenaustausch für Unternehmen.* Die Realisierung von Industrie-4.0-Konzepten bedingt die Einführung von autonomen digitalen Subsystemen mit „digitalen Spiegelbildern", die reale Objekte in der digitalen Welt repräsentieren und Daten miteinander austauschen. Hierfür ist es notwendig, Prozess- und Bestandsdaten über Unternehmens-, möglicherweise auch über Ländergrenzen hinweg auszutauschen, die z. T. als sehr sensibel für die Beurteilung der Wirtschaftlichkeit von Unternehmensprozessen oder der Auftragslage eines Unternehmens einzuordnen sind. Damit ergibt sich grundsätzlich die Gefahr des Missbrauchs dieser Daten durch Wettbewerber, andererseits ist aber auch die Digitalisierung von Industrieprozessen ohne verteilte Daten kaum mehr zu realisieren.

Einen Ausweg aus diesem Dilemma bieten Plattformen, die von Herstellern für Zulieferer oder für unternehmensübergreifende Produktions- und Logistiknetzwerke von einer neutralen Institution betrieben werden (z. B. Industrial Data Space e. V.[70]) und garantieren, dass nur genau auf die Daten zugegriffen wird, die im Rahmen eines definierten Kommunikationsprozesses zur Verfügung stehen müssen. Dabei ist wichtig, dass Verfügbarkeit und Zugang, Integrität, Vertraulichkeit und zulässige Verwertung für alle Daten eindeutig geregelt sind.[71]

(7) *Nachhaltigkeit durch langfristig angelegte Grundlagenforschung.* Die oben skizzierten Maßnahmen sollten durch eine langfristige Forschungsagenda ergänzt werden. Seit Jahrzehnten gibt es in der IT-Sicherheit einen immer schneller werdenden Kreislauf von der Entdeckung neuer Angriffsvektoren und auf diesen Angriff zugeschnittenen Abwehrmaßnahmen. Um aus diesem Kreislauf auszubrechen und Systeme zu entwickeln, die nachweislich ganze Kategorien von Angriffen unmöglich machen (wie es z. B. in der Kryptographie bereits gelungen ist), ist es notwendig, verstärkt Grundlagenforschung zum Design völlig neuartiger sicherer Systeme zu betreiben.

69 Waidner, Backes, & Müller-Quade (2017).
70 Industrial Data Space Association (o. J.).
71 Hornung & Hofmann (2017).

Risiken für Cybersicherheit

Die Entwicklung der Digitalisierung und insbesondere des Einsatzes von Big Data ist verkoppelt mit Risiken der Gefährdung der Funktionsfähigkeit informationstechnischer Systeme[72] mit erheblichen gesellschaftlichen Auswirkungen. Zugleich bietet die Nutzung von Big Data auch einen Ansatzpunkt zur Verbesserung der IT-Sicherheit. So erlauben Big Data Analytics schnelle, vielfach in Echtzeit erfolgende Vorkehrungen, um einen Angriff auf IT-Systeme oder einzelne Kommunikationsvorgänge zu erkennen, zu bekämpfen und mögliche Schäden zu begrenzen. Big Data Analytics sind insbesondere dazu in der Lage, Aktivitätsmuster, die eine Gefahr für das informationstechnische System darstellen, zu erkennen und bei der Wahrnehmung ungewöhnlicher Aktivitäten schnelle Reaktionen zu ermöglichen.

Betroffen von den Risiken der Cybersicherheit sind nicht nur Privatpersonen und Unternehmen, sondern auch staatliche Stellen. Auch handelt es sich nicht nur um ein nationales, sondern um ein trans- und internationales Problem. Cybersicherheit erfordert die Gewährleistung der Integrität cybertechnischer Systeme. Dies betrifft zum einen technische Vorkehrungen für die Vermeidung von Schadwirkungen aus dem (bestimmungsgemäßen) Gebrauch solcher Systeme (z. B. die Gewährleistung eines unfallsicheren Betriebs vernetzter autonomer Fahrzeuge oder Roboter). Im englischen Sprachgebrauch wird dieser Aspekt durch den Begriff der Cybersafety ausgedrückt. Zweitens ist die Integrität cybertechnischer Systeme gegen externe Angriffe oder externe Missbrauchsversuche (Hackerangriffe) zu schützen: Dies betrifft den Aspekt der Cybersecurity. Im Deutschen fallen beide Begriffe im Terminus „Sicherheit“ sprachlich zusammen – die Begriffe „Unfallsicherheit“ und „Einbruchsicherheit“ bilden das englische Begriffspaar Safety/Security näherungsweise ab.

Da in der EU auch der grenzüberschreitende Waren-, Dienstleistungs- und Personenverkehr von Cyberangriffen betroffen sein kann, hat die EU den Mitgliedsstaaten besondere Pflichten in Gestalt einer Richtlinie[73] auferlegt. Nach Art. 1 der Richtlinie sollen Maßnahmen ergriffen werden, um ein hohes gemeinsames Sicherheitsniveau von Netz- und Informationssystemen in der Union zu erreichen, speziell um das Funktionieren des Binnenmarktes zu verbessern. Hierfür wird vorgesehen: die Pflicht für alle Mitgliedsstaaten, eine nationale Strategie für die Sicherheit von Netz- und Informationssystemen festzulegen; die Schaffung einer Kooperationsgruppe, um die strategische Zusammenarbeit und den Informationsaustausch zwischen den Mitgliedsstaaten zu unterstützen und zu erleichtern und Vertrauen zwischen ihnen aufzubauen; die Schaffung eines Netzwerks von Computer-Notfallteams, um zum Aufbau von Vertrauen zwischen den Mitgliedsstaaten beizutragen und eine rasche und wirksame operative Zusammenarbeit zu fördern; Sicherheitsanforderungen und Meldepflichten für die Betreiber wesentlicher Dienste und für Anbieter digitaler Dienste und schließlich die Pflicht der Mitgliedsstaaten, nationale zuständige Behörden, zentrale Anlaufstellen und Computer-Notfallteams mit Aufgaben im Zusammenhang mit der Sicherheit von Netz- und Informationssystemen zu benennen. In Umsetzung der Richtlinie hat der Bundesgesetzgeber das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz) durch Novelle vom 23. Juni 2017 modifiziert (BGBl. I 1885). Hervorzuheben ist, dass diese beiden Rechtsgrundlagen auch besondere Regeln für die Betreiber „wesentlicher Dienste“ vorsehen, das heißt für öffentliche oder private Einrichtungen, die einen IT-Dienst bereitstellen, der für die Aufrechterhaltung kritischer gesellschaftlicher und/oder wirtschaftlicher Tätigkeiten unerlässlich ist, und ein Sicherheitsvorteil durch Eingriffe ersichtlich gestört würde.

72 Samsel (2016).

73 Europarl & European Council (2016b).

Dies betrifft etwa die Sektoren Luftfahrt, Schienenverkehr, Schifffahrt und Straßenverkehr. Die Leistungsfähigkeit dieser Sektoren kann durch den Einsatz von Big Data deutlich gesteigert werden. Ihre Funktionsfähigkeit ist aber gefährdet, wenn nicht auch unter Nutzung von Big Data geeignete Vorkehrungen zum Schutz der Sicherheit der Infrastrukturen getroffen werden. Ob die insoweit von der EU und dem Bundesgesetzgeber geschaffenen Vorkehrungen sowie die Tätigkeit des Bundesamts für Sicherheit ausreichen, lässt sich gegenwärtig noch nicht übersehen.

Kriminalität und Big Data

Durch die Verknüpfung von mehr oder weniger frei verfügbaren oder gehackten Daten wie Bewegungsprofilen, Daten zur Gesichtserkennung, Bankdaten, Daten persönlicher Art aus sog. sozialen Netzwerken, medizinischen Daten aus nicht hinreichend geschützten Datenbanken etc. lassen sich viele Delikte dramatisch vereinfacht begehen. Tatorte und Tatgelegenheiten können erheblich leichter ausgespäht, Opfer präziser individualisiert und verfolgbare Spuren besser vermieden werden. Hinzu kommt, dass die Begehung der Delikte teilweise aus Ländern heraus erfolgen kann, in welchen die deutschen Strafverfolgungsbehörden keinen Zugriff haben.

Als Delikte kommen beispielsweise in Betracht: Betrug mit gefälschten Internetseiten, gefälschten Arzneimitteln, Bestellung von Waren unter Scheinidentitäten etc.; Erpressung unter Nutzung von aus sozialen Netzwerken oder Datenbanken generierten Informationen; Nötigung mit der Offenbarung von rufschädigenden Informationen; Volksverhetzung, Anleitung zu Straftaten, Stalking und Mobbing unter Nutzung von mit Big Data gewonnenen Informationen über mögliche Opfer; Sachbeschädigung und Sabotage z. B. durch Einschleusen von Schadsoftware in Industrieanlagen und sog. Smart Homes. Neben Delikten gegen Privatpersonen kommen auch Delikte gegen die Allgemeinheit in Betracht wie etwa Geldwäsche, Wahlfälschung und Verstöße gegen das Kriegswaffenkontrollgesetz.

Diesen Gefahren sollte nicht nur mit Strafrechtsnormen oder etwa einem (verbesserten) Datenschutzrecht begegnet werden, sondern ihnen muss bereits von technischer Seite durch die Entwicklung geeigneter Vorkehrungen zumindest teilweise Einhalt geboten werden. Eine Verpflichtung zur Verwendung solcher Vorkehrungen sollte gesetzlich normiert werden.

▼ Handlungsfeld: Unternehmen in Gestaltungsprozesse und Regulationen einbeziehen

(1) *Selbst- und Co-Regulierung.* Zur verantwortungsvollen und verbindlichen Gestaltung der Anwendungen von digitalen Technologien kommen neben hoheitlichen Schutzvorkehrungen selbstverständlich auch Selbstregulierungen der IT-Wirtschaft oder Co-Regulierungen zwischen einerseits hoheitlichen und andererseits privaten (privatwirtschaftlichen) Akteuren in Betracht.[74] Bisher aber gibt es nur begrenzte Ansätze für wirksamen Rechtsgüterschutz Dritter durch Selbstregulierungen der IT-Wirtschaft oder durch Co-Regulierungen.[75] Als Mittel der Selbstregulierung wäre auch die Schaffung von Institutionen zur Entwicklung von Best Practices oder von Benchmarking-Systemen möglich.

74 Zu den Möglichkeiten der Selbstregulierung, allerdings vorrangig im Hinblick auf traditionelle Medien, siehe Schulz & Held (2002). Zu Fragen von Regulierung und Co-Regulierung siehe ferner Latzer, Just, Saurwein & Slominski (2002); Hoffmann-Riem (2016b). Zur Selbstregulierung speziell beim Datenschutz siehe etwa Abel (2003), S. 11; Bizer (2001), S. 168 ff.; Schröder (2012).

75 Interessant – wenn auch auf audiovisuelle (AV-) Medien und nicht speziell Big Data bezogen – sind Regelungen, die im Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Änderung der Richtlinie 2010/13/EU zur Koordinierung bestimmter Rechts- und Verwaltungsvorschriften in Mitgliedsstaaten über die Bereitstellung audiovisueller Mediendienste im Hinblick auf sich verändernde Marktgegebenheiten enthalten sind, EC (2016b).

Einseitig aufgestellte unverbindliche Grundsätze gewähren ebenso wie einseitig aufgestellte Datenschutzrichtlinien von Unternehmen nur sehr begrenzten Schutz. Angesichts der Machtasymmetrien im IT-Bereich und damit der Möglichkeit einseitiger Interessendurchsetzung durch machtvolle Unternehmen kann kaum erwartet werden, dass effektive Vorkehrungen, die das Individual- und Gemeinwohl in abgewogener Weise sichern, allein durch Selbstregulierung geschaffen werden. Hoheitlich verantwortetes und durchgesetztes Recht ist als Gegengewicht gegen private Macht und insofern als Instrument der Freiheitssicherung aller Bürgerinnen und Bürger in vielen Bereichen weiterhin unverzichtbar. Dieses kann insbesondere als Recht zur Umhegung der Selbstgestaltung bzw. Selbstregulierung durch Unternehmen eingesetzt werden (regulierte Selbstregulierung).

(2) *Codes of Conduct*. Ein mögliches regulatives Element, das gerade auch im Sinne des Verbraucher- und Datenschutzes zum Einsatz gebracht werden kann, stellen Verhaltensregeln (Codes of Conduct) dar, die von Verbänden der IT-Wirtschaft aufgestellt werden und ggf. auch im Zusammenwirken einzelner Unternehmen entstehen. Solche Codes of Conduct sind jedoch, wenn sie ausschließlich von der IT-Wirtschaft verantwortet werden, mit dem Risiko ihrer zu einseitigen Ausrichtung an den Unternehmensinteressen verknüpft. Um dies zu vermeiden, empfiehlt es sich, inhaltliche und prozedurale Mindestanforderungen zu normieren. Ansätze dafür enthält die EU-DSGVO (► Box „Art. 40–42 EU-DSGVO“). Empfehlenswert ist es, in den Verfahren auch eine Mitwirkung von Vertreterinnen und Vertretern der Zivilgesellschaft vorzusehen, die Nutzerinteressen verfolgen. Anstelle der in der EU-DSGVO bereits vorgesehenen bloßen Möglichkeiten einer hoheitlichen Überprüfung und Genehmigung der Verhaltensregeln müssten entsprechende Pflichten vorgesehen werden – ggf. auch nur zur Zertifizierung durch akkreditierte Stellen, sollte sich die bisherige Regelung nicht als wirksam erweisen.

Art. 40–42 EU-DSGVO

Diese Artikel enthalten Regelungen für von Verbänden und Unternehmen geschaffene, den Umgang mit personenbezogenen Daten betreffende Verhaltensregeln, die zur ordnungsgemäßen Anwendung der Verordnung durch Stellen der Mitgliedsstaaten und der EU beitragen sollen. Art. 40 Abs. 2 EU-DSGVO führt eine Vielzahl von Themenbereichen auf, für die Präzisierungen erfolgen können. Solche Präzisierungsanregungen sind als regulative Orientierungen für die Verhaltensregeln gedacht, zu deren Erlass die Verbände oder Vereinigungen allerdings nicht verpflichtet sind. Ebenso sind sie nicht verpflichtet, von der weiteren, in Abs. 5 vorgesehenen Möglichkeit Gebrauch zu machen, den Entwurf der Verhaltensregeln der Aufsichtsbehörde vorzulegen. Die Behörde soll – wenn der Entwurf eingereicht wird – in einer Stellungnahme darlegen, ob die Verhaltensregeln mit der Verordnung vereinbar sind. Sind dafür ausreichende Garantien vorhanden, wird der Entwurf der Verhaltensregeln von der Behörde genehmigt (Abs. 5). Anschließend gelten unterschiedliche Verfahren je nachdem, ob der Entwurf Verarbeitungstätigkeiten nur in einem oder in mehreren Mitgliedsstaaten betrifft (auch Abs. 6–8). Sind die Prüfungen positiv, kommt es am Ende des Verfahrens zu einer amtlichen Veröffentlichung (Abs. 6, 11). Gelten Verhaltensregeln in mehreren Mitgliedsstaaten, kann die EU-Kommission sogar im Wege von Durchführungsrechtsakten beschließen, dass sie allgemeine Gültigkeit in der EU besitzen (Abs. 9). Art. 41 der EU-DSGVO sieht für die Überwachung der Einhaltung von Verfahrensregeln Möglichkeiten zur Akkreditierung der dafür geeigneten Stellen vor. Auch datenschutzrechtliche Zertifizierungsverfahren (sowie Datenschutzsiegel und -prüfzeichen) werden angestrebt, s. Art. 42 EU-DSGVO.

(3) *Transnationale Governance*. Es wird empfohlen, neue – insbesondere international und global wirksame – Regelungsinstrumente einzuführen. Anzustreben sind dabei Konzepte und Einrichtungen einer vor allem transnationalen Governance im IT-Bereich, die auf Kooperation mit den unterschiedlichen Akteuren (insbesondere Verbänden und Unternehmen der IT-Wirtschaft sowie Nichtregierungsorganisationen (NGOs)) ausgerichtet sind.

▼ Handlungsfeld: Marktdiversität schützen – Oligopolisierung entgegenwirken

(*1*) *Standardisierungen*. Datenformate und Protokolle sollten branchenweit standardisiert werden, um ein Verständnis der Daten(-semantik) zu ermöglichen und den automatisierten Datenaustausch voranzubringen. Dies ist auch eine Maßnahme, um Tendenzen der Monopolbildung entgegenzuwirken. So würde eine Standardisierung Nutzerinnen und Nutzern eine schnelle und reibungslose Migration zwischen Diensten erlauben, indem sie ihre Daten problemlos „mitnehmen" und transferieren könnten. Die Wahlfreiheit des Nutzers – und damit auch seine Position gegenüber Dienstleistern – wäre gestärkt. In letzter Konsequenz könnten hier, unterstützt durch regulatorischen Druck, auch standardisierte Echtzeit-Schnittstellen gefordert werden, die es erlauben, etwa unterschiedliche Messenger-Dienste miteinander zu vernetzen und so einen nutzerseitig kontrollierten Austausch von Nachrichten über Plattformen hinweg zu implementieren. Dadurch könnten Nutzerinnen und Nutzer auf alternative Anbieter zurückgreifen oder zu einem solchen wechseln, ohne dass dies die Kommunikation innerhalb ihrer sozialen Netze negativ beeinträchtigen würde. Durch eine solche Öffnung von Plattformen würden sich die Besitz- und Verfügungsrechte in Bezug auf Daten verschieben. Auch ist ein positiver Beitrag in Bezug auf technologische Innovation zu erwarten.

(*2*) *Regulierungsrecht zum Schutz von Gemeinwohlzwecken ausweiten.* Zu den aktuell lösungsbedürftigen Problemen gehören die Disparität der Verteilung von Marktmacht und insbesondere die Oligopolisierung in besonders wichtigen IT-Teilmärkten. Dringend erscheinen effektive Maßnahmen, die nicht nur auf die Funktionsfähigkeit des Marktes, sondern auch auf die Sicherung anderer Gemeinwohlzwecke gerichtet sind. Dies kann durch besondere Gesetzgebung erfolgen, aber auch durch ein neu konzipiertes Regulierungsrecht, das Marktmacht auch insoweit begrenzt, als es im Interesse eines erweiterten Freiheitsschutzes nicht nur an ökonomischen Parametern ausgerichtet ist. Zu erwägen ist beispielsweise der Vorschlag des Europaparlaments zur Entflechtung zwischen Suchmaschinen und anderen kommerziellen Dienstleistungen.[76]

(*3*) *Fusionskontrolle erweitern – 9. Novelle GWB sorgfältig testen*. Die 9. Novelle des Gesetzes gegen Wettbewerbsbeschränkung (GWB) ermöglicht es dem Bundeskartellamt, bei der Fusionskontrolle auch das Marktpotential und die wirtschaftliche Bedeutung des Zielunternehmens zu erfassen. Mit dieser Erweiterung des Anwendungsbereichs der Fusionskontrolle hat der deutsche Gesetzgeber Schritte eingeleitet, um Wettbewerb auch dann zu schützen, wenn sich zukünftige marktmächtige Positionen noch nicht in den üblichen Erfassungsgrößen (Umsätze) messen lassen (► Box „Novelle GWB"). Die Auswirkungen der Novelle auf die digitale Wirtschaft und die Nutzung von Big-Data-Ansätzen sind allerdings offen und sollten gezielt evaluiert werden. Das Kartellamt sollte ein systematisches Monitoring vornehmen.

76 Europarl (2014), Abs. 15–18.

(*4*) *Verbesserungen der Rechtsdurchsetzung.* Die Durchsetzung von Missbrauchsverboten auf dynamischen Plattformmärkten erfolgt nur langsam und schwerfällig.[77] Verpflichtungsentscheidungen (Art. 9 VO 1/03; § 32b GWB), die als Instrument zur Steigerung der Verfahrensökonomie ins Wettbewerbsverfahrensrecht eingeführt worden sind, erfüllten diesen Zweck nicht im notwendigen Umfang. Hier sollte dem Vorschlag der Monopolkommission gefolgt werden, Verpflichtungsverfahren automatisch 1 Jahr nach dem Angebot von Verpflichtungszusagen der betroffenen Unternehmen in ein Abstellungs- und Bußgeldverfahren zu überführen.[78] Damit könnten die Verfahren beschleunigt werden.

(*5*) *Zügiges Einschreiten unter Nutzung des Verfahrensrechts.* Einem weiteren Vorschlag der Monopolkommission folgend,[79] wird empfohlen, Wettbewerbsbehörden zu ermächtigen, die Anordnung einstweiliger Maßnahmen in Zukunft stärker zu nutzen, um vermuteten Missbrauch einzuschränken oder seine Fortentwicklung bis zum Vorliegen einer abschließenden Bewertung aufzuhalten. Angesichts der hohen Dynamik in digitalen Märkten und der Neuheit der Geschäftsmodelle würde somit Zeit gewonnen, um Sachverhalte präziser zu bewerten. Die zuständigen Behörden sollten die bisher gezeigte Zögerlichkeit bei der Nutzung einstweiliger Maßnahmen überwinden, da ansonsten die bloße Prozessdynamik dazu führen kann, vollendete und nicht mehr ohne Weiteres reversible Tatsachen zu schaffen. Um zu verhindern, dass vom verstärkten Einsatz einstweiliger Maßnahmen Gefahren für Innovation ausgehen, wird die Einführung eines Testverfahrens vorgeschlagen,[80] um zu prüfen, ob wesentliche Marktveränderungen schon innerhalb von 2 Jahren zu erwarten sind. Ziel dieser und weiterer Empfehlungen ist es, die Geschwindigkeit der Regulierung an die der Wirtschaftsprozesse anzupassen.

(*6*) *Systematik zum Umgang mit marktbeherrschenden Stellungen weiterentwickeln*. Die Monopolkommission hat auf die Notwendigkeit aufmerksam gemacht, dass die missbräuchliche Ausnutzung einer marktbeherrschenden Stellung in Plattformmärkten besondere Beachtung benötigt.[81] Hier bedarf es weiterer Forschungsarbeiten, denn es fehlen z. T. noch die analytischen Werkzeuge, um eine solche Ausnutzung sinnvoll von effizienzerhöhendem Verhalten abzugrenzen. Auch im Hinblick auf die Abgrenzung von Märkten[82] werden die Besonderheiten mehrseitiger Plattformen derzeit noch nicht ausreichend berücksichtigt, so dass auch in diesem Bereich weitere Forschungsanstrengungen unternommen werden sollten.

77 Schweitzer, Fetzer, & Peitz (2016) verweisen in diesem Zusammenhang auf das seit November 2011 bei der EU-Kommission anhängige Verfahren gegen Google.

78 Monopolkommission (2015).

79 Monopolkommission (2015), Abs. 584.

80 Monopolkommission (2015), Abs. 584.

81 Monopolkommission (2015), Abs. 579.

82 Monopolkommission (2015), Abs. 585.

B Individuelle und gesellschaftliche Auswirkungen

Wie bereits in den einleitenden Kapiteln dargelegt, haben sich mit der Etablierung digitaler Dienstleister in nahezu allen privaten wie öffentlichen Lebensbereichen die Rahmenbedingungen für Privatheit fundamental verändert. Eine Vielzahl der angebotenen Leistungen wird dadurch entgolten, dass dem Anbieter durch den Nutzer das Recht eingeräumt wird, alle dem Anbieter zugänglichen Daten des Nutzers zu speichern und zu verknüpfen, nicht zuletzt, um dadurch Erkenntnisse zu gewinnen, die es Anbietern ermöglichen, auf die Interessen und Bedürfnisse des Nutzers ausgerichtete Angebote zu unterbreiten und Einfluss auf deren Entscheidungsfindungen zu nehmen.

Während ein Teil der Nutzerinnen und Nutzer dieses Vorgehen nicht als problematisch empfindet, sind anderen diese Zusammenhänge insbesondere aufgrund einer fehlenden Digitalkompetenz nicht bewusst. Darüber hinaus kommt es häufig zu der als paradox empfundenen Situation, dass selbst Nutzerinnen und Nutzer, denen der Schutz ihrer Privatsphäre wichtig ist,[83] in ihrem Onlineverhalten eine oftmals massive Preisgabe von privaten Daten billigend in Kauf nehmen (sog. Privacy Paradox[84]). Dies ist insbesondere auf eine zunehmende Zwangslage der Nutzerinnen und Nutzer zurückzuführen: Da die Nutzung vieler Dienste in der Regel nicht ohne die Preisgabe der Daten möglich ist, wäre die einzige verbleibende Alternative, auf die jeweilige Dienstleistung zu verzichten. Dieser würde jedoch mit erheblichen Einschränkungen in der sozialen, zunehmend aber auch materiellen Teilhabe in einer modernen Gesellschaft einhergehen.

Neben Nutzungsdaten werden allein schon durch die Bewegung im öffentlichen Raum und andere alltägliche Aktivitäten eine Vielzahl an Daten, teils personenbezogen, teils anonym, erfasst, deren Auswertung sich ebenfalls auf das Leben des Einzelnen auswirken kann. Durch die Digitalisierung wird damit auf vielfältige Weise in den eigentlichen Schutzraum der Privatsphäre eingedrungen, zumeist ohne dass das Individuum davon Kenntnis hat bzw. ohne dass es Kontrolle darüber ausüben kann.

Hinzu kommt, dass durch Anwendungen von Big Data und statistischen Auswertungen zunehmend gesellschaftsrelevantes Wissen und damit Macht generiert wird. Da der Zugang zu den entsprechenden Daten und Auswertungsmethoden derzeit vor allem bei wenigen privaten Unternehmen sowie begrenzt auch beim Staat liegt, entsteht eine zunehmende „informationelle Asymmetrie“: Der Bürger bzw. Nutzer kann weder nachvollziehen, auf welcher Datengrundlage konkrete Entscheidungen über ihn getroffen werden, noch kann er diese kontrollieren. Dies wird sich umso mehr intensivieren, je mehr Daten erhoben, gespeichert und verarbeitet werden.

Gesellschaftliche Bedeutung der Privatheit

Dieses Eindringen in die Privatsphäre wirkt sich nicht nur auf das Individuum, sondern auch auf die Gesellschaft insgesamt aus. So verweist die Philosophin Beate Rössler auf 3 Dimensionen von Privatheit: (1) Privatheit als individuelles Freiheitsrecht, (2) die soziale Dimension und (3) die politische Dimension des Privaten. Ihr zufolge führt der Verlust von Privatheit zu einer Einschränkung

83 Während der Begriff der „Privatsphäre“ im alltäglichen Diskurs synonym mit „Privatheit“ verwendet wird, erfolgte in den Wissenschaften und der Rechtsprechung eine Abkehr von der Sphärentheorie und damit der teilweise Verzicht auf diesen Begriff. Allerdings spricht für die synonyme Verwendung von „Privatheit“ und „Privatsphäre“, dass Letztere auch metaphorisch gemeint sein kann: ein abstrakter semantischer „Raum“ der Informationen, Handlungen und Entscheidungen, der sich durch variable Grenzen und Grenzziehungen auszeichnet und durch Zugangskontrollen manifestiert. In diesem erweiterten Verständnis wird der Begriff „Privatsphäre“ in der Privatheitsforschung weiter verwendet.

84 Barnes (2006).

individueller Freiheitsräume und zu einer Veränderung sozialer Beziehungen, die zunehmend homogenisiert werden, sowie zu einer erhöhten Manipulierbarkeit. Dies trägt wesentlich dazu bei, dass sich Einschränkungen in der Privatheit in der Folge auch auf demokratische Prozesse auswirken. Auch der Politologe und Jurist Alan F. Westin (1967) sieht Privatheit als notwendige Voraussetzung für die individuelle Autonomie, Identität und Integrität einer Person.[85] Ihm zufolge erfüllt Privatheit 4 zentrale Funktionen: *Personal Autonomy* – die Freiheit, von anderen nicht manipuliert oder dominiert zu werden, *emotional Release* – der Rückzugsraum, der es ermöglicht, frei von sozialem Druck und gesellschaftlichen Erwartungen „ganz man selbst zu sein", *Self-Evaluation* – die Gelegenheit, Erfahrungen und Eindrücke zu reflektieren, um ein authentisches, selbstbestimmtes Leben zu führen, sowie *limited and protected Communication* – die Möglichkeit, zwischen den Adressaten personenbezogener Informationen zu differenzieren, die Grenzen zwischenmenschlicher Nähe bzw. Distanz zu definieren und private Informationen in einem geschützten Raum mit Vertrauten auszutauschen. Ein wesentlicher Grund, weshalb Privatheit schützenswert ist, liegt demnach in ihrer Relevanz für eine positive und persönliche Identitätsbildung, die einer freien und selbstbestimmten Entwicklung bedarf.[86] Die langfristigen Folgen einer Gefährdung der Privatheit im Big-Data-Zeitalter[87] sind insbesondere eine Zunahme von Diskriminierung, eine Normierung der Gesellschaft, ein Verlust an Autonomie und freier Entscheidung, eine zunehmende Gefahr von Manipulation sowie eine Destabilisierung demokratischer Willensbildungs- und Entscheidungsprozesse. Eine Gesellschaft, die keine Freiheitsräume mehr garantieren kann, ist nicht in der Lage, die gesellschaftliche Vielfalt zu erhalten, aus der heraus sich ein offener und freier politischer Diskurs entfaltet.[88]

Datenschutz zum Schutz der Privatheit

Ein wesentliches Werkzeug, um den Schutz der Privatheit der Bürgerinnen und Bürger zu gewährleisten, stellt bislang das Datenschutzrecht dar (► Box „Datenschutz und Datenschutzrecht"). Das zentrale Schutzgut des Datenschutzes besteht in der informationellen Selbstbestimmung der Bürgerinnen und Bürger. Das Recht auf informationelle Selbstbestimmung wurde vom Bundesverfassungsgericht (BVerfG) bereits 1983 in seinem Volkszählungsurteil aus dem allgemeinen Persönlichkeitsrecht und dem Schutz der Menschenwürde abgeleitet und beinhaltet das Recht des Einzelnen, selbst über die Preisgabe und Verwendung personenbezogener Daten zu bestimmen. Das BVerfG erkennt hier zudem an, dass unter den Verarbeitungs- und Verknüpfungsmöglichkeiten der Informationstechnologie auch ein für sich vielleicht belanglos erscheinendes Datum einen neuen Stellenwert bekommen kann und es daher keine belanglosen Daten gibt. Dies gilt mehr denn je im Zeitalter von Big Data: Ein Datum, das für sich gesehen wenig geeignet erscheint, die informationelle Selbstbestimmung bedrohen zu können, ist beispielsweise innerhalb eines mit anderen derartigen Daten gebildeten Profils in der Lage, empfindliche Meta-Informationen über den Betroffenen zum Vorschein bringen.

Mit der am 25. Mai 2018 in Kraft getretenen EU-Datenschutz-Grundverordnung hat die Europäische Union einen neuen europaweiten Rahmen für den Datenschutz geschaffen. Da dieser Rahmen nunmehr nach Art. 3 EU-DSGVO und

85 Westin (1967), S. 35–42.

86 Vgl. Wiegerling (2011); S. 59, Floridi (2015), S. 159–166.

87 Vgl. u. a. Mayer-Schönberger & Cukier (2013), S. 198–214 zu den Risiken der Datafizierung.

88 Rössler (2016). Nach Carlos Becker und Sandra Seubert gewährleistet Privatheit darüber hinaus auch „kommunikative Autonomie" und trägt damit zur Verwirklichung von Demokratie als kommunikativem Miteinander bei, Becker & Seubert (2016).

§ 1 Abs. 4 BDSG (neu) unter den dort beschriebenen Voraussetzungen auch auf außereuropäische Unternehmen Anwendung findet, besteht die Möglichkeit, dem Datenschutz effektiver als bisher Geltung zu verschaffen. Die Möglichkeit, am Umsatz orientierte Strafzahlungen bei Verletzung des Datenschutzes vorzusehen, ermöglicht es, den Vorgaben auch gegenüber global agierenden Unternehmen Geltung zu verschaffen.

Entscheidend für den grundrechtlichen Schutz der informationellen Selbstbestimmung und das darauf bezogene Datenschutzrecht ist der Begriff der personenbezogenen Daten. Als solche gelten nach Art. 4 Nr. 1 EU-DSGVO Daten, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Als identifizierbar wird nach dieser Norm eine natürliche Person angesehen, „die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kenn-Nummer, zu Standortdaten, zu einer Onlinekennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Personen sind, identifiziert werden kann". Daten sind nicht mehr personenbezogen, wenn sie anonymisiert wurden und nicht mehr deanonymisierbar sind.[89]

Dabei ist zu berücksichtigen, dass die Techniken der Deanonymisierung immer ausgefeilter werden. Ferner ist dem Umstand Rechnung zu tragen, dass personenbezogene Folgerungen z. T. auch möglich sind, ohne alle relevanten personenbezogenen Daten bei der betroffenen Person selbst zu erheben. Dies ist etwa der Fall, wenn personenbezogene und ggf. weitere Daten im Zuge von Big-Data-Analytik mithilfe statistischer Methoden und der Ermittlung von Korrelationen zur Bildung einer Personengruppe mit vergleichbaren Charakteristika genutzt werden und anschließend auch weitere Personen dieser Gruppe auf der Grundlage einzelner gleicher Faktoren zugeordnet werden und diese Zuordnung für Folgerungen auch hinsichtlich weiterer, nicht personenbezogen erhobener Eigenschaften (etwa betreffend Fragen der Gesundheit, der Finanzkraft oder der sexuellen Orientierung) eingesetzt wird.[90]

Die Betrachtung darf daher nicht auf personenbezogene Daten beschränkt bleiben: Eine Vielzahl von Big-Data-Anwendungen beruht zwar auf nicht personenbezogenen Daten im Sinne der EU-DSGVO, doch gibt es zahlreiche Möglichkeiten, mithilfe von wenigen nicht personenbezogenen Daten Rückschlüsse auf Individuen zu ziehen. Dies ist beispielsweise der Fall, wenn sich mehrere wiederkehrende Merkmale (z. B. Aufenthaltsorte) in einem Datensatz befinden. Je größer die Datensätze, desto wahrscheinlicher sind die Merkmalskombinationen, welche die Unterscheidung zwischen personen- und vermeintlich harmlosen, nicht personenbezogenen Daten verschwimmen lassen.

Darüber hinaus besteht das Risiko, dass die potentiellen Datenschutzrisiken statistisch ermittelter Gruppenmerkmale systematisch unterschätzt werden bzw. sogar einen „blinden Fleck des Datenschutzrechts" darstellen.[91] Ein Beispiel dafür sind Predictive-Analytics-Verfahren allgemein und das Predictive-Policing-Verfahren im Besonderen. Letzteres gewinnt

89 Näher Erwägungsgrund 26 der EU-DSGVO.

90 Solche Vorgehensweisen – die etwa Datenkategorien wie Alter, Geschlecht, Familienstand, Beruf, Wohnort u.Ä. nutzen – können durch gezielte statistische Auswertungen ähnliche Aussagen erzielen wie durch die Auswertung personenbezogener Daten, ohne dass die Betroffenen etwas davon erfahren und ohne dass ihre konkreten persönlichen Eigenschaften berücksichtigt werden. Werden solche statistischen Ergebnisse als Grundlage zur Einschätzung gravierender Entscheidungen wie z. B. über die Kreditwürdigkeit oder die Eignung für eine Arbeitsstelle genutzt, kommt es zu einer starken Einschränkung der Rechte der Betroffenen. Zur Problematik vgl. Roßnagel (2016); Roßnagel & Nebel (2015), Pohle (2016).

91 von Lewinski (2014), S. 55, 59.

aus der Analyse eigentlich anonymer Falldaten der Vergangenheit, u. a. über Wohnungseinbruchdiebstähle, Informationen über Wohngebiete, die in naher Zukunft potentiell von weiteren Wohnungseinbruchdiebstählen bedroht sind. Dies soll Rückschlüsse auf die individuellen Einwohner und Passanten erlauben, ohne dass Daten über diese erhoben wurden. Hinzu kommt, dass die Predictive-Policing-Technologie auch bei der Prognose von möglichen Tätern oder Opfern von Straftaten Verwendung finden kann. Über das Datenschutzrecht hinaus ergibt sich dabei das Problem, dass der Weg hin zu präventiver Polizeiarbeit die Grenzmarken polizeilichen Handelns nach vorne zu verschieben droht. So werden statt drohender Gefahren oder begangener Straftaten Risikofaktoren problematisiert.[92]

Der Umstand, dass Datenverarbeitung heute zunehmend zum funktionalen Bestandteil in vielen Infrastrukturen geworden ist, wirft ein weiteres Problem für den Datenschutz auf.[93] Szenarien wie die „smarte Stadt", selbstfahrende Autos und effiziente Energienetze konzipieren die Datenerfassung als funktionalen Bestandteil des öffentlichen Lebens. Datenverarbeitung wird so von der zeitlich begrenzten Ausnahme zur dauerhaften Praxis. Das heißt, dass Daten nicht länger von Individuen für eingrenzbare Dienste oder Transaktionen freigegeben werden, sondern mithilfe der Geräte und Anwendungen, die die Menschen umgeben, ständig produziert und verwendet werden. In einem solchen Umfeld ist ein effektiver und nachvollziehbarer Datenschutz schwerlich umzusetzen.

Ein bislang wesentliches Instrument des Datenschutzes ist das Prinzip der informierten Einwilligung. Das Datenschutzrecht ermöglicht die Verarbeitung personenbezogener Daten insbesondere bei Vorliegen der Einwilligung der betroffenen Person. Als Einwilligung definiert Art. 4 Nr. 11 der EU-DSGVO „jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist". Die Freiwilligkeit der Einwilligung ist ein wichtiges Element für den Autonomieschutz der Nutzerinnen und Nutzer. Sind bestimmte Dienste für die Nutzerinnen und Nutzer allerdings aus gewichtigen beruflichen und persönlichen Gründen, etwa für das Handeln in der Arbeitswelt oder für die gesellschaftliche Teilhabe an Kommunikation, praktisch unverzichtbar und gibt es, wie es insbesondere in den oligopolisierten Märkten häufig der Fall ist, keine Konkurrenzangebote vergleichbarer Qualität, bleibt den Nutzerinnen und Nutzern praktisch nichts anderes übrig, als die Einwilligung zu erteilen. Die Annahme der Freiwilligkeit ihrer Abgabe ist dann eine Fiktion. Die dem Schutz der Freiwilligkeit dienende Regelung in Art. 7 Abs. 4 EU-DSGVO wirkt diesem Risiko nur zaghaft entgegen. Sie lautet: „Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, muss dem Umstand in größtmöglichem Umfang Rechnung getragen werden, ob u. a. die Erfüllung eines Vertrages, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung eines Vertrags nicht erforderlich sind."[94] Art. 7 Abs. 4 EU-DSGVO definiert nicht die Anforderungen an die Freiwilligkeit selbst, sondern bezeichnet lediglich nicht sehr präzise beschriebene Indikatoren für deren Beurteilung. Dies dürfte in Zukunft Anlass für Unsicherheit und erhebliche Kontroversen sein.

92 Zur Veränderung in der Strafverfolgung Singelnstein (2018).

93 Vgl. Roßnagel (2016), S. 8.

94 Ergänzend ist insbesondere auf Nr. 42–43 zu verweisen.

Darüber hinaus verliert das Instrument der informierten Einwilligung angesichts der systemischen Qualität von Big Data seine Wirkmöglichkeiten.[95] Die Produktion, Speicherung und Verarbeitung von Daten wird angesichts der immer weitergehenden Sammlung sämtlicher Daten aus dem Lebensumfeld des Individuums künftig immer weniger eine Frage der freiwilligen vertragsförmigen Einwilligung sein. Diese Entwicklung, sollte sie unverändert fortschreiten, bedeutet weniger das Ende der Notwendigkeit von Datenschutz als vielmehr die Erosion der Bedeutung seines bisherigen Paradigmas für die Bewältigung der vielfältigen, mit der Digitalisierung verbundenen Probleme, darunter auch der Schutz vor unbemerkter und unkontrollierter Machtausübung.

Datenschutz und Datenschutzrecht

Der Begriff Datenschutz beschreibt das Ziel, die informationelle Selbstbestimmung der Bürgerinnen und Bürger durch rechtliche, technische und organisatorische Maßnahmen zu gewährleisten. Dazu gehört u. a. der Schutz vor rechtswidriger Datenerhebung und -verarbeitung.

Das deutsche Datenschutzrecht fußt auf dem allgemeinen Persönlichkeitsrecht, das im „Grundgesetz der Bundesrepublik Deutschland“ (GG) zwar nicht ausdrücklich benannt wird, aber aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG hergeleitet wird. Dieses Grundrecht hat das Bundesverfassungsgericht (BVerfG) zunächst 1983 im Volkszählungsurteil mit dem Konzept der informationellen Selbstbestimmung weiterentwickelt. Das Recht auf informationelle Selbstbestimmung erfasst danach das Recht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen. Das BVerfG hat zudem klargestellt, dass aufgrund der Verarbeitungs- und Verknüpfungsmöglichkeiten der Informationstechnologie auch ein für sich gesehen belangloses Datum einen neuen Stellenwert bekommen kann und es insoweit keine belanglosen Daten gibt – eine Feststellung, die durch die dichte Datenverknüpfung von Big-Data-Technologien bestätigt wird. 2008 ergänzte das BVerfG den grundrechtlichen Schutz durch Anerkennung eines Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

Der europäische Gesetzgeber hatte für den datenschutzrechtlichen Bereich bislang insbesondere Richtlinien erlassen. Als Reaktion auf immer leistungsfähigere Formen der Datenverarbeitung und größere Risiken für das Recht auf informationelle Selbstbestimmung infolge weltweiter Vernetzung hat sich die EU dazu entschlossen, das europäische Datenschutzrecht grundlegend zu reformieren. Die EU-Datenschutz-Grundverordnung, die ab dem 25. Mai 2018 in den Mitgliedsstaaten gilt, soll dem Schutz vor der Erhebung und Verarbeitung personenbezogener Daten dienen. Hiermit wird das Grundrecht aus Art. 8 Abs. 1 der EU-Grundrechtecharta konkretisiert, wonach jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten hat. Die EU-Datenschutz-Grundverordnung hat das Ziel, das Datenschutzrecht EU-weit zu vereinheitlichen, wobei es die Verordnung den Mitgliedsstaaten durch Öffnungsklauseln auch ermöglicht, bestimmte Aspekte national zu regeln. Als weitere Rechtsgrundlage wurde die „Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates“ erlassen.

95 Vgl. van der Sloot (2014).

Handlungsfelder und Handlungsoptionen

▼ Handlungsfeld: Gesellschaftliche Maßnahmen

(1) *Zivilgesellschaftlich verankertes Forum.* Unter Einbeziehung von Akteuren aus den Bereichen Zivilgesellschaft, Wirtschaft, Technologie, Wissenschaft, Politik, Medien, Ethik und Bildung sollte in den jeweiligen Handlungsfeldern eine gesellschaftspolitische Vision der zukünftigen digitalen Gesellschaft entworfen werden.[96] Diese Vision soll als Zielvorstellung dienen, um eine Strategie zu entwickeln, wie sich die Lebenssituation der Bevölkerung durch den Einsatz von Big-Data-Technologien weiter verbessern, Handlungsmöglichkeiten erweitern, Chancengleichheit wahren und Autonomie stärken lassen. Eine solche digitale Strategie muss auf Einsichten und Wissen über die Treiber und Auswirkungen der Digitalisierung basieren. Um dies zu erreichen, sollten entsprechende Foren geschaffen und langfristig institutionalisiert werden.

(2) *Stärkung des gesellschaftlichen Diskurses.* Um eine gesellschaftliche Verständigung auch über ethische Standards in Big Data, den Einsatz intelligenter Systeme in den unterschiedlichsten Lebensbereichen oder über die Notwendigkeit eines wertbasierten Designs in verschiedenen Anwendungen zu fördern, bedarf es einer intensiven gesellschaftlichen Diskussion. Diese sollte durch interdisziplinäre Forschungsanstrengungen unterstützt werden, welche technologische, juristische und ethische Perspektiven einbeziehen und unterschiedliche wissenschaftsbasierte Szenarien entwickeln. Die von der Bundesregierung geplante Einsetzung einer Datenethikkommission, die als interdisziplinär besetztes und unabhängig arbeitendes Expertengremium ethische Leitlinien für das gesellschaftliche Leben im Informationszeitalter entwickeln soll, kann einen ersten Schritt in diese Richtung darstellen.

(3) *Bildungsoffensive*. Zur Förderung der digitalen Mündigkeit wird eine Bildungsoffensive empfohlen. Die sich abzeichnenden Umbrüche führen zu neuen Anforderungen in der Lebens- und Arbeitswelt jedes Einzelnen, aber auch im Hinblick auf den geforderten gesellschaftlichen Diskurs. Daher sollte Heranwachsenden wie auch Erwachsenen Wissen vermittelt und geeignete Instrumente an die Hand gegeben werden, um die Digitalkompetenz an die sich beständig weiterentwickelnden Technologien und Anwendungen anzupassen und zu erweitern. Eine solche Bildungsoffensive könnte beispielsweise über eine übergreifende Strategie für alle Schulformen und Bildungseinrichtungen erreicht werden. Dabei muss besonderes Augenmerk darauf gerichtet werden, zu verhindern, dass ungleiche Bildungsvoraussetzungen zu einem Digital Divide, d. h. einer gesellschaftlichen Spaltung in einen digital kompetenten und einen digital ungebildeten Gesellschaftsteil, führen.

(4) *Berufsethos in der IT*. Um dem zunehmenden Einsatz der Informationstechnologie in allen Lebensbereichen gerecht zu werden und mögliche Risiken von Anwendungen bereits im Forschungsstadium besser einschätzen zu können, sollten relevanten IT-Berufsgruppen ethische Perspektiven im Rahmen ihrer Ausbildung stärker vermittelt und so die Entwicklung eines Berufsethos unterstützt werden. Ein Beispiel hierfür ist das Medizinstudium, bei dem entsprechende Lehreinheiten bereits seit vielen Jahren fester Bestandteil des Curriculums sind. Auch im IT-Bereich gibt es international seit einigen Jahren Initiativen, die in diese Richtung zielen. Zu nennen sind hier z. B. die Aktivitäten des Institute of Electrical and

96 Eine wesentliche Rolle spielt hierbei auch der Verbraucherschutz; SVRV (2017).

Electronics Engineers (IEEE) und in Deutschland der Gesellschaft für Informatik.[97] Zudem sollten in Unternehmen und Forschungseinrichtungen ethische Aspekte in der Produktentwicklung und Forschung verankert werden.[98]

▼ Handlungsfeld: Transparenz und Überprüfbarkeit

(1) *Datenprovenienz*. Es gibt verschiedene Möglichkeiten, Kontrolle und Transparenz in der Datenverarbeitung zu verbessern. Zu den grundsätzlichen Möglichkeiten gehören die systematische und lückenlose Protokollierung der Herkunft von Daten (auch: Data Lineage) und die darauf aufbauende Implementierung von Geschäftslogik. Jeder Datensatz wird dabei durch Metadaten annotiert, die Aufschluss über die Datenerhebung geben (wann, durch wen, wovon abgeleitet usw.) und mögliche Einschränkungen bei der Datenverwendung spezifizieren (etwa eine maximale Speicherfrist). Durch geeignete offene Standards und Datenaustausch-Protokolle sollte dies auch system-, dienst- und anbieterübergreifend gewährleistet werden, ggf. sind hierfür Referenzarchitekturen zu entwickeln.[99] Ziel wäre es dabei, ein System aufzubauen, das es Nutzerinnen und Nutzern ermöglicht, Kontrolle darüber zu erhalten, was mit ihren Daten tatsächlich geschieht. Die so geschaffene Transparenz könnte als Grundlage für alle weiteren Schritte der Regulation der unerwünschten Weitergabe und Verarbeitung von Daten dienen. Zugleich erfordert eine solche Maßnahme aber auch die Etablierung von extrem hohen Sicherheitsstandards, um zu gewährleisten, dass diese Funktion der Rückverfolgbarkeit von Daten nicht missbraucht werden kann.

(2) *Reversibilität der Datenerfassung.* Systeme sollten so entworfen werden, dass jedes Datum, das durch einen bestimmten Kanal (mit der ihm eigenen Authentifizierung usw.) erhoben wurde, durch denselben Kanal auch wieder gelöscht werden kann. Das lässt sich etwa erreichen, indem beim Systemdesign sichergestellt wird, dass alle personenbezogenen Daten unter Verwendung einer entsprechenden User-ID zugänglich und löschbar sind. Ob und wie sich ein solches System auch auf Sekundärdaten erweitern lässt, die durch eine Verknüpfung mit den ursprünglichen Daten entstanden sind und zu deren weiterer Verbreitung beitragen, ist eine Frage, die noch intensiver Forschungstätigkeit bedarf.

(3) *Vorhersagbarkeit von Datenschutzrisiken.* Eine Verstärkung der wissenschaftlichen Forschung ist ebenfalls wünschenswert, um Metriken und Technologien zu entwickeln, die das Risiko für die Privatsphäre beim Zusammenführen von Daten vorab bemessen können. Sinnvoll sind Datenmodelle, die das Zusammenspiel von verschiedenen Arten des Datenschutzrisikos und der technischen Durchsetzung des Schutzes abbilden können. Hier kann u. a. Maschinelles Lernen vielversprechende Ansätze bieten.

▼ Handlungsfeld: Ausweitung zentraler Prinzipien des Datenschutzrechts

Bei der Verarbeitung von Big Data ist die Einhaltung der datenschutzrechtlichen Prinzipien, insbesondere der Datensparsamkeit und Zweckbindung, gefährdet. Hier werden nämlich typischerweise große Mengen von Daten verwendet, diese dabei aus ihren ursprünglichen Kontexten gelöst und für unterschiedliche Zwecke eingesetzt. Würden dieselben Anforderungen, wie sie zum Schutz personenbezogener Daten gelten, ohne Weiteres auf den

97 IEEE Standards Association (2016), GI (2018).

98 Beispielhaft kann hierfür auf das Statement der Association for Computing Machinery zur Bedeutung der Wahrung von Privatheit verwiesen werden, ACM US Public Policy Council (2018).

99 Bei Referenzarchitekturen handelt es sich um auf der Basis von Best Practice erstellte standardisierte Lösungsvorschläge für IT-Infrastrukturen.

Einsatz im Bereich der Big-Data-Analytik angewandt, bestände andererseits das Risiko, diese Analytik und die Verwendung ihrer Ergebnisse zu erschweren oder unmöglich zu machen. Daher muss an Konzepten zur Verwirklichung des Ziels gearbeitet werden, die Grundanliegen der herkömmlichen Prinzipien des Datenschutzrechts auch im Bereich von Big Data erfüllen zu können, ohne die mit Big-Data-Analytik verbundenen Chancen über Gebühr einzuschränken. Solche Konzepte könnten unter Nutzung der in der EU-DSGVO bereits angelegten Schutzvorkehrungen auf die Architekturen der Datenverarbeitungssysteme bezogen sein (Wo werden von wem Daten erhoben, gespeichert und verarbeitet?), die Datenverarbeitungsverfahren (Welche Daten werden erhoben, wie anonymisiert und pseudonymisiert, welche Daten dürfen nicht erhoben werden?) und ebenso die zulässigen Zwecksetzungen betreffen (Wissenschaft im Allgemeininteresse, Verbesserung von Dienstleistungen, verbesserte personenbezogene Werbung u. a.). Dabei wäre ferner vorzusehen, dass bestimmte, vom Gesetzgeber als grundrechtssensibel bewertete Daten im Zuge von Big-Data-Analytik nur genutzt werden dürfen, wenn vor ihrer Verwendung oder Weitergabe Markierungen und Zweckbindungen erfolgen und Löschungs- oder Sperrfristen vorgesehen werden, damit die Einhaltung der Prinzipien überprüft und gesichert werden kann. Deren Umsetzung dürfte aber schwierig sein und bedarf möglicherweise noch weiterer Ansätze. Insofern könnte der Gesetzgeber Anstöße zur Entwicklung geeigneter Methoden zur Sicherung von Zweckbindungen mithilfe rechtlicher Vorkehrungen geben.[100] Für die Weitergabe und -verwertung der Daten können weiterhin Dokumentationspflichten vorgesehen werden.

(1) *Vielfalt der Prinzipien.* An den folgenden datenschutzrechtlichen Prinzipien, die in Art. 5 EU-DSGVO normiert sind, sollte festgehalten werden: Rechtmäßigkeit, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung sowie Integrität und Vertraulichkeit.

(2) *Datensparsamkeit*. Jede Datensammlung und jedweder Datenaustausch sollten insbesondere sparsam sein, d. h. minimal in Bezug auf den bei der Datenerhebung, aber auch den bei der Datenverwertung jeweils verfolgten Zweck. Dies gilt neben dem Umfang auch für die Genauigkeit der Daten.[101] Diese sollte standardmäßig (per default) gering gehalten werden, anstatt, wie es heute häufig geschieht, Daten wie Zeitstempel, Ortsdaten, URLs oder Gerätekennungen hypergenau zu protokollieren. Abweichungen vom Sparsamkeitsprinzip bedürfen einer Rechtfertigung anhand des Erhebungszwecks. Die o. g. Architekturprinzipien können zu einer transparenteren Umsetzung beitragen.

(3) *Zweckbindung.* Um Prinzipien der Zweckbindung und der Datenminimierung zu beachten, kann es sinnvoll sein, für bestimmte Kategorien von Daten – auch im Hinblick auf Big-Data-Anwendungen – Markierungen bei deren Erhebung sowie Regelungen zu Zweckbindungen, Löschungs- oder Sperrfristen für deren Weiterverarbeitung verpflichtend vorzusehen. Auch sollten verstärkte Anstrengungen unternommen werden, um technische Lösungen für eine Reduzierung der Personenbeziehbarkeit der Daten zu entwickeln und zu implementieren. Angesichts der innovativen Möglichkeiten, die mit der weiteren Entwicklung der Digitalisierung verbunden sind, ist es eine lohnende Aufgabe, neuartige Möglichkeiten

100 Vorstellbar wären hier Maßnahmen wie z. B. das „Innovation Forcing“ oder „best available technology“-Vorgaben. Unter Innovation Forcing versteht man eine Technik, durch die regulativ Vorgaben gesetzt werden, die nach dem gegenwärtigen Stand der Technik noch nicht erreicht werden, aber als erreichbar erscheinen. Hoffmann-Riem (2016a), S. 430–432. Dabei hängt die Sinnhaftigkeit dieser Maßnahme davon ab, wie präzise der Staat Kosten, Nutzen, technische Effektivität etc. beurteilen kann, Gawel (2009), S. 231f.

101 So sind etwa Ortsdaten, die nur bis auf 100–200 Meter genau sind, in der Regel deutlich weniger problematisch als solche, die eine Genauigkeit von 5–10 Metern aufweisen. Für viele Anwendungen mag aber eine geringere Genauigkeit ausreichen.

zu entwickeln, ggf. unterstützt durch hoheitliche Vorgaben: Gelingt es den Big-Data-Verwendern nicht, die rechtlich erwarteten innovativen Lösungen zu entwickeln, müssen sie von den betroffenen Big-Data-Nutzungen absehen.

(4) *Prinzip der Datensparsamkeit technisch durch strikt lokale Datenzusammenführungen umsetzen*. Mit einer nur lokalen Zusammenführung von Daten lassen sich die meisten der gewünschten Anwendungen und Funktionen durchführen, die Daten stehen jedoch nicht mehr für spätere Auswertungen zur Verfügung.

(5) *Unbeabsichtigte Identifizierbarkeit*. Selbst wenn der Dienstleister alle Vorkehrungen zur Datenminimierung getroffen hat, kann es dennoch zu ungewollten Identifizierungen von Nutzerinnen und Nutzern kommen: etwa indem diese ohne die Folgen zu überblicken, identifizierende Daten preisgeben, z. B. über mehrere Plattformen hinweg denselben Benutzernamen verwenden, Daten wie Telefon-, Kreditkartennummern oder sogar ihr Passwort versehentlich preisgeben. Anbieter könnten hier technische Vorkehrungen treffen, die das Erheben unnötiger Daten mit speziellen Filterverfahren so weit wie möglich verhindern und Nutzerinnen und Nutzer auf die Gefahr der Verwendung verknüpfbarer Identifikatoren hinweisen.

(6) *Stärkung der Nutzerinnen und Nutzer bei Einwilligungsregeln.* Es empfiehlt sich, für die Vorgaben der Anbieter in Bezug auf die Einwilligung in die Datenverarbeitung, insbesondere für entsprechende Allgemeine Geschäftsbedingungen, verpflichtend eine Zertifizierung durch öffentlich anerkannte, akkreditierte Stellen vorzusehen und Verbraucherschutzverbände in das Zertifizierungsverfahren einzubeziehen. Es ist im Übrigen darauf hinzuwirken, dass die rechtlichen Vorgaben als Verbot der Koppelung der Bereitstellung der Dienste an eine Einwilligung in die Verarbeitung solcher Daten verstanden werden, die keinen inhaltlichen Bezug zu den nachgefragten Diensten haben.[102] Sollte sich eine solche Interpretation nicht durchsetzen, bedürfte es einer Novellierung der EU-DSGVO.

▼ Handlungsfeld: Datenhoheit

(1) *Monetarisierung von Diensten und Daten.* Den Nutzerinnen und Nutzern sollten auch andere Möglichkeiten zur Eröffnung des Zugangs zu Diensten angeboten werden als die Einwilligung in die Verarbeitung personenbezogener Daten. Die Rechtsordnung sollte eine Pflicht der Anbieter enthalten, Alternativen für die Einwilligung in die Datenverarbeitung bereitzustellen. Eine solche Alternative wäre ein Recht der Nutzerinnen und Nutzer, den Zugriff auf die Dienste gegen ein finanzielles, im Ausmaß faires Entgelt zu erhalten. Die Fairness des Preises müsste allerdings einer öffentlichen Kontrolle unterworfen werden. Rechtspolitisch wäre es sogar vertretbar, die Anbieter zu verpflichten, den Nutzerinnen und Nutzern ein faires Entgelt zu zahlen, wenn sie in die Erhebung und Verwertung besonders wertvoller Daten einwilligen. Zwar haben nicht alle Daten einen hohen wirtschaftlichen Wert. Wie aber die erheblichen Gewinnmargen vieler IT-Unternehmen, die sich über die Datenverwertung (mit)finanzieren, zeigen, kann der Zugriff auf die Daten in wirtschaftlicher Hinsicht sehr lukrativ sein und ist es vielfach auch. Sind solche Datenverarbeitungen betroffen, wären verbindliche Regelungen dahingehend sinnvoll, dass Verarbeitungen nur gegen eine Zahlung an diejenigen zulässig sind, deren Daten von den Unternehmen geschäftlich verwendet werden.

102 Einen gewissen Anknüpfungspunkt dafür bietet EU-DSGVO Erwägungsgrund 42, Satz 5: „Es sollte nur dann davon ausgegangen werden, dass sie ihre Einwilligung freiwillig gegeben hat, wenn sie eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden."

(2) *Programmgesteuerte Schnittstellen* (Application programming interfaces, APIs) zwischen Komponenten und Teilsystemen der Datenverarbeitung sind heute im automatisierten Datenaustausch üblich. Dieselben Schnittstellen eröffnen die Möglichkeit einer direkten Datenverwaltung durch die Nutzerinnen und Nutzer, quasi in einem Fernsteuermodus, wobei die Daten faktisch auf Systemen des Dienstleisters vorgehalten und verarbeitet werden. Sofern Unternehmen für die von ihnen gesammelten Daten gewisse Grundfunktionen der Datenverarbeitung wie Löschung, Verschlüsselung, Modifikation oder Verrauschung über APIs anwendergebunden bereitstellen, können Benutzerinnen und Benutzer weiterhin Kontrolle über die Daten ausüben. Anbieter sollten verpflichtet werden, ihren Nutzerinnen und Nutzern standardisierte programmgesteuerte Schnittstellen zur nachhaltigen Verwaltung ihrer persönlichen Daten anzubieten.[103] Eine solche Standardisierung der Schnittstellen würde es Drittanbietern zudem erlauben, unabhängige Softwaremodule zu entwickeln, welche im Auftrag des Nutzers Daten-Policies – und zwar anbieterübergreifend – umsetzen können.

Die Herausforderungen sind dabei nicht trivial. Zur Lösung ist es erforderlich, (a) einen geeigneten Rechtsrahmen zu schaffen, der Eigentums- und Nutzungsrechte an Daten regelt (Datennutzung auf Widerruf), und (b) Anreize zu schaffen oder rechtliche Pflichten vorzusehen, so dass eine entsprechende Funktionalität über APIs verfügbar gemacht wird. Zudem muss (c) eine serverseitige Umsetzung durch geeignetes Auditing unterstützt werden.[104] Als weiterer Vorteil eröffnet sich der allgemeinen Öffentlichkeit die Möglichkeit, verstärkt Druck auf Unternehmen ausüben zu können, indem etwa ein Großteil der Nutzerinnen und Nutzer mit einem Widerruf (Löschung, Migration) der eigenen Daten droht.

(3) *Nutzerseitige Datenspeicherung*. Eine Alternative besteht darin, Daten nutzerseitig (z. B. auf dem Smartphone) zu speichern. Die nutzerseitige Speicherung von Daten ist technisch realisierbar und erprobt, hat sich jedoch angesichts der gegenläufigen Interessen der Anbieter kaum durchgesetzt, obwohl man so in vielen Fällen eine zentrale Erhebung von Daten vermeiden könnte. Bei nutzerseitiger Speicherung würden Dienstleister beispielsweise über programmgesteuerte Schnittstellen (z. B. via HTTPS) auf Daten zugreifen, ohne dass sie diese dauerhaft speichern oder verknüpfen müssen. Der Nutzer kann die Verwendung der Daten also dauerhaft kontrollieren und von Fall zu Fall über eine Zustimmung entscheiden. Durch Kontroll- und Auditing-Prozesse kann die Einhaltung des Verbots einer persistenten zentralen Speicherung sichergestellt werden.

(4) *Werkzeuge für Selbstdatenschutz*. Zusätzlich zu betreiberseitigen Maßnahmen des Datenschutzes und der Informationssicherheit müssen Nutzerinnen und Nutzern Werkzeuge zum selbstbestimmten Schutz ihrer Daten an die Hand gegeben werden. Für Individuen ist es zunehmend unüberschaubar, welche Daten offen und verdeckt über sie erhoben und ggf. zu Profilen zusammengeführt werden. Für die informierte Entscheidung des Individuums über die Preisgabe von Informationen, die Grundvoraussetzung der selbstbestimmten Teilnahme an der Digitalisierung, ist es deshalb erforderlich, Werkzeuge zu entwickeln, die Nutzerinnen und Nutzern zum einen Information und zum zweiten eigene Kontrolle ermöglichen. Ein Beispiel eines solchen Werkzeugs wäre eine App, die den Nutzer bei seiner Entscheidung, ob und mit wem er z. B. ein bestimmtes Bild oder eine Standortinformation in einem sozialen Netzwerk teilt, unterstützt, indem zuvor mögliche Szenarien der Ver-

103 Hierzu siehe auch Hofmann & Schölkopf (2015).

104 Für weitere Details siehe Hofmann & Schölkopf (2015).

knüpfbarkeit und Weiterverbreitung dieser neuen Information aufgrund anderer bereits veröffentlichter Informationen lokal errechnet werden. In diesem Bereich des technischen Selbstdatenschutzes müssen die wissenschaftlichen Bemühungen verstärkt werden, um handhabbare Werkzeuge zu entwickeln.

▼ Handlungsfeld: Kontrolle über Algorithmen

(1) *Audit-Verfahren für Algorithmen*. Es bedarf neuer Mechanismen, die eine Kontrolle der Funktionsprinzipien und Entscheidungskriterien von Algorithmen ermöglichen, sofern deren Einsatz Rechtsgüter beeinträchtigen kann. In Betracht zu ziehen sind Vorkehrungen zur Zertifizierung, ergänzt um Verfahren der Auditierung und des Monitorings. Vor allem, wenn aufgrund der Anwendung von (prädiktiven) Big-Data-Analysen Chancen für Betroffene vereitelt werden, etwa im Zuge des Profiling oder Scoring, sind Transparenz und Kontrolle der zugrunde gelegten Algorithmen von besonderer Bedeutung.

(2) *Dokumentation des Einsatzes von Big Data.* Wirken Anwendungen auf besondere Weise auf die Grundrechte des Einzelnen ein, z. B. bei der Berechnung von Versicherungstarifen oder der Kreditgewährung, wird empfohlen, diese zu dokumentieren. Neue Verfahren des Maschinellen Lernens (sog. Interpretierbare Verfahren) erlauben es neuerdings, den gemeinhin angenommenen Blackbox-Charakter nichtlinearer Lernmethoden zu überwinden;[105] dies ermöglicht eine effektive Überprüfung durch ein faktisches Reverse Engineering der typischen heutzutage eingesetzten Lernmethoden (beispielsweise tiefer neuronaler Netze und Kernmethoden). Die technischen Möglichkeiten zu einer solchen Überprüfung sind bereits vorhanden und ihr Einsatz könnte rechtlich geregelt werden. Zur Überprüfung von Algorithmen, die als Geschäftsgeheimnis eingestuft werden, ist es z. B. denkbar, Verfahren zu etablieren, die an die Praxis sog. In-Camera-Verfahren vor Gericht (siehe auch Kap. 3, Transparenzdefizite) angelehnt werden.

▼ Handlungsfeld: Anonymisierbarkeit

Ein alternativer Ansatz, um Big-Data-Anwendungen über technische Optionen mit stärkerem Schutz der Privatsphäre zu verbinden, ist die Reduzierung des Personenbezugs der Daten. Die stärkste Form dieser Reduzierung ist die vollständige Anonymisierung von Daten, die einen Bezug von Daten auf ein einzelnes Individuum weitgehend ausschließt. (► Box „Anonymisierungsverfahren“) Die zunehmende Menge, Verfügbarkeit und Verknüpfung von Daten machen tatsächliche Anonymisierung jedoch zunehmend schwieriger, wie zahlreiche Beispiele der erfolgreichen Re-Identifizierung vermeintlich anonymisierter Datensätze in der jüngeren Vergangenheit bewiesen haben. Selbst nach erfolgter Anonymisierung existieren vielfältige Szenarien, in welchen eine Re-Identifizierung des Individuums möglich wäre. So kann es, insbesondere durch Verknüpfung mit z. B. öffentlich verfügbaren Datenquellen, passieren, dass Nutzerinnen und Nutzer durch ihre Daten eindeutig charakterisierbar sind. Kann zusätzlich eine Verbindung zu einem direkten Identifikator hergestellt werden (Name, Adresse, Telefonnummer, Kreditkartenummer, Gesicht usw.), dann ist eine Person in einem vermeintlich anonymisierten Datensatz namentlich identifizierbar.[106] Bereits wenn ein Individuum aus einem Datenpool herausgesondert werden

105 Bach et al. (2015); Montavon, Samek, & Müller (2018).

106 Das bekannteste einer Vielzahl wissenschaftlicher und journalistischer Re-Identifizierungsergebnisse stammt aus einer Studie von L. Sweeney, in welcher es den Forschern gelang, 87 Prozent der US-Bürger anhand der Daten Postleitzahl, Geburtsdatum und Geschlecht in den vermeintlich anonymisierten Zensusdaten eindeutig zu identifizieren, Sweeney (2000).

kann, gilt die Anonymität als aufgehoben (Singling Out), auch wenn auf diese Weise noch nicht der Name des Betroffenen kenntlich sein muss.

Darüber hinaus stellt sich die Frage, wie in Anbetracht der stetig wachsenden Menge an verfügbaren und somit verknüpfbaren Daten sowie der zunehmenden technischen Möglichkeiten eine dauerhafte Anonymität gewährleistet werden kann. Dabei ist andererseits zu bedenken, dass Datenverknüpfung und die daraus resultierende Datenbreite oft ein wesentlicher Erfolgsfaktor für den Einsatz von Maschinellem Lernen und Big-Data-Verfahren ist. Setzt man dennoch auf Anonymisierung, um einen höheren Grad des Datenschutzes zu erreichen, ist es notwendig, durch verstärkte Grundlagenforschung und technischen Fortschritt bestehende Konzepte weiterzuentwickeln.

(1) *Verfahren entwickeln, die Anonymitätsgarantien ermöglichen*. Es gibt bereits verschiedene technische Verfahren, die Datenbankabfragen ermöglichen, ohne Rückschlüsse auf einzelne Personen zuzulassen. Entsprechende Datenschutzkonzepte sind z. B. k-anonymity[107], l-diversity[108], t-closeness[109] und das aktuell vorherrschende Konzept der Differential Privacy[110]. In der Praxis greifen diese Konzepte aber oft nicht vollumfänglich, z. B. dann, wenn Daten dynamisch erhoben oder verändert werden. Für Big Data müssen daher neue, weiterentwickelte Konzepte geschaffen werden, die vergleichbare Garantien für hochdynamische und multidimensionale Datenbestände geben können. Daher wird empfohlen, die Forschung in diesem Bereich weiter voranzutreiben, um zu einem besseren Verständnis der Dynamiken in solchen Datenbeständen zu gelangen. Ziel ist es, Technologien zu entwickeln, die das Risiko für die Privatsphäre beim Zusammenführen oder Streaming von Daten vorab erkennen und abwenden können.

(2) *Nicht persistente Datenverknüpfungen*. Eine vergleichsweise wenig aufwendige Erschwerung von Deanonymisierung besteht im Einsatz nicht dauerhafter Datenverknüpfungen, die Daten nur gleichsam „im Vorübergehen“ (z. B. in einem temporären Hauptspeicher) zusammenführen, etwa als Input zu einem Lern- oder Analysealgorithmus. So lassen sich viele statistische Regularitäten erkennen, ohne dass eine zentrale Datenbank angelegt werden müsste, welche die Anonymität des Einzelnen aufheben würde.

(3) *Anonyme Berechtigungsnachweise.* Möglichkeiten von Nutzerinnen und Nutzern, mit verschiedenen Pseudonymen bzw. virtuellen Identitäten für verschiedene Lebensbereiche zu agieren, sollten regulatorisch nicht eingeschränkt, sondern unterstützt werden. Anbieter von Services sollten dazu angehalten werden, wenn möglich auf eine Identifizierung von Nutzerinnen und Nutzern zu verzichten und anonyme Berechtigungsnachweise zu akzeptieren. Ein Beispiel hierfür ist die Funktion des neuen Personalausweises, die Volljährigkeit eines Nutzers digital zu bestätigen.

107 Sweeney (2002).
108 Machanavajjhala, Kifer, Gehrke, & Venkitasubramaniam (2007).
109 Li, Li, & Venkatasubramanian (2007).
110 Dwork (2006).

Anonymisierungsverfahren

Die Nutzung von nicht personenbezogenen Daten unterliegt in der Regel keinen rechtlichen Restriktionen. Ein Weg für die Wissenschaft und die Unternehmen, die für Forschungs- und Entwicklungszwecke auf Daten zugreifen wollen, wird darin gesehen, sicherzustellen, dass sich auf der Grundlage der verwendeten Daten keine Rückschlüsse auf einzelne, identifizierbare Personen ziehen lassen. Da im Zeitalter von Big Data einzelne Datensätze nicht mehr per se als anonymisiert angesehen werden können, weil durch die Verknüpfung mit anderen Datensätzen ein Personenbezug wieder möglich werden kann, müssen neuere Verfahren der Anonymisierung mit Blick auf Big Data eingesetzt und weiterentwickelt werden. Die Entwicklung von Anonymisierungsverfahren ist in den vergangenen 16 Jahren signifikant vorangeschritten. Man kann zwischen Verfahren zur Aggregation und zum Verrauschen von Daten unterscheiden:

k-anonymity

Das 2002 vorgestellte Modell der k-anonymity[111] soll die Verknüpfung eines sensiblen Attributs zu einem einzelnen Individuum erschweren, da durch Aggregation immer mindestens eine Anzahl von k Individuen dasselbe sensible Attribut teilt. Ein Set an Daten bietet dann k-Anonymität, wenn die identifizierenden Informationen (Identifier) jedes einzelnen Individuums in dem Datenset von mindestens k-1 anderen Individuen ununterscheidbar sind. Ein Beispiel für eine solche Aggregation wäre eine Patientenstatistik, die nicht konkrete Geburtsdaten ausweist, sondern nur Altersspannen von ausreichender Größe. Je größer k ist, desto größer ist die Menge, innerhalb derer das Individuum ununterscheidbar ist, und umso größer ist dementsprechend seine Anonymität (k = 2 bedeutet, dass 2 Individuen im Hinblick auf ihre Attribute ununterscheidbar sind usw.). Eine Statistik ist auch dann k-anonym, wenn in einer Notarztstatistik alle männlichen Patienten zwischen 55–65 Jahren wegen eines Myokardinfarkts behandelt wurden. k-anonymity lässt allerdings zu, dass alle Mitglieder einer k-anonymen Gruppe dasselbe sensible Attribut teilen und man insofern auch eindeutige Aussagen über jedes einzelne Individuum der k-anonymen Gruppe treffen kann.

l-diversity und t-closeness

Um diesen konzeptuellen Mangel von k-anonymity auszugleichen, wurden 2007 die ergänzenden Konzepte von l-diversity[112] und t-closeness[113] entwickelt. l-diversity garantiert ein Maß an Verschiedenheit der sensiblen Attribute innerhalb einer k-anonymen Gruppe. t-closeness erweitert das k-anonymity-Modell um einen Parameter, der die Verteilung der sensiblen Attribute in den einzelnen Äquivalenzklassen mit der Verteilung in der gesamten Tabelle harmonisiert. Beide Konzepte gelten jedoch heutzutage als unzureichend für den Einsatz für Big Data, da sie eine Deanonymisierung unter Hinzuziehung von Kontextinformation nicht ausschließen.

Differential Privacy

Das 2006 von Dwork vorgestellte Konzept der Differential Privacy[114] erlaubt ebenfalls die Anonymisierung von Datenbeständen sowie anonymisierte Datenbankabfragen. In letzterem Fall behält der Verantwortliche die originalen Daten und erlaubt Dritten statistische Anfragen auf

111 Sweeney (2002).
112 Machanavajjhala, Kifer, Gehrke, & Venkitasubramaniam (2007).
113 Li, Li, & Venkatasubramanian (2007).
114 Dwork (2006).

diesen Datenbestand. Die Ergebnisse der Abfragen werden durch hinzugefügte Daten so weit „verrauscht", dass sie in der Menge zwar noch eine korrekte statistische Aussage ermöglichen, das Aussondern (Singling Out) von einzelnen Individuen jedoch verhindern. Differential Privacy wird z. B. von der Firma Apple eingesetzt, um das Nutzungsverhalten von I-Phone-Besitzern auszuwerten (z. B. häufig benutzte Funktionen und Emojis). Auch im Bereich der Anonymisierung von medizinischen Forschungsdaten ist der Einsatz von Differential Privacy vielversprechend.[115]

115 Backes, Berrang, Humbert, & Manoharan (2016).

5 Fazit

Zusammenfassend zeigen die vielen Handlungsoptionen, dass es möglich ist, den Herausforderungen der Digitalisierung für die Privatheit des Einzelnen und damit auch für die freie, demokratische Gesellschaft zu begegnen. Sie eröffnen einen Raum von Möglichkeiten, der zur Verfügung steht, um positiv in die Gestaltung unserer digitalen Zukunft einzugreifen, um das Recht des Einzelnen zu schützen und zu stärken und den sich abzeichnenden nachteiligen gesellschaftlichen Auswirkungen entgegenzuwirken. Da durch die Anwendung von Big Data unterschiedliche und z. T. gegenläufige Interessen betroffen sind und es erhebliche Machtasymmetrien gibt, bedarf es wirksamer rechtlicher Regelungen, die einerseits Innovationsspielräume offen halten, andererseits aber auch angemessenen Schutz für die Rechte und Interessen aller Betroffenen gewährleisten. Die Nutzung dieser Möglichkeiten ist eine Herausforderung, die auch, aber nicht allein im nationalen oder im EU-Raum, sondern weltweit zu bewältigen ist und trans- und internationaler Kooperation bedarf. Es reicht nicht, an den guten Willen derjenigen zu appellieren, die Big Data auswerten und anwenden.

6 Literatur

Abel, R. B. (2003). Umsetzung der Selbstregulierung im Datenschutz: Probleme und Lösungen. *Recht der Datenverarbeitung – RDV*, 11–13.

acatech (Hrsg.). (2013). *Privatheit im Internet. Chancen wahrnehmen, Risiken einschätzen, Vertrauen gestalten*. Berlin: Springer Vieweg.

ACM US Public Policy Council. (2018). *USACM Statement on the importance of preserving personal privacy*. Washington DC. Abgerufen am 16. August 2018 von https://www.acm.org/binaries/content/assets/public-policy/2018_usacm_statement_preservingpersonal-privacy.pdf

Autor, D., Dorn, D., Katz, L., Patterson, C., & Van Reenen, J. (2017). *The Fall of the Labor Share and the Rise of Superstar Firms* (No. w23396). Cambridge, MA: National Bureau of Economic Research. https://economics.mit.edu/files/12979

Bach, S., Binder, A., Montavon, G., Klauschen, F., Müller, K.-R., & Samek, W. (2015). On Pixel-Wise Explanations for Non-Linear Classifier Decisions by Layer-Wise Relevance Propagation. *PLOS ONE*, *10*(7), e0130140. https://doi.org/10.1371/journal.pone.0130140

Backes, M., Berrang, P., Humbert, M., & Manoharan, P. (2016). Membership Privacy in MicroRNA-based Studies. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (S. 319–330). Vienna, Austria: ACM.

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday*, *11*(9). Abgerufen am 16. August 2018 von http://firstmonday.org/ojs/index.php/fm/article/view/1394

Becker, C., & Seubert, S. (2016). Privatheit, kommunikative Freiheit und Demokratie. *Datenschutz und Datensicherheit – DuD*, *40*(2), 73–78. https://doi.org/10.1007/s11623-016-0549-2

BGH. (2014). *Bundesgerichtshof entscheidet über Umfang einer von der SCHUFA zu erteilenden Auskunft* (No. VI ZR 156/13). Abgerufen am 16. August 2018 von http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&Datum=Aktuell&nr=66583&linked=pm

Bizer, J. (2001). Selbstregulierung des Datenschutzes. *Datenschutz und Datensicherheit*, *25*(3).

BMBF. (2015). *Multisensoriell gestützte Erfassung von Straftätern in Menschenmengen bei komplexen Einsatzlagen (Muskat)*. Abgerufen am 10. Oktober 2017 von https://www.sifo.de/files/Projektumriss_Muskat.pdf

BMBF. (2016). *Empfehlungen zum Management von Forschungsdaten – BMBF*. Abgerufen am 17. Juli 2018 von https://www.bmbf.de/de/empfehlungen-zum-management-von-forschungsdaten-3036.html

Bundesnetzagentur. (17. Februar 2017). *Bundesnetzagentur zieht Kinderpuppe „Cayla" aus dem Verkehr*. Abgerufen am 10. Oktober 2017 von https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2017/14012017_cayla.html

Bundesnetzagentur. (2018). Bundesnetzagentur – Missbrauch von Sendeanlagen – Hinweise zu einzelnen Produktkategorien. Abgerufen am 17. Juli 2018 von https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/Datenschutz/MissbrauchSendeanlagen/HinweiseProduktkategorien/hinweiseproduktkategorien.html?nn=690686

Bundespolizei. (2017). *Test zur Gesichtserkennung am Bahnhof Berlin Südkreuz gestartet*. Abgerufen am 8. Januar 2018 von https://www.bundespolizei.de/Web/DE/04Aktuelles/01Meldungen/2017/08/170810_start_videotechnik.html

Bundestag. (2018). *Bundesdatenschutzgesetz vom 30. Juni 2017 (BGBl. I S. 2097)*. Abgerufen am 16. August 2018 von https://www.gesetze-im-internet.de/bdsg_2018/BDSG.pdf

BVerfG. (1983). *BVerfGE 65, 1 – Volkszählung*.

BVerfG. (2008a). *BVerfGE 120, 274 – Online-Durchsuchungen*.

BVerfG. (2008b). *Urteil des Ersten Senats vom 27. Februar 2008 – Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit eigener informationstechnischer Systeme* (No. 1 BvR 370/07-Rn. (1-333)). Abgerufen am 16. August 2018 von http://www.bverfg.de/e/rs20080227_1bvr037007.html

BVerfG. (2016). *141, 220 – BKA-Gesetz*.

Camera dei deputati. (2015). *Commissione per i diritti e i doveri relativi a Internet*. Abgerufen am 17. Januar 2018 von http://www.camera.it/leg17/1179

Christl, W. (2014). *Studie: Kommerzielle digitale Überwachung im Alltag – Studie_Digitale_Ueberwachung* (Studie im Auftrag der Bundesarbeitskammer). Wien: Cracked Labs. Abgerufen am 16. August 2018 von http://crackedlabs.org/dl/Studie_Digitale_Ueberwachung.pdf

Clement, R., & Schreiber, D. (2016). *Internet-Ökonomie: Grundlagen und Fallbeispiele der vernetzten Wirtschaft* (3. Auflage). Berlin, Heidelberg: Springer Gabler.

Cornils, M. (2017). Entterritorialisierung im Kommunikationsrecht. In M. Jestaedt (Hrsg.), *Grenzüberschreitungen: Berichte und Diskussionen auf der Tagung der Vereinigung der Deutschen Staatsrechtslehrer in Linz vom 5.–8. Oktober 2016*. Berlin: De Gruyter.

Cowgill, B., & Tucker, C. (2017). *Algorithmic Bias: A Counterfactual Perspective*. Abgerufen am 16. August 2018 von http://trustworthy-algorithms.org/whitepapers/Bo%20Cowgill.pdf

DELL EMC. (2014). *The EMC Privacy Index*. Abgerufen am 16. August 2018 von https://www.emc.com/collateral/brochure/privacy-index-global-in-depth-results.pdf

Der Bundesrat. (2016). *Bundesrat will Markteintrittshürden für Fintech-Unternehmen verringern*. Abgerufen am 8. Januar 2018 von https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-64356.html

DLR. (18. Mai 2017). *Mischverkehr an Kreuzungen intelligent vernetzen*. Abgerufen am 10. Oktober 2017 von http://www.dlr.de/dlr/presse/desktopdefault.aspx/tabid-10172/213_read-22488/

Drexl, J. (2016). Regulierung der Cyberwelt – Aus dem Blickwinkel des internationalen Wirtschaftsrechts. In Deutsche Gesellschaft für Internationales Recht (Hrsg.), *Freiheit und Regulierung in der Cyberwelt – Rechtsidentifikation zwischen Quelle und Gericht* (S. 95–158). Heidelberg: C.F. Müller Verlag.

Dwork, C. (2006). Differential Privacy. In M. Bugliesi, B. Preneel, V. Sassone, & I. Wegener (Hrsg.), *Automata, Languages and Programming. ICALP 2006. Lecture Notes in Computer Science* (Bd. 4052). Berlin, Heidelberg: Springer.

EC. (2014). *Case M.7217 – Facebook/WhatsApp Commission decision pursuant to Article 6(1)(b) of Council Regulation No 139/2004*. Brüssel. Abgerufen am 17. August 2018 von http://ec.europa.eu/competition/mergers/cases/decisions/m7217_20141003_20310_3962132_EN.pdf

EC. (2016a). *Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates* (Amtsblatt der Europäischen Union) (S. 89 ff.). Brüssel.

EC. (2016b). *Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Änderung der Richtlinie 2010/13/EU zur Koordinierung bestimmter Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Bereitstellung audiovisueller Mediendienste im Hinblick auf sich verändernde Marktgegebenheiten*. Brüssel: Europäische Kommission. Abgerufen am 17. August 2018 von http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52016PC0287&from=DE

EC. (2018). European Open Science Cloud (EOSC) | Open Science – Research and Innovation – European Commission. Abgerufen am 17. Juli 2018 von https://ec.europa.eu/research/openscience/index.cfm?pg=open-science-cloud

EFI. (2015). *EFI-Gutachten 2015* (Gutachten). Berlin. Abgerufen am 17. August 2018 von http://www.e-fi.de/fileadmin/Gutachten_2015/EFI_Gutachten_2015.pdf

EFI. (2016). *EFI-Gutachten 2016* (Gutachten). Berlin. Abgerufen am 17. August 2018 von https://www.bmbf.de/files/EFI_Gutachten_2016.pdf

EFI. (2017). *EFI-Gutachten 2017* (Gutachten). Berlin. Abgerufen am 17. August 2018 von http://www.e-fi.de/fileadmin/Gutachten_2017/EFI_Gutachten_2017.pdf

Eikenberg, R. (2013). Vaillant-Heizungen mit Sicherheits-Leck. *heise online*. Abgerufen am 17. August 2018 von https://www.heise.de/security/meldung/Vaillant-Heizungen-mit-Sicherheits-Leck-1840919.html

Europarl. *Entschließung des Europäischen Parlaments vom 27. November 2014 zur Stärkung der Verbraucherrechte im digitalen Binnenmarkt* (2014/2973(RSP)), P8_TA (2014)00 71 § (2014).

Europarl & European Council. (2016a). *Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates* (Richtlinie). Brüssel. Abgerufen am 17. August 2018 von https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016L0680&from=DE

Europarl & European Council. (2016b). *Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union* (Richtlinie). Brüssel.

FCA. (2015). *Regulatory sandbox*. London. Abgerufen am 17. August 2018 von https://www.fca.org.uk/publication/research/regulatory-sandbox.pdf

Fischer-Lescano, A. (2014). Der Kampf um die Internetverfassung. Rechtsfragen des Schutzes globaler Kommunikationsstrukturen vor Überwachungsmaßnahmen. *JuristenZeitung*, *69*(20), 965–974. https://doi.org/10.1628/002268814X14095838632983

Floridi, L. (2015). *Die 4. Revolution: wie die Infosphäre unser Leben verändert* (A. Walter, Übers., 1. Auflage). Berlin: Suhrkamp.

Gawel, E. (2009). Technologieförderung durch Stand der Technik: Bilanz und Perspektiven. In W. Hoffmann-Riem & M. Eifert (Hrsg.), *Innovationsfördernde Regulierung* (Bd. II, S. 197–220). Berlin: Duncker & Humblot.

GI. (2018). *Ethische Leitlinien*. Abgerufen am 18. September 2018 von https://gi.de/ueber-uns/organisation/unsere-ethischen-leitlinien/

Goldfarb, A., Greenstein, S. M., Tucker, C., & National Bureau of Economic Research (Hrsg.). (2015). *Economic analysis of the digital economy*. Chicago, Ill.: Univ. of Chicago Press.

Goldfarb, A., & Tucker, C. (2017). *Digital Economics* (No. w23684). Cambridge, MA: National Bureau of Economic Research. https://www.nber.org/papers/w23684

Hauser, M. (2015). *Das IT-Grundrecht: Schnittfelder und Auswirkungen*. Berlin: Duncker & Humblot.

Hildebrandt, M. (2016). *Smart technologies and the end(s) of law: novel entanglements of law and technology* (Paperback edition). Cheltenham, UK Northampton, MA, USA: EE Edward Elgar Publishing.

Hoffmann-Riem, W. (2016a). *Innovation und Recht, Recht und Innovation: Recht im Ensemble seiner Kontexte*. Tübingen: Mohr Siebeck.

Hoffmann-Riem, W. (2016b). Selbstregelung, Selbstregulierung und regulierte Selbstregulierung im digitalen Kontext. In M. Fehling & U. Schliesky (Hrsg.), *Neue Macht- und Verantwortungsstrukturen in der digitalen Welt* (S. 27–52). Nomos Verlagsgesellschaft mbH & Co. KG. https://doi.org/10.5771/9783845276014-27

Hoffmann-Riem, W. (2017). Verhaltenssteuerung durch Algorithmen – Eine Herausforderung für das Recht. *Archiv des Öffentlichen Rechts*, 142(1), 1–42. https://doi.org/10.1628/000389117X14894104852645

Hoffmann-Riem, W. (Hrsg.). (2018). *Big Data – Regulative Herausforderungen* (Bd. 77). Baden-Baden: Nomos.

Hofmann, T., & Schölkopf, B. (29. Januar 2015). Vom Monopol auf Daten ist abzuraten. *Frankfurter Allgemeine Zeitung*, S. 14.

Hornung, G. (2015). *Grundrechtsinnovationen*. Tübingen: Mohr Siebeck.

Hornung, G., & Hofmann, K. (2017). *Industrie 4.0 und das Recht: Drei zentrale Herausforderungen*. München: Plattform Industrie 4.0, acatech. Abgerufen am 17. August 2018 von https://www.acatech.de/wp-content/uploads/2018/03/WissBeirat_I40-bf_acatech_Recht_und_Industrie40_bf.pdf

IEEE Standards Association. (2016). *IEEE Standards Association Introduces Global Initiative for Ethical Considerations in the Design of Autonomous Systems*. Abgerufen am 18. Januar 2018 von http://standards.ieee.org/news/2016/ieee_autonomous_systems.html

Industrial Data Space Association. (o. J.). Industrial Data Space e.V. Abgerufen am 18. Januar 2018 von http://www.industrialdataspace.org/

Kagermann, H., Riemensperger, F., Hoke, D., Helbig, J., & Stocksmeier, D. (Hrsg.). (2014). *Smart Service Welt. Umsetzungsempfehlungen für das Zukunftsprojekt internetbasierte Dienste für die Wirtschaft*. Berlin: acatech. Abgerufen am 17. August 2018 von https://www.acatech.de/wp-content/uploads/2015/03/BerichtSmartService2015_mitUmschlag_bf.pdf

Kagermann, H., Wahlster, W., & Helbig, J. (Hrsg.). (2013). *Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0*. Frankfurt am Main. Abgerufen am 17. August 2018 von https://www.bmbf.de/files/Umsetzungsempfehlungen_Industrie4_0.pdf

Kosinski, M., Stillwell, D., & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences*, *110*(15), 5802–5805. https://doi.org/10.1073/pnas.1218772110

Kosinski, M., & Wang, Y. (2017). Deep neural networks are more accurate than humans at detecting sexual orientation from facial images. *PsyArXiv Preprints*. https://doi.org/10.17605/OSF.IO/HV28A

Krempl, S. (30. August 2017). *Smart Toys: Bundesnetzagentur ließ 400 Kaufangebote im Netz löschen*. Abgerufen am 10. Oktober 2017 von https://www.heise.de/newsticker/meldung/Smart-Toys-Bundesnetzagentur-liess-400-Kaufangebote-im-Netz-loeschen-3816717.html

Kühl, E. (2018, April 4). Bis zu 87 Millionen Facebook-Nutzer betroffen. ZEIT-Online. Abgerufen am 10.10.2018 von https://www.zeit.de/digital/internet/2018-04/datenmissbrauch-facebook-zuckerberg-cambridge-analytica

Kühling, J., Buchner, B., Bäcker, M., Bergt, M., Boehm, F., Caspar, J., & Dix, A. (2018). *Datenschutz-Grundverordnung/BDSG: Kommentar* (2. Auflage). München: C.H. Beck.

Latzer, M., Hollnbuchner, K., Just, N., & Saurwein, F. (2016). The economics of algorithmic selection on the Internet. In J. Bauer & M. Latzer (Hrsg.), *Handbook on the Economics of the Internet* (S. 395–425). Edward Elgar Publishing. https://doi.org/10.4337/9780857939852

Latzer, M., Just, N., Saurwein, F., & Slominski, P. (2002). *Selbst- und Ko-Regulierung im Mediamatiksektor: Alternative Regulierungsformen zwischen Staat und Markt*. Heidelberg: Springer VS. Abgerufen am 17. August 2018 von http://link.springer.com/10.1007/978-3-663-11349-2

Levin, J. (2011). *The Economics of Internet Markets* (No. w16852). Cambridge, MA: National Bureau of Economic Research. https://doi.org/10.3386/w16852

Lewinski, K. von. (2014). *Die Matrix des Datenschutzes: Besichtigung und Ordnung eines Begriffsfeldes*. Tübingen: Mohr Siebeck.

Li, N., Li, T., & Venkatasubramanian, S. (2007). t-Closeness: Privacy Beyond k-Anonymity and l-Diversity (S. 106–115). IEEE. https://doi.org/10.1109/ICDE.2007.367856

Machanavajjhala, A., Kifer, D., Gehrke, J., & Venkitasubramaniam, M. (2007). L-diversity: Privacy beyond k-anonymity. *ACM Transactions on Knowledge Discovery from Data*, *1*(1), 3–es. https://doi.org/10.1145/1217299.1217302

Marauhn, T. (2015). Sicherung grund- und menschenrechtlicher Standards gegenüber neuen Gefährdungen durch private und ausländische Akteure. *Veröffentlichungen der Vereinigung der deutschen Staatsrechtslehrer*, *74*, 373–400.

MAS. (2016). *FinTech Regulatory Sandbox Guidelines* (Richtlinien). Singapur. Abgerufen am 17. August 2018 von http://www.mas.gov.sg/~/media/Smart%20Financial%20Centre/Sandbox/FinTech%20Regulatory%20Sandbox%20Guidelines.pdf

Matsakis, L. (2017). Study That Claimed AI Could Determine a Person's Sexuality Is Under Ethical Review. Abgerufen am 16. Januar 2018 von https://motherboard.vice.com/en_us/article/j5gedd/study-that-claimed-ai-could-determine-a-persons-sexuality-is-under-ethical-review

Mayer-Schönberger, V., & Cukier, K. (2013). *Big Data: die Revolution, die unser Leben verändern wird* (D. Mallett, Übers., 2. Auflage). München: Redline Verlag.

Mönig, J. M. (2017). *Vom „oikos" zum Cyberspace: das Private in der politischen Philosophie Hannah Arendts*. Bielefeld: transcript.

Monopolkommission. (2015). *Wettbewerbspolitik: Herausforderung digitale Märkte* (Sondergutachten der Monopolkommission gemäß § 44 Abs. 1 Satz 4 GWB No. 68). Bonn. Abgerufen am 17. August 2018 von http://www.monopolkommission.de/images/PDF/SG/SG68/S68_volltext.pdf

Montavon, G., Samek, W., & Müller, K.-R. (2018). Methods for interpreting and understanding deep neural networks. *Digital Signal Processing*, 73, 1–15. https://doi.org/10.1016/j.dsp.2017.10.011

Nissenbaum, H. F. (2010). *Privacy in context: technology, policy, and the integrity of social life*. Stanford, CA: Stanford Law Books, an imprint of Standford University Press.

Paal, B. P., Pauly, D. A., & Ernst, S. (2018). *Datenschutz-Grundverordnung Bundesdatenschutzgesetz* (2. Auflage). München: C.H. Beck.

Peitz, M., & Waldfogel, J. (Hrsg.). (2012). *The Oxford Handbook of the Digial Economy*. Oxford, New York: Oxford University Press.

Peters, R. (2010). *Internet-Ökonomie*. Berlin: Springer.

Pohle, J. (2016). PERSONAL DATA NOT FOUND: Personenbezogene Entscheidungen als überfällige Neuausrichtung im Datenschutz. *Datenschutz Nachrichten – DANA*, *1*, 14–19.

Reece, A. G., & Danforth, C. M. (2017). Instagram photos reveal predictive markers of depression. *EPJ Data Science*, *6*(1), 15. https://doi.org/10.1140/epjds/s13688-017-0110-z

Rochet, J.-C., & Tirole, J. (2003). Platform Competition in Two-Sided Markets. *Journal of the European Economic Associa*, *1*(4), 990–1029.

Rössler, B. (2001). *Der Wert des Privaten* (1. Auflage, Originalausgabe). Frankfurt am Main: Suhrkamp.

Rössler, B. (2016). Wie wir uns regieren. Soziale Dimensionen des Privaten in der Post-Snowden-Ära, *01-2016*, 103–118.

Roßnagel, A. (2016). Eine Zukunft ohne Selbstbestimmung. *Spektrum Kompakt – Der digitale Mensch*, 41–49.

Roßnagel, A., & Nebel, M. (2015). (Verlorene) Selbstbestimmung im Datenmeer: Privatheit im Zeitalter von Big Data. *Datenschutz und Datensicherheit – DuD*, *39*(7), 455–459. https://doi.org/10.1007/s11623-015-0449-x

Rysman, M. (2009). The Economics of Two-Sided Markets. *Journal of Economic Perspectives*, *23*(3), 125–143. https://doi.org/10.1257/jep.23.3.125

Samsel, H. (2016). Risiken der Informationstechnologie. In H. Pünder & A. Klafki (Hrsg.), *Risiko und Katastrophe als Herausforderung für die Verwaltung* (Bd. 40, S. 121 ff.). Baden-Baden: Nomos.

Schliesky, U., Hoffmann, C., Luch, A. D., Schulz, S. E., & Borchers, K. C. (Hrsg.). (2014). *Schutzpflichten und Drittwirkung im Internet: das Grundgesetz im digitalen Zeitalter* (1. Auflage). Baden-Baden: Nomos.

Schmalensee, R., & Evans, D. (2007). Industrial Organization of Markets with Two-Sided Platforms. *Competition Policy International*, *3*(1), 151–179.

Schröder, M. (2012). Selbstregulierung im Datenschutzrecht – Notwehr oder Konzept? *Zeitschrift für Datenschutz – ZD*, *9*, 418–420.

Schütt, K. T., Arbabzadah, F., Chmiela, S., Müller, K. R., & Tkatchenko, A. (2017). Quantum-chemical insights from deep tensor neural networks. *Nature Communications*, *8*, 13890. https://doi.org/10.1038/ncomms13890

Schulz, W., & Held, T. (2002). *Regulierte Selbstregulierung als Form modernen Regierens: Endbericht Mai 2002*. Hamburg: Verl. Hans-Bredow-Inst. Abgerufen am 17. August 2018 von https://www.hans-bredow-institut.de/uploads/media/Publikationen/cms/media/a80e5e6dbc2427639ca0f437fe76d3c4c95634ac.pdf

Schweitzer, H., Fetzer, T., & Peitz, M. (2016). *Digitale Plattformen: Bausteine für einen künftigen Ordnungsrahmen* (Diskussionspapier No. 16-042). Mannheim: Zentrum für Europäische Wirtschaftsforschung. Abgerufen am 17. August 2018 von https://ub-madoc.bib.uni-mannheim.de/41160/1/dp16042.pdf

Shy, O. (2011). A Short Survey of Network Economics. *Review of Industrial Organization*, *38*(2), 119–149. https://doi.org/10.1007/s11151-011-9288-6

Singelnstein, T. (2018). Big Data und Strafverfolgung. In W. Hoffmann-Riem (Hrsg.), *Big Data – Regulative Herausforderungen* (Bd. 77). Baden-Baden: Nomos.

Spitz, M. (2009). Verräterisches Handy. Abgerufen am 5. Januar 2018 von http://www.zeit.de/datenschutz/malte-spitz-vorratsdaten

Stalder, F. (2016). *Kultur der Digitalität* (1. Auflage, Originalausgabe). Berlin: Suhrkamp.

SVRV. (2017). *Digitale Souveränität* (Gutachten des Sachverständigenrats für Verbraucherfragen). Berlin. Abgerufen am 17. August 2018 von http://www.svr-verbraucherfragen.de/wp-content/uploads/Gutachten_Digitale_Souver%C3%A4nit%C3%A4t_.pdf

Sweeney, L. (2000). *Simple Demographics Often Identify People Uniquely* (No. 3). Pittsburgh: Carnegie Mellon University. Abgerufen am 17. August 2018 von https://dataprivacylab.org/projects/identifiability/paper1.pdf

Sweeney, L. (2002). k-Anonymity: A model for protecting privacy. *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems*, *10*(5), 557–570.

UN. (2016). *E-government in support of sustainable development* (E-Government Survey 2016). New York.

van der Sloot, B. (2014). Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation. *International Data Privacy Law*, *4*(4), 307–325. https://doi.org/10.1093/idpl/ipu014

Waidner, M., Backes, M., & Müller-Quade, J. (2017). *Positionspapier Cybersicherheit in Deutschland*. Stuttgart: Fraunhofer Verlag. Abgerufen am 17. August 2018 von https://www.kompetenz-it-sicherheit.de/wp-content/uploads/2017/02/Positionspapier_der_drei_Kompetenzzentren_IT-Sicherheit_web.pdf

Wehage, J.-C. (2013). *Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und seine Auswirkungen auf das bürgerliche Recht*. Göttingen: Univ.-Verl. Göttingen.

Westin, A. F. (1967). *Privacy and freedom*. London: Bodley head.

Wiegerling, K. (2011). *Philosophie intelligenter Welten*. Paderborn München: Wilhelm Fink.

Wischmeyer, T. (2016). Informationssicherheitsrecht (Regulating Information Security). *Die Verwaltung*, *50*(2). Abgerufen am 17. August 2018 von https://papers.ssrn.com/abstract=2844464

Wischmeyer, T. (2018). Regulierung intelligenter Systeme. *Archiv Des Oeffentlichen Rechts*, *143*(1), 1–66. https://doi.org/10.1628/aoer-2018-0002

7 Abkürzungsverzeichnis

ACM	Association for Computing Machinery (US)
API	Application programming interface (Schnittstelle zur Anwendungsprogrammierung)
AV	audiovisuell
BDSG	Bundesdatenschutzgesetz
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BSI	Bundesamt für Sicherheit in der Informationstechnik
BMBF	Bundesministerium für Bildung und Forschung
BVerfG	Bundesverfassungsgericht
DLR	Deutsches Zentrum für Luft- und Raumfahrt
EU-DSGVO	Europäische Datenschutz-Grundverordnung
EC	European Commission (Europäische Kommission)
EFI	Expertenkommission Forschung und Innovation
EOSC	European Science Cloud
EU	Europäische Union
Europarl	Europäisches Parlament
FCA	Financial Conduct Authority (Vereinigtes Königreich)
GG	Grundgesetz
GI	Gesellschaft für Informatik
GWB	Gesetz gegen Wettbewerbsbeschränkung
HTTPS	Hypertext Transfer Protocoll secure (sicheres Hypertext-Übertragungsprotokoll)
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
ISMS	Information-Security-Management-System
IT	Informationstechnologie
MAS	Monetary Authority of Singapore
ML	Mitglied der Leopoldina
NFDI	Nationale Forschungsdateninfrastruktur
NGO	non-governmental organization (Nichtregierungsorganisation)
SVRV	Sachverständigenrat für Verbraucherfragen
UN	United Nations (Vereinte Nationen)

8 Autorinnen und Autoren

Prof. Dr. Michael Backes
CISPA Helmholtz-Zentrum für Informationssicherheit

Michael Backes ist der Gründungsdirektor und CEO des CISPA Helmholtz-Zentrum für Informationssicherheit. Die Forschungsergebnisse von Michael Backes sind durch mehr als 250 referierte Publikationen in den führenden internationalen Zeitschriften und Tagungsbänden nachgewiesen und durch wissenschaftliche Preise vielfach ausgezeichnet. So erhielt er 2009 als erster Forscher Deutschlands den weltweiten MIT TR35 Award. Im Oktober 2018 erhielt er den Ehrendoktortitel der Universität Nancy, Frankreich. Michel Backes ist Mitglied der Deutschen Akademie der Technikwissenschaften – acatech.

Prof. Dr. Erwin Böttinger
Hasso-Plattner-Institut für Digital Engineering gGmbH, Universität Potsdam / Digital Health Center

Erwin Böttinger ist Professor und Chair für Digital Health und Personalized Medicine an der gemeinsamen Digital Engineering Fakultät der Hasso-Plattner-Institut (HPI) gGmbH und der Universität Potsdam. Er ist Gründungsdirektor des HPI Digital Health Centers. Von November 2015 bis Juli 2017 war Erwin Böttinger Vorsitzender des Vorstands des Berliner Instituts für Gesundheitsforschung/Berlin Institute of Health (BIH). Er gilt als internationaler Experte für Personalisierte Medizin und Digital Health, insbesondere durch seine Leistungen als Gründungsdirektor des Charles-Bronfman-Instituts für Personalisierte Medizin an der Icahn School of Medicine at Mount Sinai in New York, USA, von 2005 bis 2015.

Prof. Dr. Johannes Buchmann
Fachbereich Informatik, Technische Universität Darmstadt

Die Spezialgebiete von Johannes Buchmann sind Computeralgebra, Kryptographie und Cybersicherheit. In seiner Forschung konzentriert er sich auf langfristige Cybersicherheit für das Zeitalter der Quantencomputer und die gesellschaftlichen Aspekte der Cybersicherheit. Er hat zum Beispiel zusammen mit seiner Arbeitsgruppe neue Post-Quanten-Kryptographie-Verfahren entwickelt, die jetzt internationale Standards sind und das Projekt Internet Privacy der Deutschen Akademie der Technikwissenschaften acatech geleitet. Er arbeitet mit Forschungseinrichtungen und Unternehmen weltweit zusammen, zum Beispiel mit dem National Institute for Information and Communication Technology NICT in, der University of Tokyo in Japan, der University of Waterloo in Kanada, der Tallinn University in Estland und Intel. Johannes Buchmann ist Sprecher des DFG-Sonderforschungsbereiches CROSSING, Sprecher des Profilbereichs CYSEC der TU Darmstadt und Sprecher des Center for Research in Security and Privacy CRISP in Darmstadt. Er ist Mitglied der Nationalen Akademie der Wissenschaften Leopoldina, der Deutschen Akademie der Technikwissenschaften – acatech, der Akademie der Wissenschaften und Literatur Mainz und der Berlin-Brandenburgischen Akademie der Wissenschaften.

Prof. Dr.-Ing. Jörg Eberspächer
Technische Universität München

Jörg Eberspächer ist emeritierter Ordinarius für Kommunikationsnetze mit den Forschungsschwerpunkten Netzarchitekturen für breitbandige Mobilfunknetze und

schnelles Internet, selbstorganisierende Netze sowie techno-ökonomische Bewertung von Netzen. Darüber hinaus befasst er sich Im MÜNCHNER KREIS und im Center for Digital Technology and Management (CDTM) mit interdisziplinären und gesellschaftlichen Aspekten von Anwendungen der Informations-und Kommunikationstechnik. Er ist Mitglied der Nationalen Akademie der Wissenschaften Leopoldina und der Deutschen Akademie der Technikwissenschaften acatech.

Prof. Anja Feldmann, Ph.D.
Direktorin für Internet Architektur,
Max-Planck-Institut für Informatik

Anja Feldmanns Forschung beschäftigt sich mit dem Internet, insbesondere mit Untersuchungen des Internetverkehrs, um Netzwerk-Engpässe und Sicherheitslücken zu erkennen und dann zu beheben.

Anja Feldmann studierte Informatik an der Universität Paderborn, promovierte an der Carnegie Mellon University. Die folgenden vier Jahre forschte sie an den AT&T Labs Research, bevor sie Professuren an der Universität des Saarlands, der TU München und der TU Berlin innehatte.

Anfang 2018 schließlich übernahm sie die Stelle einer Direktorin am Max-Planck-Institut für Informatik in Saarbrücken, und ist Honorarprofessorin an der TU Berlin sowie der Universität des Saarlands. Im Mai 2012 wurde sie in den Aufsichtsrat von SAP berufen. Für ihre innovative Forschung wurde sie mit dem Gottfried Wilhelm Leibniz-Preis und dem Berliner Wissenschaftspreis ausgezeichnet. Sie ist Mitglied der Berlin-Brandenburgischen Akademie der Wissenschaften und der Nationalen Akademie der Wissenschaften Leopoldina.

Prof. Dr. Petra Grimm
Institut für Digitale Ethik,
Hochschule der Medien Stuttgart

Petra Grimm ist Professorin für Medienforschung und Kommunikationswissenschaft. Ihre Fachgebiete sind Digitale Ethik, Medienwissenschaft und Narratologie. Schwerpunkte ihrer Arbeit sind: Digitalisierung der Gesellschaft, Ethics and Privacy by Design, Mediennutzung von Kindern und Jugendlichen sowie Medien und Gewalt. Aktuell forscht sie zu Ethics by Design in autonomen Fahrzeugen (BMBF-Projekt KoFFi), präventive digitale Sicherheitskommunikation und Zivilcourage (BMBF-Projekt PRÄDISIKO), Learning Analytics für Prüfungsleistungen und Studienerfolg (MWK-BaWü-Projekt LAPS) und SmartIdentifikation (BMBF-Projekt).

Prof. Dietmar Harhoff, Ph.D.
Direktor, Max-Planck-Institut für Innovation und Wettbewerb, München

Dietmar Harhoff leitet die wirtschaftswissenschaftliche Abteilung des Max-Planck-Instituts für Innovation und Wettbewerb. Die Abteilung analysiert Innovationsprozesse und Rahmenbedingungen für Entrepreneurship. In den Forschungsarbeiten des Instituts werden auch Aspekte der digitalen Transformation und der Datenökonomie untersucht. Dietmar Harhoff ist als Vorsitzender der Expertenkommission Forschung und Innovation (EFI) und als Mitglied des Wissenschaftlichen Beirats beim Bundesministerium für Wirtschaft beratend für die Bundesregierung tätig. Dietmar Harhoff berät zudem Startup-Unternehmen und Inkubator-Organisationen. Er ist Mitglied der Nationalen Akademie der Wissenschaften Leopoldina, der Bayerischen Akademie der Wissenschaften und der Deutschen Akademie der Technikwissenschaften – acatech.

Prof. Dr. Otthein Herzog
Tongji University, Shanghai, PRC, China
Intelligent Urbanization Co-Creation Center

Otthein Herzog ist Informatiker und arbeitet seit mehr als 30 Jahren auf dem Gebiet der Künstlichen Intelligenz mit den Schwerpunkten Wissensrepräsentation und Wissensverarbeitung, Maschinelles Lernen, Multiagentensysteme und Big Data Analytics für Anwendungsgebiete wie

Industrie 4.0 und Smart Cities sowie die semantische Analyse und Synthese von Bildern und Videos. Seine gegenwärtigen Projekte auf dem Gebiet Smart Cities werden im Rahmen von Horizon 2020 von der Europäischen Union, der Stadt Shanghai und dem Ministry of Science and Technology in China finanziert. Er ist auch an der Jacobs University Bremen und der Universität Bremen tätig und darüber hinaus seit 1998 Affiliate Professor am Machine Learning and Inference Laboratory der George Mason University, Fairfax, VA. Er ist Mitglied der Deutschen Akademie der Technikwissenschaften – acatech.

Prof. Dr. Thomas Hoeren
Institut für Informations-, Telekommunikations- und Medienrecht (ITM), Westfälische Wilhelms-Universität Münster

Thomas Hoeren ist Rechtswissenschaftler auf dem Gebiet des Informationsrechts. Seine Forschungsinhalte umfassen alle zivilen Rechtsgebiete, die Einfluss auf Information haben – wie etwa das Urheberrecht, IT-Recht, Medienrecht, Datenschutzrecht und Teile des Gewerblichen Rechtsschutzes. Er ist Direktor des ITM, das zurzeit die Forschungsstelle Recht des DFN, die Forschungsstelle für Gewerblichen Rechtsschutz e.V. und die Koordination des deutschlandweiten interdisziplinären Forschungsclusters zu Big Data „Abida“ beherbergt. Thomas Hoeren ist Mitglied der Europäischen Akademie der Wissenschaften und Künste sowie Generalberichterstatter der Liga für Wettbewerbsrecht. Bis 2004 war er Mitglied der Task Force Group on Intellectual Property der Europäischen Kommission und des Wissenschaftlichen Beirats der DENIC eG. Er erhielt mehrere Auszeichnungen, darunter den Forschungspreis Technische Kommunikation und den Preis für deutsch-niederländische Wissenschaftskooperation.

Prof. Dr. Wolfgang Hoffmann-Riem
Affiliate Professor für Recht und Innovation der Bucerius Law School in Hamburg

Wolfgang Hoffmann-Riem ist emeritierter ord. Professor für Öffentliches Recht und Verwaltungswissenschaften der Universität Hamburg und Richter des Bundesverfassungsgerichts a. D.. Seine Forschungsschwerpunkte sind Verfassungs- und Verwaltungsrecht, rechtswissenschaftliche Innovationsforschung, Medien- und Informationswissenschaft.

Prof. Dr. Jeanette Hofmann
Professorin für Internetpolitik an der Freien Universität Berlin

Die Politikwissenschaftlerin Jeanette Hofmann leitet am Wissenschaftszentrum Berlin für Sozialforschung die Projektgruppe „Politikfeld Internet“. Ihre aktuelle Forschung beschäftigt sich mit Digitalisierung und Demokratie sowie der Entstehung von Internetpolitik in Deutschland. Weitere Forschungsschwerpunkte betreffen die Regulierung des Internet auf internationaler Ebene und Big Data als Gegenstand wie auch als quantifizierende Form von Regulierung. Sie ist Gründungsdirektorin des Alexander von Humboldt Instituts für Internet und Gesellschaft, das nach einer initialen Finanzierung von Google von einer Reihe weiterer Unternehmen und öffentlichen Institutionen gefördert wird. Zudem leitet sie als Principal Investigator zwei Forschungsgruppen am neu gegründeten Weizenbaum Institut für die vernetzte Gesellschaft zu den Themen ‚Digitalisierung und Demokratie‘ und ‚Quantifizierung und gesellschaftliche Regulierung‘. Im Wettbewerb um das deutsche Internet Institut hat sie den Berliner Antrag auf wissenschaftlicher Ebene koordiniert. Von 2010 bis 2013 war sie Sachverständige in der Enquete-Kommission ‚Internet und digitale Gesellschaft‘ des Deutschen Bundestages.

Prof. Dr. Thomas Hofmann
Institut für Maschinelles Lernen, Eidgenössische Technischen Hochschule Zürich

Thomas Hofmann ist Professor für Datenanalytik und ein Experte für maschinelles Lernen und künstliche Intelligenz. Seine wissenschaftlichen Arbeiten der letzten

25 Jahre reichen von der Grundlagenforschung in Lerntheorie, Modellierung und Optimierung bis hin zu Anwendungen, insbesondere im Bereich des Text- und Bildverstehens. Er ist Co-Direktor des Max-Planck ETH Zentrums für Lernende Systeme und Mitgründer/CTO von 1plusX. Vor seinem Wechsel an die ETH Zürich war er knapp 8 Jahre für Google als Entwicklungsleiter am Standort Zürich tätig, hier vor allem im Bereich Web-, Produktsuche und Werbeoptimierung. Seine Gruppe unterhält finanzierte Kooperationen mit Google, Microsoft, IBM, sowie 1plusX und erhält finanzielle Zuwendungen vom SNF (Schweizer Nationalfonds) und der InnoSuisse. Im Nebenamt hat Thomas Hofmann als externer Experte in einer Arbeitsgruppe des Deutschen Ethikrats mitgewirkt. Er berät regelmäßig Start-Ups in technischen und strategischen Fragen und betätigt sich im kleinen Umfang als Privatinvestor.

Prof. Dr. Paul Hoyningen-Huene
Institut für Philosophie, Leibniz Universität Hannover (pensioniert)

Paul Hoyningen-Huenes Forschungsschwerpunkte sind die allgemeine Wissenschaftsphilosophie, die Wissenschaftsdynamik, die Philosophie verschiedener Einzelwissenschaften (insbesondere Philosophie der Ökonomik) sowie die Wissenschaftsethik. Er ist Lehrbeauftragter am Department of Economics der Universität Zürich und seit 2001 Mitglied der Nationalen Akademie der Wissenschaften Leopoldina.

Prof. Dr. Jan C. Joerden
Lehrstuhl für Strafrecht, insbesondere Internationales Strafrecht und Strafrechtsvergleichung, Rechtsphilosophie, Europa-Universität Viadrina Frankfurt (Oder)

Jan Joerden war von 1994 bis 2002 Prorektor der Europa-Universität Viadrina. Seit 1995 ist er Leiter des Interdisziplinären Zentrums für Ethik an der EUV (Finanzierung durch Haushaltsmittel der Universität und von Fall zu Fall eingeworbene Drittmittel). 2007/08 war er Senior Fellow am Alfried-Krupp-Wissenschaftskolleg Greifswald und 2009/10 Fellow und Leiter einer Forschungsgruppe am Zentrum für interdisziplinäre Forschung (ZiF) der Universität Bielefeld. Mitwirkung an Politikberatung im Rahmen von Leopoldina und Acatech.

Prof. Dr.-Ing. Paul J. Kühn
Institut für Kommunikationsnetze und Rechnersysteme (IKR), Universität Stuttgart

Paul Kühn forscht auf dem Gebiet der Informationstechnik, der verteilten Systeme, Kommunikationsnetze und -protokolle sowie Performance Modellierung. Er befasst sich dabei u.a. mit Cyber-Physical Systems, Warteschlangentheorie, Parallelverarbeitung, Energie-Effizienz von Cloud Data Centers und Echtzeit-Performance. Von 1981 bis 2009 leitete er das Institut für Kommunikationsnetze und Rechnersysteme. Bei seiner Forschung hat er gemeinsame Projekte mit Firmen wie der Siemens AG (Entwicklung von Packet Switching), Philips Kommunikations Industrie (Test von Vermittlungssystemen), Telenorma (Signalisiernetze) und Alcatel-Lucent (Big Data Analytics). Darüber hinaus ist er auch beratend für Unternehmen wie Siemens Enterprise/Unify tätig.

Prof. Dr. Dr. Thomas Lengauer
Max-Planck-Institut für Informatik, Saarbrücken

Prof. Lengauer ist Mathematiker und Informatiker und hat in den letzten 25 Jahren hauptsächlich im Bereich der Bioinformatik geforscht. Forschungsthemen waren die Vorhersage von Struktur und Funktion von Proteinen und die Berechnung vom Bindeverhalten von Wirkstoffen an Proteine. Gegenwärtig forscht Thomas Lengauer zur Analyse von Genom-, Transkriptom- und Epigenomdaten sowie zur bioinformatischen Analyse der Resistenz von Viren gegen Wirkstoffe. Er ist Präsident der International Society for Computational Biology und Präsidiumsmitglied der Leopoldina sowie Sprecher

ihrer Wissenschaftlichen Kommission „Digitalisierte Gesellschaft“. Er ist Mitglied der Wissenschaftlichen Kommission der Einstein-Stiftung und der Wissenschaftlichen Beiräte des Heidelberg Institute for Theoretical Studies sowie des Zentrums für Biotechnologie (CeBiTec) der Universität Bielefeld. Er ist Mitglied der Nationalen Akademie der Wissenschaften Leopoldina, der Deutschen Akademie der Technikwissenschaft acatech sowie der Academia Europaea.

Prof. Dr. Volker Markl
Fachgebietsleiter Datenbanksysteme und Informationsmanagement (DIMA) an der Technischen Universität Berlin

Volker Markls aktuelle Forschungsinteressen sind neuartige Hardwarearchitekturen für das Informationsmanagement, die skalierbare Verarbeitung und Optimierung von Programmen zur deklarativen Datenanalyse sowie die skalierbare Datenwissenschaft, einschließlich Graph Mining, Text Mining und maschinelles Lernen. Volker Markl ist Chief Scientist und Forschungsgruppenleiter der Gruppe „Intelligente Analyse von Massendaten – Smart Data“ am Deutschen Forschungszentrum für künstliche Intelligenz (DFKI), Direktor des Berlin Big Data Centers (BBDC), Co-Direktor des Berliner Zentrum für Maschinelles Lernen und Status-Professor an der Universität von Toronto. Er ist Gründungsmitglied der Big Data Value Association/Big Data Value PPP, wurde 2018 zum Präsidenten der VLDB Endowment (01.01.2018 – 31.12.2021) gewählt, ist Arbeitsgruppenleiter der Plattform Lernende Systeme, Mitglied des wissenschaftlichen Beirats des Alexander von Humboldt-Instituts für Internet und Gesellschaft (HIIG), Principal Investigator des Einstein Center Digital Future sowie Mitglied des Lenkungsausschusses der Graduiertenschule HEIBRiDS. Volker Markl war außerdem Mitbegründer, Berater und Mentor mehrerer Start-ups, darunter DataArtisans, Parstream und Aklamio. Darüber hinaus berät und kooperiert Prof. Markl mit verschiedenen IT-Unternehmen, darunter IBM, SAP, Microsoft, Deutsche Telekom, HP, Oracle, Amazon, Huawei, Zalando sowie vielen KMU.

Prof. Dr. Klaus-Robert Müller
Professor für Informatik an der TU Berlin (Sprecher der AG)

Klaus-Robert Müller ist seit 2006 Informatikprofessor an der TU Berlin und Sprecher des Berliner Zentrums für maschinelles Lernen. Er war Gastwissenschaftler am Institute for Pure and Applied Mathematics (IPAM) der University of California, Los Angeles (USA). Seit 2012 ist er Distinguished Professor der Korea University in Seoul, 2014 übernahm er das Co-Direktorat des Berlin Big Data Center. 2014 wurde Klaus-Robert Müller mit dem Berliner Wissenschaftspreis des Regierenden Bürgermeisters, sowie 2017 mit dem Vodafone Innovation Award ausgezeichnet. Seit 2017 ist er externes wissenschaftliches Mitglied der Max-Planck-Gesellschaft. Seine Forschungsinteressen sind intelligente Datenanalyse, maschinelles Lernen, statistische Signalverarbeitung und statistische Lerntheorie mit Anwendungsschwerpunkten in Industrie und Wissenschaften: Quantenchemie, digitale Pathologie und Neurowissenschaften – insbesondere die Erforschung der Schnittstelle zwischen Hirn und Maschine: das nichtinvasive EEG-basierte Brain Computer Interface. Das von ihm geleitete Institut wird sowohl von öffentlicher Hand (BMBF, EU, DFG, NRF) als auch von Unternehmen (u.a. BSH, Fraunhofer, Daimler, P3 group, BASF, Amazon, Google, Nikon, Facebook, Pfizer) finanziert. Darüber hinaus ist Klaus-Robert Müller auch beratend für Unternehmen und Institutionen wie Fraunhofer, Korea University, Aalto University, Aarhus University, IPAM, die deutsche Bundesregierung und den ERC sowie den SNF tätig. Er ist Mitglied der Nationale Akademie der Wissenschaften Leopoldina und der Berlin Brandenburgischen Akademie der Wissenschaften.

Prof. Dr. Peter Propping ML †
Institut für Humangenetik, Rheinische Friedrich-Wilhelms-Universität Bonn

Die wissenschaftlichen Arbeitsgebiete von Peter Propping umfassten die Medizinische Genetik, insbesondere die Vererbung genetisch komplexer neuropsychiatrischer Störungen wie Alkoholismus, bipolare affektive Störung, Schizophrenie, Epilepsie sowie von Krebsdispositionen. Außerdem beschäftigte er sich mit der Geschichte der Humangenetik und Eugenik. Von 1984 bis 2008 war er Direktor des Instituts für Humangenetik an der Universität Bonn. Er war Mitglied der Nationalen Akademie der Wissenschaften Leopoldina.

Prof. Dr. Helge J. Ritter
Technische Fakultät an der Universität Bielefeld

Helge Ritter ist Neuroinformatiker und seit 1990 Professor an der Technischen Fakultät der Universität Bielefeld. Seine Forschungsschwerpunkte sind selbstorganisierende und lernende Systeme und ihre Anwendung auf maschinelles Sehen, Robotersteuerung, Datenanalyse und interaktive Mensch-Maschine-Schnittstellen. Helge Ritter wurde 1999 mit dem SEL Alcatel Research Prize ausgezeichnet und 2001 mit dem Leibniz Preis der Deutschen Forschungsgemeinschaft. Er ist einer der Gründungsdirektoren des Bielefelder Forschungsinstituts für Kognition und Robotik (CoR-Lab) und seit 2007 Koordinator des Exzellenzclusters CITEC mit dem Forschungsschwerpunkt Kognitive Interaktionstechnologie. Beide Institute verbinden Grundlagen- und Anwendungsforschung in Kooperation mit etlichen Partnern, darunter Honda Research Europe, Miele, Bertelsmann und die von Bodelschwinghschen Stiftungen Bethel. Helge Ritter ist Mitglied der Nordrhein-Westfälischen Akademie der Wissenschaften und der Künste und der Deutschen Akademie der Technikwissenschaft – acatech.

Prof. Dr. Bernhard Schölkopf
Max-Planck-Institut für Intelligente Systeme Tübingen

Bernhard Schölkopf erforscht maschinelles Lernen und kausale Inferenz. Er ist Gründungsdirektor am MPI für Intelligente Systeme und wurde vielfach ausgezeichnet (u.a. J.K. Aggarwal Prize, Akademiepreis der BBAW, Royal Society Milner Award, Leibniz-Preis). In der Vergangenheit war er u.a. für die Bell Labs und für Microsoft Research tätig, zurzeit unterstützt er die Firma Amazon im Rahmen einer Nebentätigkeit beim Aufbau eines Forschungszentrums in Tübingen. Er ist Mitglied der Nationalen Akademie der Wissenschaften Leopoldina.

Prof. Dr. Fritz Strack
ehem. Lehrstuhl für Psychologie II, Universität Würzburg

Fritz Strack studierte Psychologie an der Universität Mannheim und an der Stanford University. Er war von 1991 bis 1995 als Professor an der Universität Trier tätig. Von 1995 bis 2016 war er Professor für Sozialpsychologie an der Universität Würzburg und Inhaber des Lehrstuhls für Psychologie II. Fritz Strack befasst sich mit Themen wie Soziale Kognition, Urteils- und Entscheidungsprozesse, Emotionen sowie automatische und kontrollierte Prozesse der Verhaltenssteuerung. Fritz Strack erhielt zahlreiche wissenschaftliche Auszeichnungen, darunter 2004 die Wilhelm-Wundt-Medaille der Deutschen Gesellschaft für Psychologie (gemeinsam mit Norbert Schwarz) und die Auszeichnung des Lebenswerks („distinguished scientist award“) durch die Society of Experimental Social Psychology (SESP). Er war Mitglied zahlreicher wissenschaftlicher Beiräte, u.a. des Hanse-Wissenschaftskollegs, des Institutes of Advanced Study in Toulouse IAST und des Bundesinstituts für Risikobewertung. Fritz Strack ist Mitglied der Nationalen Akademie der Wissenschaften Leopoldina.

Externe Gutachterinnen und Gutachter

Prof. Dr. Wilfried Juling	Karlsruher Institut für Technologie, Karlsruhe
Prof. Dr. Beate Roessler	Fakultät für Geisteswissenschaften, Universität Amsterdam
Prof. Dr. Alexander Roßnagel	Öffentliches Recht, Umwelt- und Technikrecht, Universität Kassel
Prof. Dr. Martin Vingron	Max-Planck-Institut für molekulare Genetik, Berlin

Die Akademien danken allen Autorinnen und Autoren sowie Gutachterinnen und Gutachtern sehr herzlich für Ihre Beiträge.

Wissenschaftliche Referentinnen

Dr. Stefanie Westermann	Nationale Akademie der Wissenschaften Leopoldina
Dr. Elke Witt	Nationale Akademie der Wissenschaften Leopoldina

Ausgewählte Publikationen der Schriftenreihe zur wissenschaftsbasierten Politikberatung

2018

Artenrückgang in der Agrarlandschaft
ISBN: 978-3-8047-3932-1

Künstliche Photosynthese
ISBN: 978-3-8047-3644-3

2017

Verbraucherpolitik für die Energiewende
ISBN: 978-3-8047-3666-5

Rohstoffe für die Energiewende: Wege zu einer sicheren und nachhaltigen Versorgung
ISBN: 978-3-8047-3664-1

Das Energiesystem resilient gestalten: Maßnahmen für eine gesicherte Versorgung
ISBN: 978-3-8047-3668-9

Social Media und digitale Wissenschaftskommunikation: Analyse und Empfehlungen zum Umgang mit Chancen und Risiken in der Demokratie
ISBN: 978-3-8047-3631-3

Promotion im Umbruch
ISBN: 978-3-8047-3633-7

2016

Additive Fertigung
ISBN: 978-3-8047-3676-4

Wissenschaftliche und gesellschaftliche Bedeutung bevölkerungsweiter Längsschnittstudien
ISBN: 978-3-8047-3552-1

2015

Mit Energieszenarien gut beraten
ISBN: 978-3-8047-3507-1

Flexibilitätskonzepte für die Stromversorgung 2050
ISBN: 978-3-8047-3503-3

Chancen und Grenzen des *genome editing*
ISBN: 978-3-8047-3493-7

Medizinische Versorgung im Alter – Welche Evidenz brauchen wir?
ISBN: 978-3-8047-3427-2

Perspektiven der Quantentechnologien
ISBN: 978-3-8047-3343-5

Public Health in Deutschland – Strukturen, Entwicklungen und globale Herausforderungen
ISBN: 378-9-8047-3345-9

Staatsschulden: Ursachen, Wirkungen und Grenzen
ISBN: 978-3-8047-3284-1

Alle Publikationen der Schriftenreihe sind auf den Internetseiten der Akademien als kostenfreies pdf-Dokument verfügbar.

Deutsche Akademie der Naturforscher Leopoldina e. V. Nationale Akademie der Wissenschaften

Jägerberg 1
06108 Halle (Saale)
Tel.: (0345) 472 39-867
Fax: (0345) 472 39-839
E-Mail: politikberatung@leopoldina.org

Berliner Büro:
Reinhardtstraße 14
10117 Berlin

acatech – Deutsche Akademie der Technikwissenschaften e. V.

Karolinenplatz 4
80333 München
Tel.: (089) 52 03 09-0
Fax: (089) 52 03 09-900
E-Mail: info@acatech.de

Hauptstadtbüro:
Pariser Platz 4a
10117 Berlin

Union der deutschen Akademien der Wissenschaften e. V.

Geschwister-Scholl-Straße 2
55131 Mainz
Tel.: (06131) 218528-10
Fax: (06131) 218528-11
E-Mail: info@akademienunion.de

Berliner Büro:
Jägerstraße 22/23
10117 Berlin

Die Nationale Akademie der Wissenschaften Leopoldina, acatech – Deutsche Akademie der Technikwissenschaften und die Union der deutschen Akademien der Wissenschaften unterstützen Politik und Gesellschaft unabhängig und wissenschaftsbasiert bei der Beantwortung von Zukunftsfragen zu aktuellen Themen. Die Akademiemitglieder und weitere Experten sind hervorragende Wissenschaftlerinnen und Wissenschaftler aus dem In- und Ausland. In interdisziplinären Arbeitsgruppen erarbeiten sie Stellungnahmen, die nach externer Begutachtung vom Ständigen Ausschuss der Nationalen Akademie der Wissenschaften Leopoldina verabschiedet und anschließend in der *Schriftenreihe zur wissenschaftsbasierten Politikberatung* veröffentlicht werden.

Schriftenreihe zur wissenschaftsbasierten Politikberatung

ISBN: 978-3-8047-3642-9