Leopoldina
Nationale Akademie
der Wissenschaften

acatech
DEUTSCHE AKADEMIE DER
TECHNIKWISSENSCHAFTEN

UNION
DER DEUTSCHEN AKADEMIEN
DER WISSENSCHAFTEN

2018
Kurzfassung der Stellungnahme

Privatheit in Zeiten der Digitalisierung

Nationale Akademie der Wissenschaften Leopoldina
acatech – Deutsche Akademie der Technikwissenschaften
Union der deutschen Akademien der Wissenschaften

Privatheit gilt als ein für alle Menschen wesentlicher Schutz- und Rückzugsraum. Das Recht auf Privatheit zählt zu den Freiheitsrechten und gilt als wichtige Grundlage für die freie Entwicklung und Entfaltung der Persönlichkeit. Eine Gesellschaft, die Freiheitsräume nicht mehr garantieren kann, ist nicht in der Lage, die gesellschaftliche Vielfalt zu erhalten, aus der heraus sich ein offener und freier Diskurs entfaltet.

Der Einsatz digitaler Technologien ist mit erheblichen Chancen zur Verbesserung der Lebensverhältnisse verbunden. Zugleich birgt er aber ernstzunehmende Risiken, die sich unter anderem auch auf die Privatheit beziehen. Zu den meist grundsätzlich positiv bewerteten Anwendungen gehören beispielsweise neue Kommunikationswege, veränderte Mobilitätsformen, zusätzliche Dienstleistungen sowie erweiterte Forschungsmöglichkeiten in Wissenschaft, Medizin und Technik.

Wesentliches Kennzeichen der Digitalisierung sind ständig steigende Datenmengen. Durch Analysen von Daten, insbesondere durch deren Verknüpfung und Vernetzung mithilfe von Verfahren des Maschinellen Lernens, können Zusammenhänge erkannt werden, welche weit über das Wahrnehmungs- und Urteilsvermögen des einzelnen Menschen hinausgehen. Jedoch steigen auch die Risiken für die Privatsphäre jedes einzelnen Menschen mit der zunehmenden

Menge an privaten Daten, die mithilfe digitaler Technologien erzeugt und ausgewertet werden: Die Offenlegung weiter Teile des privaten Lebens und Handelns kann soziale Kontrollmöglichkeiten erweitern sowie zu subtiler oder offener Diskriminierung führen. Auch eine nicht oder nur begrenzt wahrnehmbare Steuerung individuellen oder gesellschaftlichen Verhaltens bis hin zur Manipulation sind hierdurch möglich. Risiken bestehen zudem aufgrund einer erleichterten Überwachung durch private und staatliche Akteure.

Seine Tiefe und sein Umfang machen den digitalen Wandel zu einer gesamtgesellschaftlichen Aufgabe von höchster Bedeutung. Staat und Gesellschaft stehen damit vor großen Herausforderungen: Die positiven Entwicklungsmöglichkeiten durch die Digitalisierung sind offen zu halten und zu unterstützen, während zugleich entstehenden Risiken vorgebeugt werden muss und Gefahren abzuwehren sind.

Die Digitalisierung hat sich in den letzten Jahrzehnten weitgehend unreguliert und unkontrolliert entwickelt. Dies hat in manchen Anwendungsbereichen zu einem digitalen „Wilden Westen“ geführt, in dem einige wenige profitieren. Dies schränkt Rechte und Freiräume der Nutzer ein. Mit der vorliegenden Stellungnahme möchten die Akademien verschiedene Handlungsoptionen auf technischer und regulatorischer Ebene aufzeigen, um auch in Zeiten zunehmender Digitalisierung den Schutz der Privatsphäre zu realisieren.

Der Schutz der Rechte der Nutzerinnen und Nutzer sowie ihrer Privatsphäre ist dabei aber nicht als Hemmnis für wirtschaftliche Entwicklung und 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.

Herausforderungen beim Schutz der Privatheit

Der Schutz der Privatheit berührt auch Gemeinwohlziele wie zum Beispiel individuelle und kollektive Selbstbestimmung, Persönlichkeitsschutz, Chancengerechtigkeit, Sicherheit, Schutz vor Manipulation und Diskriminierung. Diese Freiheitsrechte können durch den Einsatz digitaler Techniken, wie Big-Data-Anwendungen oder Maschinelles Lernen, vonseiten privater und hoheitlicher Akteure zur Auswertung und Verknüpfung großer Datenmengen erheblich beeinträchtigt werden. Die Gewährleistung von Freiheit ist aber eine zentrale Aufgabe des demokratischen Rechtsstaates.

Der Einsatz digitaler Technologien stellt die Rechtsordnung vor eine zentrale Frage: Inwieweit können die vorhandenen rechtlichen Regeln den geschützten Bereich der Privatheit weiterhin aufrechterhalten? Dabei sind neben dem Schutz des Einzelnen gegenüber staatlichen Instanzen auch ausreichende Schutzmöglichkeiten der Menschen gegenüber den Unternehmen zu gewährleisten, durch die die digitale Transformation wesentlich erfolgt.

Erschwert wird der Einsatz von Recht grundsätzlich dadurch, dass die neuen Technologien Entgrenzungen mit sich bringen. Digitale Technologien und deren Infrastrukturen, eingesetzte Geschäftsmodelle und die mit digitalisierter Technik erbrachten Dienste sind nicht regional begrenzt, sondern häufig transnational oder global verfügbar. Damit stellen sie das Recht, das meist mithilfe von Grenzziehungen arbeitet, vor besondere Herausforderungen.

In wirtschaftlicher Hinsicht haben die grenzüberschreitenden Möglichkeiten der digitalen Transformation den Aufbau globaler Machtpositionen erleichtert. Einige wenige Konzerne haben es geschafft, in wichtigen Teilmärkten globale Oligopole zu bilden und immer weitere Marktsegmente zu besetzen. Dies kann u. a. zu Marktverschließungen und damit einer Unterbindung von Wettbewerb führen. In Bezug auf das grundsätzlich einschlägige Kartellrecht sind deshalb weitergehende, nicht marktbezogene Regelungen erforderlich, die auch die Durchsetzung von Gemeinwohlzielen berücksichtigen.

Ein weiteres Problem ist der erhebliche Mangel an Transparenz beim Einsatz digitaler Techniken und bei der Handhabung der entsprechenden Geschäftsmodelle. Häufig ist nicht bekannt, welche Daten Unternehmen generieren, mit anderen Daten verknüpfen, in weitere Geschäftsbereiche übertragen oder an fremde Unternehmen weitergeben. Weder der Öffentlichkeit noch den zuständigen Kontrollbehörden ist hinreichend bekannt, in welcher Weise und mit welchen Zielen Unternehmen Big Data und darauf bezogene Analytik nutzen oder wie deren maschinelle Lernalgorithmen konzipiert sind. All dies erschwert die Setzung, Anwendung und Kontrolle von Recht. Erste Schritte im Hinblick auf eine europaweit einheitliche Etablierung von Datenschutzstandards wurden mit der EU-Datenschutz-Grundverordnung (EU-DSGVO) unternommen.

Im Folgenden werden darüberhinausgehende Handlungsoptionen in ökonomisch und gesellschaftlich relevanten Feldern skizziert. Die teils regulatorischen, teils technischen Vorschläge sollen aufzeigen, dass es möglich ist, den Herausforderungen der Digitalisierung für die Privatheit des Einzelnen und für die freie, demokratische Gesellschaft zu begegnen. Da von der Digitalisierung vielfach 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 Umsetzung der aufgezeigten Möglichkeiten ist eine Herausforderung, die sowohl national als auch international zu bewältigen ist und trans- und internationaler Kooperation bedarf.

Handlungsfelder und Handlungsoptionen

A. Ökonomisch relevante Handlungsfelder

▼ 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 einfach absehbar. Frühe Regulierung kann leicht bei Unsicherheit bezüglich der Auswirkungen schädlich sein. Daher kann es sinnvoll sein, abgegrenzte kontrollierte Experimentierräume zu öffnen, in denen neue Geschäftsmodelle und Technologien zunächst ohne Eingriffe des Staates erprobt werden können.

▼ Handlungsfeld: Systemsicherheit als relevanten Wirtschaftsfaktor erkennen und Standards etablieren

(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 oder Datenkorruption entwickelt werden.

(2) *Präventives Design.* Für die Systemsicherheit ist es wesentlich, kritische Systeme und Dienste nach Maßgabe von Security by Design zu entwickeln. Dabei sollte nur Software zum Einsatz kommen, die für den Betrieb des Systems unverzichtbar ist und deren Korrektheit garantiert werden kann. 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.

(3) *Angriffsdetektion und -abwehr.* Etablierte Maßnahmen zur bestmöglichen Absicherung der Systeme und Infrastrukturen nach Stand der Technik sollten verstärkt als Standards und “Best Practices” umgesetzt werden. 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 eine Nachvollziehbarkeit und Zuordnung von Angriffen ermöglichen. Regulatorisch ist zu prüfen, ob Anreize zum Datenaustausch über registrierte Angriffe geschaffen werden sollten, die über die gesetzlichen Vorgaben für Betreiber kritischer Infrastrukturen hinausgehen. Generell gilt es, die Durchführung systematischer 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. In kritischen Anwendungsbereichen sollten zudem Sicherheitstests oder Zertifikate nachgewiesen werden. Dafür sind Standards für praxisrelevante und branchenspezifische Tests zu entwickeln. Diese Maßnahmen sollten durch die Pflicht ergänzt werden, Sicherheitsupdates für bekannt gewordene Sicherheitslücken bereitzustellen.

(6) *Sicherer Datenaustausch für Unternehmen.* Industrie-4.0-Konzepte benötigen autonome digitale Subsysteme, um unternehmens- und länderübergreifend sensible Daten miteinander auszutauschen. Hierfür sollten Plattformen ausgebaut werden, die von neutralen Institutionen betrieben werden. Dabei ist zu gewährleisten, dass nur auf die Daten zugegriffen werden kann, die im Rahmen eines definierten Kommunikationsprozesses zur Verfügung stehen müssen. Wichtig ist zudem, Verfügbarkeit und Zugang, Integrität, Vertraulichkeit sowie die zulässige Verwertung für alle Daten eindeutig zu regeln.

(7) *Nachhaltigkeit durch langfristig angelegte Grundlagenforschung zur IT-Sicherheit.* Seit Jahrzehnten gibt es in der IT-Sicherheit einen immer schneller werdenden Kreislauf von der Entdeckung eines neuen Angriffsvektors und der 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.

▼ Handlungsfeld: Unternehmen in Gestaltungsprozesse und Regulationen einbeziehen

(1) *Selbst- und Co-Regulierung.* Neben staatlichen Regulierungen können auch Selbstregulierungen der IT-Wirtschaft oder Co-Regulierungen zwischen staatlichen und privatwirtschaftlichen Akteuren zu einer verantwortungsvollen Gestaltung der Anwendungen von digitalen Technologien beitragen. Dabei können auch Institutionen hilfreich sein, die Best Practices oder Benchmarking-Systeme entwickeln.

(2) *Codes of Conduct.* Im Interesse des Verbraucher- und Datenschutzes können Verhaltensregeln (Codes of Conduct) von Verbänden der IT-Wirtschaft aufgestellt werden und ggf. auch im Zusammenwirken einzelner Unternehmen entstehen. Um das Risiko einer einseitigen Ausrichtung solcher Codes of Conduct an Unternehmensinteressen zu vermeiden, empfiehlt es sich, inhaltliche und prozedurale Mindestanforderungen festzulegen und für gesellschaftlich besonders wichtige Codes of Conduct eine Zertifizierung vorzusehen. In den Verfahren der Entwicklung der Verhaltensregeln sollten Vertreterinnen und Vertreter der Zivilgesellschaft mitwirken.

(3) *Transnationale Governance.* Angesichts der Inter- und Transnationalität vieler Bereiche der Digitalisierung ist es erforderlich, neue Konzepte und Einrichtungen einer transnationalen Governance im IT-Bereiche zu entwickeln, die auch auf Kooperation mit unterschiedlichen Akteuren 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. In letzter Konsequenz könnten hier auch standardisierte Echtzeit-Schnittstellen gefordert werden, die es erlauben, unterschiedliche Dienste miteinander zu vernetzen und so einen nutzerseitig kontrollierten Austausch von Daten über Plattformen hinweg zu implementieren. Durch eine solche Öffnung von Plattformen würden sich die Besitz- und Verfügungsrechte in Bezug auf Daten verschieben.

(2) *Regulierungsrecht zum Schutz von Gemeinwohlzwecken ausweiten.* Das bestehende Kartellrecht gilt der Sicherung der Funktionsfähigkeit der Märkte. Es hat es aber schon gegenwärtig nur begrenzt vermocht, der Disparität der Verteilung von Marktmacht und der Oligopolisierung in den IT-Teilmärkten entgegenzuwirken. Dringend geboten 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 oder durch ein neu konzipiertes Regulierungsrecht erfolgen, das Marktmacht auch insoweit begrenzt, als es im Interesse eines erweiterten Freiheitsschutzes nicht nur an ökonomischen Parametern ausgerichtet ist.

(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. Die Auswirkungen der Novelle auf die digitale Wirtschaft und die Nutzung von Big-Data-Ansätzen sollten gezielt evaluiert werden.

(4) *Verbesserungen der Rechtsdurchsetzung.* Um die Durchsetzung rechtlicher Regulationen auf dynamischen Plattformmärkten zu verbessern, sollte dem Vorschlag der Monopolkommission gefolgt werden, bei nicht eingehaltenen Verpflichtungszusagen von Unternehmen nach einem Jahr automatisch ein Abstellungs- und Bußgeldverfahren einzuleiten.

(5) *Zügiges Einschreiten unter Nutzung des Verfahrensrechts.* Einem weiteren Vorschlag der Monopolkommission folgend, wird empfohlen, Wettbewerbsbehörden zu ermächtigen, die Anordnung einstweiliger Maßnahmen in Zukunft stärker zu nutzen, um vermutetem Missbrauch entgegenzuwirken. Um zu verhindern, dass vom verstärkten Einsatz einstweiliger Maßnahmen Gefahren für Innovation ausgehen, wird die Einführung eines Testverfahrens vorgeschlagen, um zu prüfen, ob wesentliche Marktveränderungen schon innerhalb von 2 Jahren zu erwarten sind.

(6) *Systematik zum Umgang mit marktbeherrschenden Stellungen weiterentwickeln.* In Bezug auf das Erkennen missbräuchlicher Ausnutzung einer marktbeherrschenden Stellung in Plattformmärkten bedarf es weiterer Forschungsarbeiten. Hier fehlen z.T. noch die analytischen Werkzeuge, um eine solche Ausnutzung sinnvoll von effizienzerhöhendem Verhalten abzugrenzen. Auch im Hinblick auf die Abgrenzung von Märkten werden die Besonderheiten mehrseitiger Plattformen derzeit noch nicht ausreichend berücksichtigt.

B. Handlungsfelder in Bezug auf individuelle und gesellschaftliche Auswirkungen der Digitalisierung

▼ Handlungsfeld: Gesellschaftliche Maßnahmen

(1) *Zivilgesellschaftlich verankertes Forum.* Unter Einbeziehung von Akteuren aus den Bereichen Zivilgesellschaft, Wirtschaft, Technologie, Wissenschaft, Politik, Medien und Bildung sollte in den jeweiligen Handlungsfeldern eine gesellschaftspolitische Vision der zukünftigen digitalen Gesellschaft entworfen werden.

(2) *Stärkung des gesellschaftlichen Diskurses.* Um eine gesellschaftliche Verständigung über ethische Standards in Big Data, den Einsatz intelligenter Systeme in den unterschiedlichsten Lebensbereichen und über die Notwendigkeit eines wertebasierten Designs in verschiedenen Anwendungen zu fördern, bedarf es einer intensiven gesellschaftlichen Diskussion. Diese sollte durch interdisziplinäre Forschungsanstrengungen unterstützt werden, technologische, juristische und ethische Perspektiven einbeziehen und unterschiedliche wissenschaftsbasierte Szenarien entwickeln.

(3) *Bildungsoffensive.* Zur Förderung der digitalen Mündigkeit wird eine Bildungsoffensive für alle Altersklassen empfohlen. Diese sollte den Menschen Wissen vermitteln und ihnen geeignete Instrumente an die Hand geben, um ihre Digitalkompetenz an die sich beständig weiterentwickelnden Technologien und Anwendungen anzupassen und zu erweitern. Dabei muss besonderes Augenmerk darauf gerichtet werden, zu verhindern, dass ungleiche Bildungsvoraussetzungen zu einer gesellschaftlichen Spaltung in einen digital kompetenten und einen digital wenig gebildeten Gesellschaftsteil führen.

(4) *Berufsethos in der IT.* Relevanten IT-Berufsgruppen sollten ethische Perspektiven im Rahmen ihrer Ausbildung stärker vermittelt und so die Entwicklung eines Berufsethos unterstützt werden. Zudem wird empfohlen, in Unternehmen und Forschungseinrichtungen ethische Aspekte in der Produktentwicklung und Forschung zu verankern.

▼ Handlungsfeld: Transparenz und Überprüfbarkeit

(1) *Datenprovenienz.* Zu den grundsätzlichen Möglichkeiten, Kontrolle und Transparenz in der Datenverarbeitung zu verbessern, gehören die systematische und lückenlose Protokollierung der Herkunft von Daten und die darauf aufbauende Implementierung von Geschäftslogik. Durch geeignete offene Standards und Datenaustausch-Protokolle könnte dies auch system-, dienst- und anbieterübergreifend gewährleistet werden. Ziel wäre, 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 weitere 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 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. Wie sich ein solches System auch auf Sekundärdaten erweitern ließe, die durch eine Verknüpfung verfügbarer Daten entstanden sind, ist eine Frage, die noch intensiver Forschungstätigkeit bedarf.

(3) *Vorhersagbarkeit von Datenschutzrisiken.* Eine Verstärkung der 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 Modelle, die potentielle Datenschutzrisiken und vorhandene Schutzmaßnahmen einer konkreten Anwendung für den Nutzer verständlich darstellen können. Hier kann u. a. Maschinelles Lernen vielversprechende Ansätze bieten.

▼ Handlungsfeld: Ausweitung zentraler Prinzipien des Datenschutzrechts

(1) *Vielfalt der Prinzipien.* Insbesondere an den folgenden in Art. 5 DSGVO normierten datenschutzrechtlichen Prinzipien sollte festgehalten werden: Rechtmäßigkeit, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung sowie Integrität und Vertraulichkeit.

(2) *Datensparsamkeit.* Jede Datensammlung und jedweder Datenaustausch sollten sparsam sein, d. h. minimal in Bezug auf den bei der Datenerhebung und der Datenverwertung verfolgten Zweck. Dies gilt neben dem Umfang auch für die Genauigkeit der Daten. Diese sollte standardmäßig gering gehalten werden. Abweichungen vom Sparsamkeitsprinzip bedürfen einer Rechtfertigung anhand des Erhebungs- bzw. Verwendungszwecks.

(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.

(4) *Prinzip der Datensparsamkeit technisch durch strikt lokale Datenzusammenführungen umsetzen.* Mit einer nur lokalen Zusammenführung von Daten lassen sich die meisten der gewünschten Dienste, 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. 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 verpflichtend eine Zertifizierung der entsprechenden Allgemeinen Geschäftsbedingungen vorzunehmen. Diese sollte durch öffentlich anerkannte, akkreditierte Stellen vorgenommen werden, unter Einbeziehung von Verbraucherschutzverbänden. Es empfiehlt sich auch, darauf hinzuwirken, dass die rechtlichen Vorgaben als Verbot einer Koppelung der Bereitstellung der Dienste an eine Einwilligung in die Verarbeitung solcher Daten verstanden werden, die keinen inhaltlichen Bezug zu den nachgefragten Diensten haben. 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 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. 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.

(2) *Programmgesteuerte Schnittstellen* (Application programming interfaces, APIs) Anbieter sollten verpflichtet werden, ihren Nutzerinnen und Nutzern standardisierte programmgesteuerte Schnittstellen zur nachhaltigen Verwaltung ihrer persönlichen Daten anzubieten. Eine solche Standardisierung der Schnittstellen würde es Drittanbietern erlauben, unabhängige Softwaremodule zu entwickeln, welche im Auftrag des Nutzers Daten-Policies – und zwar anbieterübergreifend – umsetzen können. Dazu ist erforderlich, (a) einen geeigneten Rechtsrahmen zu schaffen, der Eigentums- und Nutzungsrechte an Daten regelt (etwa 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.

(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 bisher kaum durchgesetzt. Durch Kontroll- und Auditing-Prozesse kann die Einhaltung des Verbots einer dauerhaften 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 die informierte Entscheidung des Individuums über die Preisgabe von Informationen – eine Grundvoraussetzung der selbstbestimmten Teilnahme an der Digitalisierung – ist es erforderlich, Werkzeuge zu entwickeln, die Nutzerinnen und Nutzern zum einen Information und zum zweiten eigene Kontrolle ermöglichen. In diesem Bereich des technischen Selbstdatenschutzes müssen die wissenschaftlich-technischen 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, sind Transparenz, Erklärbarkeit und Kontrolle der zugrunde gelegten Algorithmen von besonderer Bedeutung.

(2) *Dokumentation des Einsatzes von Big Data.* Neue Verfahren des Maschinellen Lernens erlauben es neuerdings, den gemeinhin angenommenen Blackbox-Charakter nichtlinearer Lernmethoden zu überwinden. Dies ermöglicht eine effektive Überprüfung ihrer Funktionsweise durch ein faktisches Reverse Engineering. Die technischen Möglichkeiten zu einer solchen Überprüfung und Erklärung sind bereits vorhanden und ihr Einsatz könnte rechtlich geregelt 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. Die zunehmende Menge, Verfügbarkeit und Verknüpfung von Daten machen tatsächliche Anonymisierung jedoch zunehmend schwieriger. 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 gilt es jedoch auch zu bedenken, dass Datenverknüpfung und die daraus resultierende Datenbreite oft ein wesentlicher Erfolgsfaktor für den Einsatz von Maschinellem Lernen und Big-Data-Verfahren ist.

(1) *Verfahren entwickeln, die Anonymitätsgarantien ermöglichen.* Es gibt bereits verschiedene technische Verfahren, die Datenbankabfragen ermöglichen, ohne Rückschlüsse auf einzelne Personen zuzulassen. 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.

(2) *Nicht persistente Datenverknüpfungen.* Viele statistische Regularitäten lassen sich erkennen, ohne dass eine zentrale Datenbank angelegt werden müsste, welche die Anonymität des Einzelnen aufheben würde. Durch Nutzung von Daten gleichsam „im Vorübergehen“ müssen die Daten nicht gespeichert oder dauerhaft miteinander verknüpft werden, so dass eine De-Anonymisierung erschwert wird.

(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.

Fazit

Mit den dargestellten Handlungsoptionen lässt sich unsere digitale Zukunft positiv gestalten. Dabei gilt es, das Recht des Einzelnen auf Privatheit zu schützen und die freie demokratische Gesellschaft zu stärken. Es reicht nicht aus, an den guten Willen derjenigen zu appellieren, die mit digitalen Technologien Daten sammeln, auswerten und nutzen. Es bedarf vielmehr wirksamer rechtlicher Regelungen, die einerseits Innovationsspielräume offen halten, andererseits aber auch angemessenen Schutz für die Rechte und Interessen aller Betroffenen gewährleisten. Die Umsetzung dieser Möglichkeiten ist eine Herausforderung, die nicht allein im nationalen oder im EU-Raum zu bewältigen ist. Sie muss in trans- und internationaler Kooperation weltweit angegangen werden.

Mitwirkende der Arbeitsgruppe

Leitung: Prof. Dr. Klaus-Robert Müller (Institut für Softwaretechnik und Theoretische Informatik, Technische Universität Berlin); **Mitwirkende:** Prof. Dr. Michael Backes (CISPA – Helmholtz-Zentrum für Informationssicherheit), Prof. Dr. Erwin Böttinger (Hasso-Plattner-Institut für Digital Engineering GmbH und Universität Potsdam /Digital Health Center), Prof. Dr. Johannes Buchmann (Fachbereich Informatik, Technische Universität Darmstadt), Prof. Dr. Jörg Eberspächer (Technische Universität München), Prof. Anja Feldmann Ph.D. (Max-Planck-Institut für Informatik, Saarbrücken), Prof. Dr. Petra Grimm (Institut für Digitale Ethik, Hochschule der Medien, Stuttgart), Prof. Dietmar Harhoff, Ph.D. (Max-Planck-Institut für Innovation und Wettbewerb, München), Prof. Dr. Otthein Herzog (Tongji University, Shanghai, PRC, China Intelligent Urbanization Co-Creation Center), Prof. Dr. Thomas Hoeren (Institut für Informations-, Telekommunikations- und Medienrecht, Westfälische Wilhelms-Universität Münster), Prof. Dr. Wolfgang Hoffmann-Riem (Affiliate Professor für Recht und Innovation der Bucerius Law School in Hamburg), Prof. Dr. Jeanette Hofmann (Professorin für Internetpolitik an der Freien Universität Berlin), Prof. Dr. Thomas Hofmann (Institut für Maschinelles Lernen, Eidgenössische Technische Hochschule Zürich), Prof. Dr. Paul Hoyningen-Huene (Institut für Philosophie, Leibniz Universität Hannover), Prof. Dr. Jan C. Joerden (Lehrstuhl für Strafrecht, insbesondere Internationales Strafrecht und Strafrechtsvergleichung, Rechtsphilosophie, Europa-Universität Viadrina Frankfurt (Oder)), Prof. Dr. Paul J. Kühn (Institut für Kommunikationsnetze und Rechnersysteme, Universität Stuttgart), Prof. Dr. Thomas Lengauer (Max-Planck-Institut für Informatik, Saarbrücken), Prof. Dr. Volker Markl (Institut für Softwaretechnik und Theoretische Informatik, Fachgebiet Datenbanksysteme und Informationsmanagement, TU Berlin), Prof. Dr. Peter Propping † (Institut für Humangenetik, Rheinische Friedrich-Wilhelms-Universität Bonn), Prof. Dr. Helge Ritter (Technische Fakultät, Universität Bielefeld), Prof. Dr. Bernhard Schölkopf (Max-Planck-Institut für Intelligente Systeme, Tübingen), Prof. Dr. Fritz Strack (ehem. Lehrstuhl für Psychologie II, Universität Würzburg); **Redaktion:** Dr. Stefanie Westermann und Dr. Elke Witt (Nationale Akademie der Wissenschaften Leopoldina)

Kontakt:
Dr. Elke Witt
Nationale Akademie der Wissenschaften Leopoldina
Abteilung Wissenschaft – Politik – Gesellschaft
Tel: +49(0)345 472 39 867
E-Mail: politikberatung@leopoldina.org

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.

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