Gutachten der Datenethikkommission

Kurz-
fassung

daten
ethik
kommission

Gutachten der Datenethikkommission

daten
ethik
kommission

Inhaltsverzeichnis

Die Langfassung des Gutachtens kann im Internet unter www.datenethikkommission.de heruntergeladen werden.

Ausschließlich zum Zweck der besseren Lesbarkeit wird im vorliegenden Gutachten der Datenethikkommission auf die geschlechtsspezifische Schreibweise verzichtet. Alle personenbezogenen Bezeichnungen sind geschlechtsneutral zu verstehen.

Leitgedanken

Die Digitalisierung verändert unsere Gesellschaft tiefgreifend. Neuartige datenbasierte Technologien können für das Leben des Einzelnen und das gesellschaftliche Zusammenleben Nutzen stiften, die Produktivität der Wirtschaft steigern, zu mehr Nachhaltigkeit und zu grundlegenden Fortschritten in der Wissenschaft beitragen. Gleichzeitig zeigen sich jedoch auch Risiken der Digitalisierung für grundlegende Rechte und Freiheiten. Es stellen sich damit zahlreiche ethische und rechtliche Fragen, in deren Mittelpunkt die gewünschte Rolle und die Gestaltung der neuen Technologien stehen. Wenn der digitale Wandel dem Wohl der gesamten Gesellschaft dienen soll, müssen sich Gesellschaft und Politik mit der Gestaltung datenbasierter Technologien einschließlich der Künstlichen Intelligenz (KI) befassen.

Die Bundesregierung hat am 18. Juli 2018 die Datenethikkommission (DEK) eingesetzt. Sie erhielt den Auftrag, innerhalb eines Jahres ethische Maßstäbe und Leitlinien sowie konkrete Handlungsempfehlungen für den Schutz des Einzelnen, die Wahrung des gesellschaftlichen Zusammenlebens und die Sicherung und Förderung des Wohlstands im Informationszeitalter zu entwickeln. Dazu hat die Bundesregierung der DEK Leitfragen an die Hand gegeben, die sich auf die drei Themenfelder Algorithmenbasierte Prognose- und Entscheidungsprozesse (ADM), KI und Daten konzentrieren. Aus Sicht der DEK ist allerdings KI lediglich eine besondere Ausprägung algorithmischer Systeme und teilt viele ethisch und rechtlich relevante Eigenschaften mit anderen Arten solcher Systeme, weshalb die DEK ihre Ausführungen auf **Daten** und **algorithmische Systeme** allgemein bezieht.

Die DEK hat sich für ihr Gutachten an den folgenden **Leitgedanken** orientiert:

- Menschenzentrierte und werteorientierte Gestaltung von Technologie
- Förderung digitaler Kompetenzen und kritischer Reflexion in der digitalen Welt
- Stärkung des Schutzes von persönlicher Freiheit, Selbstbestimmung und Integrität
- Förderung verantwortungsvoller und gemeinwohlverträglicher Datennutzungen
- Risikoadaptierte Regulierung und wirksame Kontrolle algorithmischer Systeme
- Wahrung und Förderung von Demokratie und gesellschaftlichem Zusammenhalt
- Ausrichtung digitaler Strategien an Zielen der Nachhaltigkeit
- Stärkung der digitalen Souveränität Deutschlands und Europas

1

Allgemeine ethische und rechtliche Grundsätze und Prinzipien

Der Mensch ist moralisch verantwortlich für sein Handeln – er kann der moralischen Dimension nicht entkommen. Welche Ziele er verfolgt, welche Gründe er dafür hat und welche Mittel er einsetzt, liegt in seiner Verantwortung. Bei der Gestaltung unserer technologisch geprägten Zukunft ist dieser Dimension sowie der gesellschaftlichen Bedingtheit des menschlichen Handelns stets Rechnung zu tragen. Dabei gilt unverrückbar, dass Technik dem Menschen dient und nicht der Mensch der Technik unterworfen wird. Dieses **Verständnis vom Menschen** liegt unserer Verfassungsordnung zugrunde und steht in der Tradition der europäischen Kultur- und Geistesgeschichte.

Durch digitale Technologien hat sich unser ethischer Ordnungsrahmen im Sinne der grundlegenden Werte, Rechte und Freiheiten, wie sie in der deutschen Verfassung und in der europäischen Charta der Grundrechte verankert sind, nicht verändert. Diese Werte, Rechte und Freiheiten erfordern angesichts neuer Herausforderungen jedoch eine erneute Vergewisserung und neue Abwägungen. Die folgenden ethischen und rechtlichen Grundsätze und Prinzipien hält die DEK vor diesem Hintergrund für gesellschaftlich anerkannte und unverzichtbare Handlungsmaßstäbe:

Die Würde des Menschen
Die Würde des Menschen, die für den unbedingten Wert jedes menschlichen Lebewesens steht, verbietet etwa die digitale Totalvermessung des Individuums ebenso wie seine Herabwürdigung durch Täuschung, Manipulation oder Ausgrenzung.

Selbstbestimmung
Die Selbstbestimmung ist elementarer Ausdruck von Freiheit und schließt die informationelle Selbstbestimmung mit ein. Wird der Mensch selbstbestimmter Akteur in der Datengesellschaft, kann von „digitaler Selbstbestimmung“ gesprochen werden.

Privatheit
Das Recht auf Privatheit dient der Wahrung der Freiheit und der Integrität der persönlichen Identität. Sie kann durch umfassende Erhebung und Auswertung von Daten bis hin in die intimsten Bereiche bedroht sein.

Sicherheit
Die körperliche und emotionale Sicherheit des Menschen und die Sicherheit der Umwelt schützen hochrangige Güter. Sicherheit zu gewährleisten stellt hohe Anforderungen beispielsweise in der Mensch-Maschine-Interaktion oder bezüglich der Resilienz von Systemen gegenüber Angriffen und missbräuchlicher Verwendung.

Demokratie

Digitale Technologien sind systemrelevant für die Entfaltung der Demokratie. Sie ermöglichen neue Formen der politischen Beteiligung, können aber auch Gefahren im Hinblick auf Manipulation und Radikalisierung mit sich bringen.

Gerechtigkeit und Solidarität

Angesichts der massiven daten- und technologieinduzierten Anhäufung von Macht und neuen Gefahren von Ausgrenzung und Diskriminierung ist die Gewährleistung von Zugangs- und Verteilungsgerechtigkeit eine dringliche Aufgabe. Digitalisierung sollte gesellschaftliche Teilhabe unterstützen und damit den sozialen Zusammenhalt fördern.

Nachhaltigkeit

Digitale Entwicklung steht auch im Dienste nachhaltiger Entwicklung. Digitale Technologien sollten dazu beitragen, ökonomische, ökologische und soziale Nachhaltigkeitsziele zu verwirklichen.

Ethik geht nicht im Recht auf, d. h. nicht alles, was ethisch relevant ist, kann und sollte rechtlich reguliert werden, und umgekehrt gibt es Aspekte rechtlicher Regulierung, die rein pragmatisch motiviert sind. Das Recht muss aber mögliche ethische Implikationen stets reflektieren und ethischen Ansprüchen genügen. Die DEK ist der Ansicht, dass **ethische Grundsätze und Prinzipien rechtliche Regulierung nicht entbehrlich machen können**. Dies ist insbesondere dort der Fall, wo angesichts der Grundrechtsrelevanz eine Entscheidung des demokratisch legitimierten Gesetzgebers notwendig ist. Dies legt zudem die Grundlage dafür, dass Bürger, Unternehmen und Institutionen auf eine ethisch ausgerichtete gesellschaftliche Transformation vertrauen können. **Regulierung soll gleichwohl technologische und soziale Innovationen sowie eine dynamische Marktentwicklung nicht blockieren.** Allzu starre und detaillierte Gesetze können Handlungsspielräume einschränken und bürokratischen Aufwand auf eine Weise erhöhen, dass innovative Prozesse in Deutschland der Geschwindigkeit der internationalen technologischen Entwicklungen nicht mehr folgen können.

Das Recht ist allerdings nur eines von mehreren Formaten, um ethische Prinzipien zu implementieren. Die Komplexität und Dynamik von Datenökosystemen erfordert das **Zusammenwirken verschiedener Governance-Instrumente** auf unterschiedlichen Ebenen (Mehr-Ebenen-Governance). Diese Instrumente umfassen neben rechtlicher Regulierung und Standardisierung verschiedene Formen der Ko- oder Selbstregulierung. Ferner kann Technik und ihr Design selbst als Governance-Instrument genutzt werden. Das Gleiche gilt für Geschäftsmodelle und Möglichkeiten ökonomischer Lenkung. In einem weiteren Sinne gehören zur Governance auch bildungs- und forschungspolitische Entscheidungen. Jedes der genannten Governance-Instrumente muss nicht nur national, sondern gerade auch **europäisch und international** gedacht werden.

Aus Sicht der DEK sind die Leitfragen der Bundesregierung aus zwei verschiedenen Perspektiven formuliert, einer primär auf Daten fokussierten Perspektive **(„Daten-Perspektive“)** und einer primär auf algorithmische Systeme fokussierten Perspektive **(„Algorithmen-Perspektive“)**. Bei den beiden Perspektiven handelt es sich weder um miteinander konkurrierende Sichtweisen noch um verschiedene Seiten ein- und derselben Medaille, sondern um **sich wechselseitig ergänzende und bedingende ethische Diskurse**, welche sich typischerweise auch in unterschiedlichen Governance-Instrumenten, einschließlich unterschiedlicher Rechtsakte, widerspiegeln.

2

Daten

Die **Daten-Perspektive** richtet die Sicht auf die digitalen Daten, die zum Maschinellen Lernen, als Datenbasis für algorithmisch geprägte Entscheidungen und für eine Fülle weiterer Zwecke verwendet werden. Sie betrachtet Daten vor allem im Hinblick auf deren Herkunft sowie auf die möglichen Auswirkungen der Datenverarbeitung auf bestimmte Akteure, die mit Kontext und Bedeutungsgehalt der Daten zu tun haben, sowie auf die Gesellschaft. Aus ethischer wie aus rechtlicher Sicht geht es einerseits um **objektive Anforderungen** an den Umgang mit Daten, noch mehr aber typischerweise um **subjektive Rechte**, welche Akteure gegenüber einem bestimmten anderen Akteur oder auch gegenüber jedermann geltend machen können. Eine zentrale Unterscheidung ist diejenige zwischen personenbezogenen und nicht personenbezogenen Daten, welche über die Anwendbarkeit des Datenschutzrechts entscheidet.

Allgemeine Anforderungen an den Umgang mit Daten

Zu den objektiven Anforderungen an jede verantwortungsvolle Nutzung von Daten gehören nach Auffassung der DEK die folgenden datenethischen Grundsätze:

- **Vorausschauende Verantwortung:** Bei der Sammlung, Verarbeitung und Weitergabe von Daten müssen mögliche Auswirkungen auf Einzelne oder die Allgemeinheit unter Berücksichtigung künftiger Akkumulations-, Netzwerk- und Skaleneffekte, technologischer Möglichkeiten und Akteurskonstellationen abgeschätzt werden.

- **Achtung der Rechte beteiligter Personen:** Akteure, die an der Generierung von Daten beteiligt waren – sei es als Subjekt der Information, sei es in einer anderen Rolle –, können Rechte in Bezug auf diese Daten zustehen, die zu achten sind.

- **Wohlfahrt durch Nutzen und Teilen von Daten:** Daten können als nicht-rivales Gut vervielfältigt und parallel von vielen Akteuren zu vielen verschiedenen Zwecken genutzt werden und damit das Gemeinwohl fördern.

- **Zweckadäquate Datenqualität:** Ein verantwortungsvoller Umgang mit Daten setzt die Sicherstellung einer dem jeweiligen Zweck angemessenen Datenqualität voraus.

- **Risikoadäquate Informationssicherheit:** Daten sind anfällig gegenüber Ausspähung und Verfälschung von außen und können, in andere Hände gelangt, nur schwer zurückgeholt werden. Es bedarf daher eines dem jeweiligen Risikopotenzial angemessenen Maßes an Informationssicherheit.

- **Interessenadäquate Transparenz:** Derjenige, der Daten als Verantwortlicher verarbeitet, muss bereit und in der Lage sein, dafür Rechenschaft abzulegen. Dies erfordert ein angemessenes Maß an Transparenz und Dokumentation des Handelns und ggf. auch entsprechende Haftungsregelungen.

Datenrechte und korrespondierende Datenpflichten

Um sich als Akteure in der Datengesellschaft selbstbestimmt bewegen zu können, bedürfen Personen subjektiver Rechte, die ihnen gegenüber anderen Akteuren zustehen. Dies betrifft in erster Linie die Rechte eines jeden Menschen in Bezug auf seine **personenbezogenen Daten**, die sich aus dem grundrechtlich verbürgten Recht auf informationelle Selbstbestimmung ableiten und durch das geltende Datenschutzrecht gewährleistet werden. Digitale Selbstbestimmung umfasst darüber hinaus auch die selbstbestimmte wirtschaftliche Verwertung der eigenen Datenbestände sowie den selbstbestimmten Umgang mit **nicht-personenbezogenen Daten**, die etwa

durch den Wirkbetrieb eigener Geräte generiert werden. Nach Auffassung der DEK gilt ein Recht auf digitale Selbstbestimmung im Grundsatz auch für Unternehmen und **juristische Personen** und – zumindest in Ansätzen – für Gruppen von Personen (Kollektive).

Vielfach tragen unterschiedliche Akteure in unterschiedlichen Rollen zur Generierung von Daten bei – sei es als Subjekt der Information, sei es als Eigentümer einer datengenerierenden Vorrichtung, sei es in einer anderen Rolle. Ein solcher Beitrag zur Generierung von Daten sollte nach Auffassung der DEK aber nicht zu exklusiven Eigentumsrechten an Daten führen, sondern vielmehr gegebenenfalls zu Datenrechten in der Form spezieller **Mitsprache- und Teilhaberechte** eines Akteurs, mit denen korrespondierende Pflichten anderer Akteure einhergehen. Anerkennung und Ausgestaltung solcher Datenrechte eines Akteurs hängen von den folgenden allgemeinen Faktoren ab:

a) Umfang und Art des **Beitrags dieses Akteurs zur Datengenerierung**;

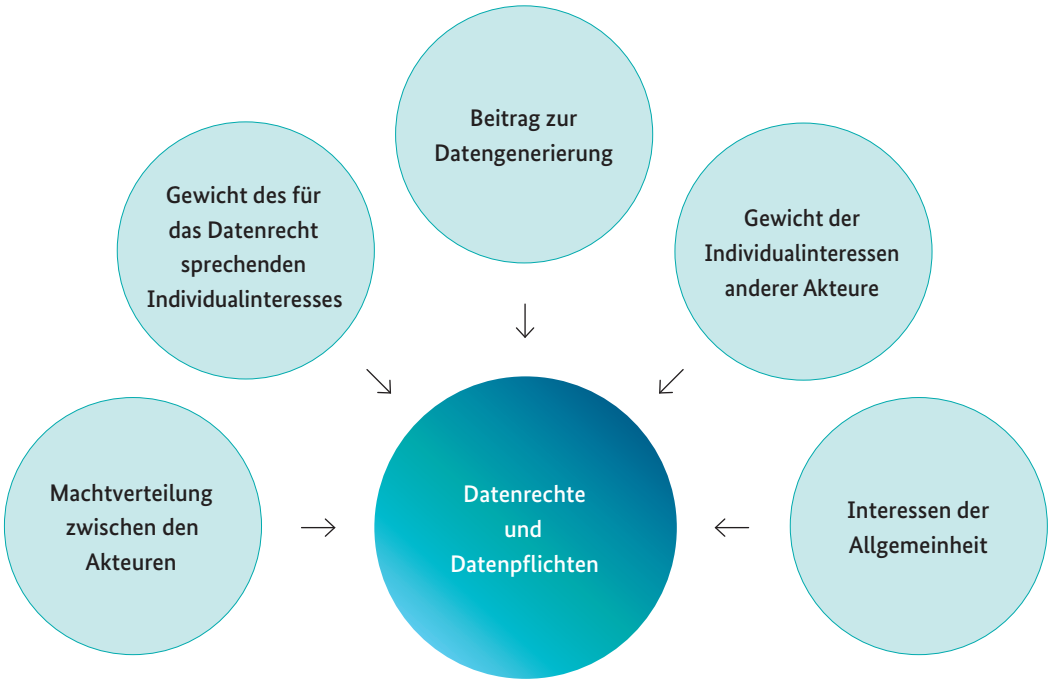
b) **Gewicht seines Individualinteresses** an der Gewährung des Datenrechts;

c) Gewicht der ggf. **konfligierenden Individualinteressen** desjenigen Akteurs, dem gegenüber das Datenrecht geltend gemacht wird, oder Dritter, unter Berücksichtigung von Ausgleichsmöglichkeiten (z. B. Schutzmaßnahmen, Vergütung);

d) **Interessen der Allgemeinheit**; und

e) **Machtverteilung** zwischen den Akteuren.

Abbildung 1:
Faktoren für die Ausgestaltung von Datenrechten und Datenpflichten



In ihrer Zielrichtung können Datenrechte insbesondere gerichtet sein auf

- eine **Unterlassung** der Datennutzung (bis hin zur Löschungspflicht);
- eine **Korrektur** von Daten;
- **Zugang** zu Daten (bis hin zu Portabilität); oder
- wirtschaftliche **Teilhabe**.

Für jede dieser Ausprägungen gelten jeweils eigene **Konkretisierungen**. Dabei kommt es nach Auffassung der DEK etwa bei Unterlassungs-Verlangen maßgeblich auf das Schädigungspotenzial einer Datennutzung sowie auf die Umstände an, unter denen der Beitrag zur Datengenerierung geleistet wurde. Auch für Korrektur-Verlangen kann das Schädigungspotenzial relevant sein, doch sind die Anforderungen geringer. Bei Zugangs-Verlangen eines Akteurs gilt ein abgestuftes Spektrum berechtigter Zugangsinteressen, die insbesondere in bestehenden Wertschöpfungssystemen zum Tragen kommen. Eigenständige Rechte einer Person auf wirtschaftliche Teilhabe an der Wertschöpfung, die andere mit Daten betreiben, kommen dagegen nur unter extrem engen Voraussetzungen in Betracht. Die **Betroffenenrechte** der Datenschutz-Grundverordnung (DSGVO) sind eine besonders wichtige und – weil einheitlich an der Qualifikation von Daten als personenbezogen anknüpfend – in gewisser Weise typisierte Ausprägung dieser Grundsätze speziell zum Schutz derjenigen natürlichen Person, auf die sich die Information bezieht.

Unter Berücksichtigung dieser Grundsätze gelangt die DEK zusammenfassend zu den folgenden zentralen Handlungsempfehlungen:

Anforderungen an die Nutzung personenbezogener Daten

1

Die DEK empfiehlt **Maßnahmen gegen ethisch nicht-vertretbare Datennutzungen**. Dazu gehören etwa Totalüberwachung, die Integrität der Persönlichkeit verletzende Profilbildung, gezielte Ausnutzung von Vulnerabilitäten, sog. Addictive Designs und Dark Patterns, dem Demokratieprinzip zuwiderlaufende Beeinflussung politischer Wahlen, Lock-in und systematische Schädigung von Verbrauchern sowie viele Formen des Handels mit personenbezogenen Daten.

2

Sowohl das Datenschutzrecht als auch die übrige Rechtsordnung (u. a. Zivilrecht, Lauterkeitsrecht) enthalten bereits eine Fülle von Instrumenten, die gegen derartige Datennutzungen eingesetzt werden können. Gemessen an Breitenwirkung und Schädigungspotenzial werden diese Instrumente indessen bislang nicht in ausreichender Weise genutzt – insbesondere gegenüber marktmächtigen Unternehmen. Dieses **Vollzugsdefizit** hat verschiedene Ursachen, die es systematisch anzugehen gilt.

3

Neben der Schärfung des Bewusstseins bei handelnden Akteuren (z. B. Aufsichtsbehörden) für die bereits bestehenden Möglichkeiten ist dringend eine **Konkretisierung und punktuelle Verschärfung des geltenden Rechtsrahmens** angezeigt. Dazu gehören etwa eine spezielle Normierung von datenspezifischen Klauselverboten, Schutz- und Treuepflichten, Deliktstatbeständen und unlauteren Geschäftspraktiken sowie die Schaffung eines weitaus konkreteren Rechtsrahmens für Profilbildungen und Scoring wie auch für den Datenhandel.

4

Um die Wirkungskraft der Aufsichtsbehörden zu erhöhen, bedürfen diese einer weitaus besseren personellen und sachlichen Ausstattung. Sofern es nicht gelingt, die Abstimmung unter den deutschen Datenschutzaufsichtsbehörden zu verstärken und zu formalisieren und so die einheitliche und kohärente Anwendung des Datenschutzrechts zu gewährleisten, ist eine **Zentralisierung der Datenschutzaufsicht für den Markt** in einer – mit einem weiten Mandat ausgestatteten und eng mit anderen Fachaufsichtsbehörden kooperierenden – Behörde auf Bundesebene zu erwägen. Die Zuständigkeit der Landesdatenschutzbehörden für den öffentlichen Bereich soll hingegen unangetastet bleiben.

5

Die Anerkennung von **„Dateneigentum“** im Sinne eines dem Sacheigentum oder dem geistigen Eigentum nachgebildeten Ausschließlichkeitsrechts an Daten würde nach Auffassung der DEK bestehende Probleme nicht lösen und stattdessen eine Reihe neuer Probleme schaffen. Sie wird daher **nicht empfohlen**. Die DEK empfiehlt auch nicht die Anerkennung genereller wirtschaftlicher Verwertungsrechte an personenbezogenen Daten, wie sie etwa durch Verwertungsgesellschaften geltend gemacht werden könnten.

6

Wenngleich die plakative Bezeichnung zur allgemeinen Bewusstseinsbildung beigetragen hat, plädiert die DEK dafür, **von der Bezeichnung von Daten als „Gegenleistung“ abzusehen**. Unabhängig von der künftigen Auslegung des sog. Koppelungsverbots durch die Aufsichtsbehörden und den EuGH fordert die DEK, dass Verbrauchern jeweils **zumutbare Alternativen** gegenüber der Freigabe von Daten zur auch kommerziellen Nutzung angeboten werden müssen (z. B. entsprechend ausgestaltete **Bezahlmodelle**).

7

Die Verwendung von Daten zur **personalisierten Risikoeinschätzung** (z. B. im Rahmen von Telematiktarifen bei bestimmten Versicherungen) sollte an **enge Voraussetzungen** geknüpft werden. So darf die Datenverarbeitung beispielsweise nicht den Kern privater Lebensführung betreffen, es muss ein klarer ursächlicher Zusammenhang zwischen Daten und Risiko vorliegen, und die Preisdifferenz zwischen personalisiertem und nicht personalisiertem Tarif sollte im Einzelnen noch festzulegende Prozentwerte nicht überschreiten. Weitere Anforderungen betreffen Transparenz, Nichtdiskriminierung und den Schutz dritter Personen.

8

Die DEK empfiehlt der Bundesregierung, Fragen rund um den **„digitalen Nachlass“** mit dem Urteil des BGH von 2018 nicht als erledigt anzusehen. Die praktisch lückenlose Aufzeichnung von digital geführter Kommunikation, die in vielen Fällen an die Stelle des flüchtig gesprochenen Wortes tritt, und ihre Aushändigung an Erben bedeutet eine neue Dimension von Gefährdung für die Privatheit. Ihr sollte mit einer Reihe von Maßnahmen begegnet werden, welche neue Pflichten von Diensteanbietern, Qualitätssicherung bei Angeboten digitaler Nachlassplanung sowie nationale Regelungen zum postmortalen Datenschutz umfassen.

9

Die DEK empfiehlt der Bundesregierung, die Sozialpartner einzuladen, ausgehend von den bereits in Tarifverträgen bestehenden Beispielen guter Übung eine gemeinsame Linie für gesetzliche Konkretisierungen des **Beschäftigtendatenschutzes** zu entwickeln. Dabei sollten auch die Belange von Personen in unüblichen Beschäftigungsformen berücksichtigt werden.

10

Mit Blick auf die Vorteile eines **digitalisierten Gesundheitswesens** spricht sich die DEK für einen raschen Ausbau digitaler Infrastrukturen innerhalb des Gesundheitssektors aus. Der qualitative und quantitative Ausbau digitalisierter Versorgungsmaßnahmen sollte die informationelle Selbstbestimmung des Patienten stärken. Hierzu gehört der partizipative Auf- und Ausbau der elektronischen Patientenakte (ePA) sowie die Weiterentwicklung von Verfahren zur Prüfung und Bewertung digitaler Gesundheitsanwendungen im ersten und zweiten Gesundheitsmarkt.

11

Die DEK fordert, dem erheblichen Vollzugsdefizit des geltenden Rechts betreffend den **Schutz von Kindern und Jugendlichen** im digitalen Raum abzuhelfen. Insbesondere sollten Technologien – einschließlich eines effektiven Identitätenmanagements – sowie Standardoptionen entwickelt und verpflichtend vorgesehen werden, welche einen zuverlässigen Schutz der Kinder und Jugendlichen gewährleisten und zugleich familienadäquat sind, indem sie Erziehungsberechtigte weder überfordern noch eine übermäßige Überwachung im privaten Bereich ermöglichen oder gar hierzu animieren.

12

Was den Umgang mit Daten **pflege- und schutzbedürftiger Menschen** betrifft, sollte für professionelle Akteure im Pflegebereich durch Standards und Leitlinien mehr Rechtssicherheit geschaffen werden. Zugleich ist eine gesetzliche Klarstellung zu erwägen, dass – soweit eine Datenverarbeitung auf die Einwilligung des pflege- und schutzbedürftigen Menschen gestützt werden muss – in Patientenverfügungen auch bestimmte Dispositionen in Bezug auf die Datenverarbeitung (z. B. für den Fall der dauernden Einwilligungsunfähigkeit infolge von Demenz) getroffen werden können.

13

Die DEK empfiehlt, eine Reihe verbindlicher Vorgaben für **datenschutzfreundliches Design von Produkten und Dienstleistungen** einzuführen und damit die an Verantwortliche im Sinne der DSGVO gerichteten Vorgaben von Datenschutz „by design“ und „by default“ bereits auf der Ebene der Hersteller wie auch der Diensteanbieter wirksam werden zu lassen. Dies betrifft insbesondere Vorgaben für Verbraucherendgeräte. In diesem Zusammenhang sind auch einheitliche Bildsymbole (Piktogramme) einzuführen, die dem Verbraucher eine informierte Kaufentscheidung ermöglichen.

14

Ferner bedarf es einer Reihe weiterer Maßnahmen auf verschiedenen Ebenen, um für Hersteller effektive **Anreize zur Implementierung eines datenschutzfreundlichen Designs** zu schaffen. Neben wirksamen Rechtsbehelfen entlang der Vertriebskette, mit deren Hilfe Hersteller mit in die Verantwortung für unzureichenden Datenschutz „by design“ und „by default“ genommen werden können, ist insbesondere an Vorgaben in Ausschreibungsbedingungen und Beschaffungsrichtlinien für die öffentliche Hand sowie an Bedingungen bei Förderprogrammen zu denken. Das Gleiche gilt für datenschutzfreundliche **Methoden der Produktentwicklung**, einschließlich des Trainierens algorithmischer Systeme.

15

Trotz des berechtigten Fokus auf Datenschutz natürlicher Personen darf der **Schutzbedarf von Unternehmen und juristischen Personen** nicht in den Hintergrund treten. Durch die umfassende Verknüpfbarkeit von Einzeldaten kann ein lückenloses Bild interner Betriebsabläufe entstehen und in die Hände von Konkurrenten, Verhandlungspartnern, Übernahmeinteressenten usw. gelangen. Dies stellt aufgrund umfangreicher Datenflüsse in Drittstaaten u. a. eine Gefährdung der digitalen Souveränität Deutschlands und Europas dar. Viele Handlungsempfehlungen sind daher sinngemäß auch auf die Daten juristischer Personen zu übertragen. Die DEK fordert die Bundesregierung auf, Schritte zu unternehmen, um den **datenbezogenen Schutz von Unternehmen zu verbessern**.

Verbesserung des kontrollierten Zugangs zu personenbezogenen Daten

16

Die DEK sieht in einer Datennutzung für gemeinwohlorientierte Forschungszwecke (z. B. zur Verbesserung der Gesundheitsfürsorge) enormes Potenzial, das es zum Wohle des Einzelnen und der Allgemeinheit zu nutzen gilt. Das geltende Datenschutzrecht erkennt dieses Potenzial durch eine Reihe weitreichender Privilegierungen prinzipiell an. Allerdings bestehen auch Unsicherheiten, insbesondere mit Blick auf die Reichweite des sog. Weiterverarbeitungsprivilegs sowie des Forschungsbegriffs im Zusammenhang mit der Entwicklung von Produkten. Dem muss aus Sicht der DEK durch entsprechende **gesetzliche Klarstellungen** begegnet werden.

17

Die Zersplitterung der Rechtslage, sowohl innerhalb Deutschlands als auch der EU Mitgliedstaaten untereinander, kann ein Hindernis für datengetriebene Forschung darstellen. Empfohlen wird daher eine **Harmonisierung der forschungsspezifischen Regelungen** sowohl auf Bundes- und Landesebene als auch der verschiedenen nationalen Regelungen innerhalb der EU. Auch die Einführung eines Notifizierungsverfahrens für mitgliedstaatliche Regelungen zum Forschungsdatenschutz sowie die Einrichtung einer europäischen Clearing-Stelle für grenzüberschreitende Forschungsprojekte könnte eine Erleichterung bringen.

18

Bei Forschung mit besonders sensiblen Kategorien personenbezogener Daten (z. B. Gesundheitsdaten) sollten Forschende durch **Handreichungen** zur rechtssicheren Einholung von Einwilligungen sowie durch die Förderung und gesetzliche **Anerkennung innovativer Einwilligungsmodelle** unterstützt werden. Zusätzlich zu den weiteren Entwicklungen zur Reichweite des sog. Weiterverarbeitungsprivilegs für die Forschung könnten dazu auch digitale Einwilligungsassistenten oder ein sog. Meta Consent gehören.

19

Die DEK unterstützt prinzipiell die Entwicklung in Richtung eines **„lernenden Gesundheitssystems“**, in dem die Daten aus der alltäglichen Gesundheitsversorgung systematisch und qualitätsgestützt im Sinne der evidenzbasierten Medizin genutzt werden, um die Versorgung kontinuierlich zu verbessern. Allerdings sollte flankierend, beispielsweise durch **Verwertungsverbote**, mehr Schutz vor dem erheblichen Diskriminierungspotenzial sensibler Datenkategorien geschaffen werden.

20

Im Zentrum aller Bemühungen um eine Verbesserung des kontrollierten Zugangs zu (ursprünglich) personenbezogenen Daten steht die Entwicklung von Verfahren und Standards der **Anonymisierung** und **Pseudonymisierung**. Durch rechtliche Vermutungen, dass bei Einhaltung des Standards kein Personenbezug mehr gegeben ist bzw. dass „geeignete Garantien“ für die Rechte betroffener Personen vorliegen, könnte die Rechtssicherheit deutlich verbessert werden. Diese Maßnahmen sollten flankiert werden durch strafbewehrte Verbote einer De-Anonymisierung (für den Fall, dass bei bisher anonymen Daten, etwa durch die Entwicklung der Technik, ein Personenbezug hergestellt werden kann) bzw. der Aufhebung der Pseudonymisierung jenseits eng definierter Rechtfertigungsgründe. Auch die Forschung im Bereich **synthetischer Daten** ist vielversprechend und sollte weiter gefördert werden.

21

Großes Potenzial sieht die DEK grundsätzlich auch in **innovativen Datenmanagement- und Datentreuhandsystemen**, sofern diese praxisgerecht, robust und datenschutzkonform ausgestaltet sind. Solche Modelle rangieren von rein technischen Dashboards (**Privacy Management Tools,** PMT) bis hin zu umfassenden Dienstleistungen der Daten- und Einwilligungsverwaltung (**Personal Information Management Services,** PIMS). Ziel ist die Befähigung des Einzelnen zur Kontrolle über seine personenbezogenen Daten sowie die Entlastung des Einzelnen von Entscheidungen, die ihn überfordern. Die DEK empfiehlt, Forschung und Entwicklung im Bereich von Datenmanagement- und Datentreuhandsystemen intensiv zu fördern, mahnt aber auch an, dass eine die Rechte und Interessen aller Beteiligten wahrende Entwicklung ohne eine **begleitende europäische Regulierung** nicht zu erwarten ist. Diese Regulierung müsste zentrale Funktionen absichern, ohne die Betreiber solcher Systeme nur sehr eingeschränkt tätig werden können. Andererseits geht es um den Schutz des Einzelnen vor vermeintlichen Interessenwaltern, die in Wahrheit vorrangig wirtschaftliche Eigeninteressen oder Interessen Dritter vertreten. Sofern dieser Schutz auch in der Praxis garantiert werden kann, kann Datentreuhandmodellen die Funktion einer wichtigen Schnittstelle zwischen Belangen des Datenschutzes und der Datenwirtschaft zukommen.

22

In Bezug auf das Recht auf **Datenportabilität** aus Art. 20 DSGVO empfiehlt die DEK die Erarbeitung branchenbezogener Verhaltensregeln und Standards betreffend Datenformate. Soweit Art. 20 DSGVO nicht nur Anbieterwechsel erleichtern, sondern auch den Datenzugang für andere Anbieter verbessern soll, empfiehlt sich eine sorgfältige Evaluierung, wie sich das bestehende Portabilitätsrecht auf den Markt auswirkt und wie eine zunehmende Stärkung der Marktmacht weniger Anbieter verhindert werden kann. Bevor die Ergebnisse einer solchen Evaluierung vorliegen, sollte von einer vorschnellen Erweiterung des Portabilitätsrechts, etwa auf andere als bereitgestellte Daten oder auf Portierung in Echtzeit, abgesehen werden.

23

Eine **Pflicht zur Interoperabilität bzw. Interkonnektivität** in bestimmten Sektoren – etwa bei Messenger-Diensten und sozialen Netzwerken – könnte dazu beitragen, Markteintrittsbarrieren für neue Anbieter zu senken. Für eine solche Pflicht würde sich eine asymmetrische, d. h. nach Marktmacht gestaffelte Regulierung empfehlen. Dies wäre auch eine Voraussetzung dafür, bestimmte Basisdienstleistungen der Informationsgesellschaft in Europa neu aufzubauen bzw. zu stärken.

Datenzugangsdebatten jenseits des Personenbezugs

24

Für die Entwicklung der europäischen Datenwirtschaft sieht die DEK einen zentralen Faktor im Zugang europäischer Unternehmen zu geeigneten nicht-personenbezogenen Daten in geeigneter Qualität. **Datenzugang** nutzt allerdings nur Akteuren, die ein entsprechendes Bewusstsein für die Bedeutung von Daten haben und über entsprechende Datenkompetenz verfügen, und in ganz überproportionalem Ausmaß denjenigen, bei denen bereits der größte Ausgangsbestand an Daten und die besten Dateninfrastrukturen vorhanden sind. Die DEK empfiehlt daher, bei der Diskussion um eine Verbesserung des Datenzugangs stets die genannten Faktoren gemäß dem **ASISA-Prinzip** *(Awareness – Skills – Infrastructures – Stocks – Access)* mit zu berücksichtigen.

25

Daher unterstützt die DEK die bereits auf europäischer Ebene begonnenen Maßnahmen zur Förderung von **Dateninfrastrukturen** im weitesten Sinne (z. B. Plattformen, Standards für Programmierschnittstellen und weitere Elemente, Modellverträge, EU-Unterstützungszentrum) und empfiehlt der Bundesregierung, diese weiterhin durch entsprechende Bemühungen auf nationaler Ebene zu flankieren. In diesem Zusammenhang bietet sich die Einrichtung einer Ombudsstelle auf Bundesebene an, welche bei Aushandlung von Datenzugangsvereinbarungen und bei Streitigkeiten hilft und vermittelt.

26

Die DEK sieht einen Schlüsselfaktor in einer holistisch gedachten, nachhaltigen und strategischen **Wirtschaftspolitik**, welche der Abwanderung innovativer europäischer Unternehmen bzw. deren Aufkauf durch Akteure aus Drittstaaten ebenso effektiv entgegenwirkt wie der übermäßigen Abhängigkeit von Infrastrukturen (z. B. Serverkapazitäten) in Drittstaaten. Dabei ist die richtige Balance zu finden zwischen gewollter internationaler Kooperation und Vernetzung einerseits und andererseits der entschlossenen Übernahme von Verantwortung für nachhaltige Sicherheit und Wohlfahrt in Europa vor dem Hintergrund sich wandelnder globaler Machtverhältnisse.

27

Die DEK sieht auch unter dem Blickwinkel einer Förderung der Datenwirtschaft keinen Bedarf nach der Einführung neuer Ausschließlichkeitsrechte („Dateneigentum", „Datenerzeugerrecht"), sondern empfiehlt stattdessen eine **beschränkte Drittwirkung vertraglicher Vereinbarungen** (z. B. betreffend Beschränkungen der Nutzung und Weitergabe von Daten) nach dem Vorbild des neuen europäischen Regimes zum Schutz von Geschäftsgeheimnissen. Ferner wäre es wünschenswert, wenn gesetzlich Wege aufgezeigt würden, wie europäische Unternehmen – etwa unter Einschaltung von Treuhändern – unter voller Wahrung kartellrechtlicher Belange bei der Datennutzung kooperieren können **(„Datenpartnerschaften")**.

28

In bestehenden Wertschöpfungssystemen (z. B. Produktions- und Vertriebsketten) fallen vielfach Daten an, die innerhalb wie außerhalb des Wertschöpfungssystems von enormer wirtschaftlicher Bedeutung sind. Die zwischen den einzelnen Teilnehmern eines Wertschöpfungssystems bestehenden Verträge enthalten aber häufig entweder keine bzw. eine unfaire und/oder ineffiziente Regelung des Datenzugangs, oder es fehlt ganz an einer vertraglichen Vereinbarung. Weit über die klassische „Datenwirtschaft" hinaus ist daher **Bewusstseinsbildung bei Wirtschaftstreibenden** erforderlich, die durch praktische Hilfestellungen (z. B. Modellverträge) ergänzt werden sollte.

29

Darüber hinaus regt die DEK eine **behutsame Ergänzung des geltenden Rechtsrahmens** an. Dabei sollte ein erster Schritt darin liegen, die Sonderbeziehung zwischen einer Partei, welche zur Generierung von Daten in einem Wertschöpfungssystem beigetragen hat, und der Partei, welche die Daten faktisch kontrolliert, in § 311 BGB explizit anzuführen. Unter anderem sollte die Aufnahme von Vertragsverhandlungen über ein faires und effizientes Datenzugangsregime Bestandteil einer solchen allgemeinen Treuepflicht sein. Im Übrigen sollte geprüft werden, ob darüber hinaus Maßnahmen erforderlich sind, welche von punktuellen Klauselverboten in B2B-Geschäften über ein dispositives Datenschuldrecht bis zu sektorspezifischen Datenzugangsrechten rangieren könnten.

30

Die DEK sieht großes Potenzial in **Konzepten offener Daten des öffentlichen Sektors** (Open Government Data, OGD) und empfiehlt, solche Konzepte auszubauen und zu fördern. Sie empfiehlt eine Reihe von Maßnahmen, die einen teilweise noch nicht ganz vollzogenen **Bewusstseinswandel öffentlicher Stellen** befördern und das Teilen von Daten im Rahmen von OGD-Konzepten praktisch erleichtern könnten. Dazu gehört neben der Etablierung entsprechender **Infrastrukturen** (z. B. Plattformen) auch eine Harmonisierung und punktuelle Ergänzung des derzeit zersplitterten und nicht in jeder Hinsicht konsistenten **Rechtsrahmens**.

31

Allerdings sieht die DEK auch ein schwer zu lösendes Spannungsverhältnis zwischen der Diskussion um OGD (mit Prinzipien wie „offen by default“ und „offen für alle Zwecke“) einerseits und um besseren Schutz von Geschäftsgeheimnissen und personenbezogenen Daten (mit gesetzlichen Vorgaben wie „Datenschutz by default“) andererseits. Sie plädiert dafür, in Zweifelsfällen zugunsten des staatlichen Schutzauftrags zu entscheiden, der in Bezug auf Daten, welche Einzelne oder Unternehmen dem Staat – oft nicht freiwillig – anvertraut haben (z. B. Steuerdaten), besteht. Diesem **staatlichen Schutzauftrag** ist durch eine Reihe von Maßnahmen nachzukommen, die auch technische und rechtliche Schutzvorkehrungen gegen Missbrauch umfassen.

32

In diesem Zusammenhang wird insbesondere empfohlen, für das Teilen von Daten durch den öffentlichen Sektor **Standardlizenzen und Modellkonditionen** zu entwickeln und – mindestens sektorspezifisch – deren Verwendung bindend vorzuschreiben. Diese sollten klar definierte Garantien für die Rechte betroffener Dritter enthalten. Ferner sollten sie Mechanismen vorsehen, die geeignet sind, eine gemeinwohlschädigende Nutzung der Daten ebenso zu verhindern wie eine wettbewerbsrechtlich unerwünschte Verstärkung bestehender Marktmacht oder eine Doppelbelastung des Steuerzahlers.

33

Betreffend **Konzepte offener Daten im privaten Sektor** sollte in erster Linie auf die **Ermutigung und Förderung eines freiwilligen Teilens** von Daten gesetzt werden. Dabei ist nicht nur an Infrastrukturen (z. B. Plattformen) zu denken, sondern auch an eine breite Palette möglicher Anreizstrukturen, etwa bei der Besteuerung, bei öffentlichen Ausschreibungen, bei Förderprogrammen oder bei Genehmigungsverfahren. Gesetzliche Datenzugangsrechte und korrespondierende Zugangsgewährungspflichten sollten dagegen erst in zweiter Linie in Betracht gezogen werden.

34

Insgesamt rät die DEK bei allgemeinen gesetzlichen Datenzugangsrechten zu einem behutsamen Vorgehen, idealerweise **zunächst in ausgewählten Sektoren**. Beispielsweise könnte ein Bedarf im Nachrichten-, Mobilitäts- oder Energiesektor geprüft werden. Dabei sind jeweils alle möglichen Konsequenzen einer Zugangsgewährungs- oder gar Offenlegungspflicht sorgsam zu bedenken und gegeneinander abzuwägen, angefangen von möglichen Implikationen für den Datenschutz und Schutz von Geschäftsgeheimnissen, über Folgen für Investitionsentscheidungen und die Verteilung von Marktmacht bis hin zu den strategischen Interessen deutscher und europäischer Unternehmen im Verhältnis zu Unternehmen in Drittstaaten.

35

Die DEK empfiehlt, Zugangsgewährungspflichten privater Unternehmen **zugunsten gemeinwohlorientierter Zwecke und des öffentlichen Sektors** (Business-to-Government, B2G) in Erwägung zu ziehen. Auch diesbezüglich dürfte indessen ein behutsames und sektorspezifisches Vorgehen anzuraten sein.

3

Algorithmische Systeme

Die primär auf algorithmische Systeme ausgerichtete Perspektive **(Algorithmen-Perspektive)** richtet den Blick auf die Architektur und Dynamik des datenverarbeitenden algorithmischen Systems und seine Auswirkungen auf Einzelne und die Gesellschaft. Der ethische und rechtliche Diskurs fokussiert dabei typischerweise auf die Beziehung von Mensch und Maschine und mit Blick auf Künstliche Intelligenz (KI) insbesondere auf die Automatisierung sowie auf die Verlagerung auch komplexer Handlungs- und Entscheidungsprozesse auf sog. autonome Systeme. In Abgrenzung zur Daten-Perspektive müssen die vom System betroffenen Personen nicht notwendig auch etwas mit den Daten zu tun haben, die das System verarbeitet – insbesondere können sich ethisch nicht vertretbare Auswirkungen auf Einzelne auch dann ergeben, wenn ausschließlich nicht-personenbezogene Daten genutzt wurden (z. B. für das Training eines algorithmischen Systems). Eine zentrale aktuelle Debatte, die hier zu verorten ist, ist diejenige um eine „Algorithmenkontrolle“ oder um die Haftung für KI.

Allgemeine Anforderungen an algorithmische Systeme

Die DEK unterscheidet je nach der konkreten Aufgabenverteilung zwischen menschlichem Akteur und Maschine drei unterschiedliche Stufen des Einbezugs von algorithmischen Systemen in menschliche Entscheidungen:

a) **algorithmenbasierte** Entscheidungen sind menschliche Entscheidungen, die sich auf algorithmisch berechnete (Teil-)Informationen stützen;

b) **algorithmengetriebene** Entscheidungen sind menschliche Entscheidungen, die durch die Ergebnisse algorithmischer Systeme in einer Weise geprägt werden, dass der tatsächliche Entscheidungsspielraum und damit die Selbstbestimmung des Menschen eingeschränkt werden;

c) **algorithmendeterminierte** Entscheidungen führen automatisiert zu Konsequenzen, so dass im Einzelfall keine menschliche Entscheidung mehr vorgesehen ist.

Ein verantwortungsvoller Umgang mit algorithmischen Systemen sollte sich nach Auffassung der DEK an folgenden Grundsätzen orientieren:

- **Menschenzentriertes Design:** Systeme müssen den Menschen, der die Systeme anwendet oder von ihren Entscheidungen betroffen ist, seine grundlegenden Rechte und Freiheiten, sein körperliches und emotionales Wohlbefinden, seine Kompetenzentwicklung und seine Grundbedürfnisse in den Mittelpunkt stellen.

- **Vereinbarkeit mit gesellschaftlichen Grundwerten:** Bei der Gestaltung von Systemen sind Auswirkungen gesamtgesellschaftlicher Relevanz zu berücksichtigen, insbesondere auf die demokratische Willensbildung, die Bürgernähe staatlichen Handelns, den Wettbewerb, die Zukunft der Arbeit und die digitale Souveränität Deutschlands und Europas.

- **Nachhaltigkeit:** Bei der Gestaltung und dem Einsatz algorithmischer Systeme erhalten Aspekte der Verfügbarkeit menschlicher Kompetenzen, der Partizipation, des Umweltschutzes und der nachhaltigen Ressourcenbewirtschaftung sowie des nachhaltigen wirtschaftlichen Handelns wachsende Bedeutung.

- **Qualität und Leistungsfähigkeit:** Algorithmische Systeme müssen korrekt und zuverlässig funktionieren, um die mit ihrer Hilfe verfolgten Zwecke zu erreichen.

- **Robustheit und Sicherheit:** Robuste und sichere Systemgestaltung umfasst sowohl die Sicherheit des Systems gegen Einflüsse von außen als auch den Schutz der Menschen und der Umwelt vor negativen Einflüssen durch das System.

- **Minimierung von Verzerrungen und Diskriminierung:** Die Entscheidungsmuster, die algorithmischen Systemen zugrunde liegen, dürfen keine systematischen Verzerrungen (Biases) aufweisen oder zu diskriminierenden Entscheidungen führen.

- **Transparenz, Erklärbarkeit und Nachvollziehbarkeit:** Es ist essenziell, dass sowohl die Anwender der algorithmischen Systeme deren Funktionsweise verstehen, erklären und kontrollieren können, als auch, dass die von einer Entscheidung Betroffenen genügend Informationen erhalten, um ihre Rechte angemessen wahrnehmen und die Entscheidung infrage stellen zu können.

- **Klare Rechenschaftsstrukturen:** Der Einsatz algorithmischer Systeme verlangt eine klare Zuordnung von Verantwortung und Rechenschaftspflichten einschließlich einer möglichen Haftung.

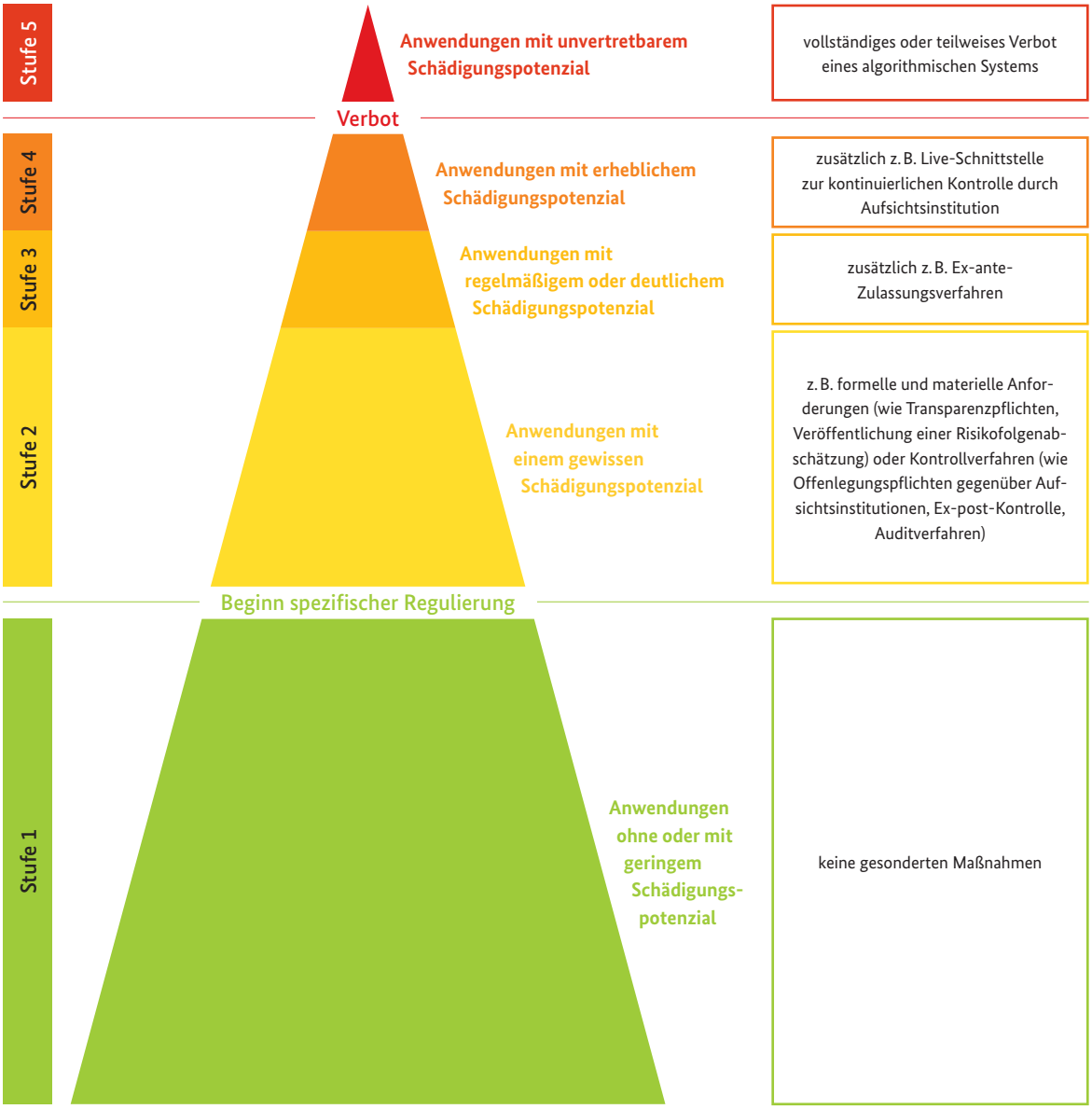
Systemkritikalität

Die konkret an ein algorithmisches System zu stellenden Anforderungen – insbesondere auch im Hinblick auf Transparenz und Kontrolle – sind abhängig von der **Systemkritikalität**. Die Systemkritikalität setzt am Schädigungspotenzial des algorithmischen Systems an. Dabei bedeutet Schädigungspotenzial die Kombination aus der **Wahrscheinlichkeit eines Schadenseintritts** und der **Schwere des zu befürchtenden Schadens**.

Die **Schwere** zu befürchtender Schäden, etwa im Falle einer Fehlentscheidung, bezieht sich auf die Wertigkeit der betroffenen Rechtsgüter und Interessen (z. B. Recht auf Privatheit, Grundrecht auf Leben und körperliche Unversehrtheit, Diskriminierungsverbot), die Höhe eines möglichen Schadens für Einzelne (einschließlich immaterieller Schäden bzw. monetär schwer zu beziffernder Nutzeneinbußen), die Zahl der Betroffenen, die Summe der potenziellen Schäden und den gesamtgesellschaftlichen Schaden, der über eine reine Summierung von Einzelschäden weit hinausgehen kann. Die **Wahrscheinlichkeit** eines Schadenseintritts hängt auch von den konkreten Systemeigenschaften ab – insbesondere von der Rolle algorithmischer Systemkomponenten im Entscheidungsprozess, der Komplexität der Entscheidung, den Wirkungen der Entscheidung und der Reversibilität der Wirkungen. Schwere und Wahrscheinlichkeit zu befürchtender Schäden können zudem abhängig sein vom staatlichen oder privaten Charakter des Handelns und – gerade in wirtschaftlichen Zusammenhängen – von der Marktmacht desjenigen Akteurs, der sich des algorithmischen Systems bedient.

Unter Berücksichtigung dieser Grundsätze gelangt die DEK zusammenfassend zu den folgenden Handlungsempfehlungen:

Abbildung 2:
Kritikalitätspyramide und risikoadaptiertes Regulierungssystem für den Einsatz algorithmischer Systeme



Empfehlung eines risikoadaptierten Regulierungsansatzes

36

Die DEK empfiehlt einen **risikoadaptierten Regulierungsansatz** für algorithmische Systeme. Er sollte auf dem Grundsatz aufbauen, dass ein steigendes Schädigungspotenzial mit wachsenden Anforderungen und Eingriffstiefen der regulatorischen Instrumente einhergeht. Für die Beurteilung kommt es jeweils auf das **gesamte sozio-technische System** an, also alle Komponenten einer algorithmischen Anwendung einschließlich aller menschlichen Akteure, von der Entwicklungsphase (z. B. hinsichtlich der verwendeten Trainingsdaten) bis hin zur Implementierung in einer Anwendungsumgebung und zur Phase von Bewertung und Korrektur.

37

Die DEK empfiehlt, die Bestimmung des Schädigungspotenzials algorithmischer Systeme für Einzelne und/oder die Gesellschaft anhand eines **übergreifenden Modells** einheitlich vorzunehmen. Dafür sollte der Gesetzgeber mit Hilfe von **Kriterien** ein Prüfschema definieren, nach welchem die Kritikalität algorithmischer Systeme auf der Grundlage der von der DEK vorgestellten allgemeinen ethischen und rechtlichen Grundsätze und Prinzipien zu bestimmen ist.

38

Regulatorische Instrumente und **Anforderungen** an algorithmische Systeme sollten u. a. Korrektur- und Kontrollinstrumente, Vorgaben für die Transparenz, die Erklärbarkeit und die Nachvollziehbarkeit der Ergebnisse sowie Regelungen zur Zuordnung von Verantwortlichkeit und Haftung für den Einsatz umfassen.

39

Die DEK erachtet es als sinnvoll, mit Blick auf das Schädigungspotenzial algorithmischer Systeme in einem ersten Schritt **fünf Kritikalitäts-Stufen** zu unterscheiden. Auf der untersten Stufe (Stufe 1) von Anwendungen ohne oder mit geringem Schädigungspotenzial besteht keine Notwendigkeit einer besonderen Kontrolle oder von Anforderungen, die über die allgemeinen Qualitätsanforderungen, welche auch für Produkte ohne algorithmische Elemente gelten, hinausgehen.

40

Bei Anwendungen mit einem **gewissen Schädigungspotenzial** (Stufe 2) kann und soll bedarfsgerechte Regulierung einsetzen, wie etwa Ex-post-Kontrollen, die Pflicht zur Erstellung und Veröffentlichung einer angemessenen Risikofolgenabschätzung, Offenlegungspflichten gegenüber Aufsichtsinstitutionen oder auch gesteigerte Transparenzpflichten sowie Auskunftsrechte für Betroffene.

41

Bei Anwendungen mit **regelmäßigem** oder **deutlichem Schädigungspotenzial** (Stufe 3) können zusätzlich Zulassungsverfahren gerechtfertigt sein. Bei Anwendungen mit **erheblichem Schädigungspotenzial** (Stufe 4) fordert die DEK darüber hinaus verschärfte Kontroll- und Transparenzpflichten bis hin zu einer Veröffentlichung der in die algorithmische Berechnung einfließenden Faktoren und deren Gewichtung, der Datengrundlage und des algorithmischen Entscheidungsmodells sowie die Möglichkeit einer kontinuierlichen behördlichen Kontrolle über eine Live-Schnittstelle zum System.

42

Bei **Anwendungen mit unvertretbarem Schädigungspotenzial** (Stufe 5) ist schließlich ein vollständiges oder teilweises **Verbot** auszusprechen.

43

Zur Umsetzung der durch die DEK vorgeschlagenen Maßnahmen empfiehlt die DEK eine Regulierung algorithmischer Systeme durch allgemeine **horizontale Vorgaben im Recht** der Europäischen Union **(Verordnung für Algorithmische Systeme, EUVAS)**. Dieser horizontale Rechtsakt sollte die zentralen Grundprinzipien für algorithmische Systeme enthalten, wie sie die DEK als Anforderungen an algorithmische Systeme entwickelt hat. Insbesondere sollte er im Lichte der Systemkritikalität allgemeine materielle Regelungen zur Zulässigkeit und Gestaltung algorithmischer Systeme, zur Transparenz, zu Betroffenenrechten, zu organisatorischen und technischen Absicherungen und zu den Institutionen und Strukturen der Aufsicht bündeln. Der horizontale Rechtsakt sollte auf der Ebene der EU und der Mitgliedstaaten eine **sektorale Konkretisierung erfahren**, die wiederum am Gedanken der Systemkritikalität orientiert ist.

44

Im Zuge der hier empfohlenen Entwicklung einer EUVAS sollte die Aufgabenverteilung zwischen dieser Regulierung und der **DSGVO** überdacht werden. Dabei ist zum einen zu berücksichtigen, dass sich spezifische Risiken algorithmischer Systeme für den Einzelnen und für Gruppen auch dann manifestieren können, wenn keine personenbezogenen Daten verarbeitet werden, und dass die Risiken nicht unbedingt solche des Datenschutzes sind, wenn sie etwa das Vermögen, Eigentum, körperliche Integrität oder Diskriminierung betreffen. Zum anderen ist zu bedenken, dass für eine künftige horizontale Regulierung algorithmischer Systeme ein flexibleres, stärker risikoadaptiertes Regulierungsregime als für den Datenschutz in Betracht gezogen werden sollte.

Instrumente

45

Die DEK empfiehlt bei algorithmischen Systemen erhöhter Systemkritikalität (ab Stufe 2) eine **Kennzeichnungspflicht**: Eine solche Pflicht trägt Betreibern auf, deutlich zu machen, wann und in welchem Umfang algorithmische Systeme zum Einsatz kommen (Information über das „Ob“). Eine Kennzeichnungspflicht sollte unabhängig von der Systemkritikalität stets im Falle einer ethisch relevanten Verwechselungsgefahr zwischen Mensch und algorithmischem System bestehen.

46

Das Recht einer betroffenen Person auf aussagekräftige **Informationen** über die „involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen“ eines algorithmischen Systems (vgl. DSGVO) sollte nicht nur für vollständig automatisierte Systeme, sondern bereits für **Profilbildungen als solche** und unabhängig von einer nachgelagerten Entscheidungssituation bestehen. Es sollte – abgestuft nach der Systemkritikalität – künftig auch bereits für algorithmenbasierte Entscheidungen greifen. Dazu sollte teilweise eine gesetzliche Klarstellung und teilweise eine Erweiterung der Regelung auf europäischer Ebene erfolgen.

47

In bestimmten Bereichen kann es sachgerecht sein, dem Betreiber algorithmischer Systeme zusätzlich zur allgemeinen Erläuterung der Logik (Vorgehensweise) und Tragweite des Systems eine **individuelle Erklärung** der getroffenen Entscheidung abzuverlangen. Wesentlich ist dabei, dass betroffene Personen verständlich, relevant und konkret informiert werden. Die DEK begrüßt daher die technischen Bemühungen, die Erklärbarkeit algorithmischer (insbesondere selbstlernender) Systeme zu stärken („Explainable AI“), und empfiehlt der Bundesregierung, die weitere Forschung und Entwicklung in diesem Bereich zu fördern.

48

In bestimmten Sektoren, in denen nicht nur individuelle, sondern in besonderem Maße auch gesellschaftliche Interessen berührt sind, sollten auch **nicht unmittelbar betroffene Personen** ein Recht auf Zugang zu bestimmten Informationen über die algorithmischen Systeme erhalten. Entsprechende Rechte werden in erster Linie für journalistische und Forschungszwecke infrage kommen und sind zudem mit Blick auf die betroffenen Interessen der Betreiber durch hinreichende Schutzmaßnahmen zu flankieren. Unter Umständen, insbesondere beim staatlichen Einsatz von algorithmischen Systemen mit einem erheblichen Schädigungspotenzial (Stufe 4), kommen nach Ansicht der DEK darüber hinaus auch voraussetzungslose Informationszugangsansprüche in Frage.

49

Bei algorithmischen Systemen ab einem gewissen Schädigungspotenzial (ab Stufe 2) ist es sachgerecht und zumutbar, dem Betreiber gesetzlich die Erstellung und Veröffentlichung einer angemessenen **Risikofolgenabschätzung** abzuverlangen, die auch bei der Verarbeitung nicht-personenbezogener Daten greift und Risiken außerhalb des Datenschutzes berücksichtigt. Sie sollte insbesondere auch eine Abschätzung der Risiken für Selbstbestimmung, Privatheit, körperliche Unversehrtheit, persönliche Integrität sowie Vermögen, Eigentum und Diskriminierung umfassen. Außerdem sollte sie neben den zugrundeliegenden Daten und der Logik des Modells auch Qualitätsmaße und Fairnessmaße zu den Daten und zur Modellgüte berücksichtigen, etwa zu Bias oder (statistischen) Fehlerquoten (insgesamt oder für bestimmte Teilgruppen), die ein System bei der Vorhersage/Kategorienbildung aufweist.

50

Die Anforderungen an **Dokumentation und Protokollierung** in Bezug auf die verwendeten Datensätze und Modelle, die Granularität, die Aufbewahrungszeiten und die Verwendungszwecke sollten konkretisiert werden, damit die Verantwortlichen und Auftragsverarbeiter Rechtsklarheit erhalten. Zum anderen sollte für sensible Anwendungen künftig eine Pflicht etabliert werden, die Programmabläufe einer Software, die nachhaltige Schäden verursachen können, zu dokumentieren und zu protokollieren. Die verwendeten Datensätze und Modelle sind so zu beschreiben, dass diese für Aufsichtsinstitutionen im Falle einer Kontrolle nachvollziehbar sind (etwa hinsichtlich der Herkunft und Aufbereitung von Datensätzen oder der Optimierungsziele der Modelle).

51

Der Normgeber sollte Betreibern ein Mindestmaß an **technischen und mathematisch-prozeduralen Qualitätsgarantien** abverlangen, welche die Korrektheit und Rechtmäßigkeit der algorithmisch ermittelten Ergebnisse durch Verfahrensvorgaben absichern. Dazu können insbesondere Vorgaben für Korrektur- und Kontrollmechanismen oder für die Datenqualität sowie die Sicherheit des Systems gehören. So wäre es beispielsweise sachgerecht, qualitative Anforderungen an das Verhältnis zwischen der Datengrundlage und dem Ergebnis des algorithmischen Datenverarbeitungsprozesses vorzugeben.

52

Beim Einsatz algorithmischer Systeme im Kontext menschlicher Entscheidungen sieht die DEK zunächst Klarstellungs- und Konkretisierungsbedarf betreffend die Anwendungsvoraussetzungen und Rechtsfolgen von Art. 22 DSGVO. Darüber hinaus empfiehlt die DEK, **Schutzmechanismen auch für algorithmenbasierte und -getriebene Entscheidungssysteme** vorzusehen, da sich der Einfluss dieser Systeme in der Praxis nahezu ebenso stark auswirken kann wie bei algorithmendeterminierten Anwendungen. Diesbezüglich empfiehlt sich anstelle des von Art. 22 DSGVO bislang verfolgten Verbotsprinzips ein flexibleres, risikoadaptiertes Regulierungsregime, das dem Einzelnen angemessene Schutzgarantien (insbesondere im Falle von Profiling) und Verteidigungsmöglichkeiten gegen Fehler und Bedrohungen seiner Rechte vermittelt.

53

Es ist erwägenswert, den **Anwendungsbereich des Antidiskriminierungsrechts** in situativer Hinsicht auf Diskriminierungen auszudehnen, die auf einer automatisierten Datenauswertung oder einem automatisierten Entscheidungsverfahren beruhen. Der Gesetzgeber sollte darüber hinaus Maßnahmen eines wirksamen Schutzes gegen **Diskriminierungen aufgrund von Gruppenmerkmalen** etablieren, die an sich nicht zu den gesetzlich geschützten Diskriminierungsmerkmalen zählen, und bei denen Diskriminierungen derzeit vielfach auch nicht als mittelbare Diskriminierung aufgrund eines geschützten Merkmals qualifiziert werden können.

54

Zusätzlich zu bereits bestehender Regulierung ist es für algorithmische Systeme mit deutlichem oder regelmäßigem (Stufe 3) oder sogar erheblichem Schädigungspotenzial (Stufe 4) sinnvoll, **Zulassungsverfahren oder Vorabprüfungen** von algorithmischen Systemen durch Aufsichtsinstitutionen zu etablieren, um Schäden für einzelne Betroffene, Bevölkerungsgruppen oder die Gesellschaft als Ganzes abzuwenden.

Institutionen

55

Die DEK empfiehlt der Bundesregierung, die bestehenden Aufsichtsinstitutionen und -strukturen im Rahmen ihrer Zuständigkeit zu stärken, neu auszurichten und, wo erforderlich, auch neue Institutionen und Strukturen zu schaffen. Dabei sollten die behördlichen Aufsichtsaufgaben und Kontrollbefugnisse primär jeweils denjenigen **sektoralen Aufsichtsbehörden** zugewiesen werden, die bereits sektorspezifische Sachkompetenzen ausgebildet haben. Von großer Bedeutung ist es dabei, dass die zuständigen Behörden mit den erforderlichen finanziellen, personellen und technischen **Ressourcen** ausgestattet werden.

56

Darüber hinaus empfiehlt die DEK der Bundesregierung die Schaffung eines **bundesweiten Kompetenzzentrums Algorithmische Systeme**, welches die sektoralen Aufsichtsbehörden durch technischen und regulatorischen Sachverstand in ihrer Aufgabe unterstützt, algorithmische Systeme im Hinblick auf die Einhaltung von Recht und Gesetz zu kontrollieren.

57

Aus Sicht der DEK sollten Initiativen unterstützt werden, die – ggf. differenziert nach kritischen Anwendungsbereichen – technisch-statistische **Standards für die Qualität von Testverfahren und Audits** festlegen. Für die Überprüfbarkeit algorithmischer Systeme können derartige Testverfahren künftig eine zentrale Rolle spielen, wenn sie hinreichend aussagekräftig, verlässlich und sicher ausgestaltet sind.

58

Innovative Formen der **Ko- und Selbstregulierung** verdienen aus Sicht der DEK neben und in Ergänzung zu staatlichen Formen der Regulierung besondere Aufmerksamkeit. Die DEK empfiehlt der Bundesregierung die Prüfung verschiedener Modelle der Ko- und Selbstregulierung, die für bestimmte Konstellationen adäquate Antworten liefern können.

59

Die DEK hält es für erwägenswert, den Betreibern – nach dem Regulierungsmodell „Comply or Explain" – die gesetzliche Pflicht aufzuerlegen, sich zu den Regeln eines **Algorithmic Accountability Codex** zu bekennen. Die Erarbeitung eines solchen bindenden Codex für die Betreiber von algorithmischen Systemen könnte dabei durch eine unabhängige, paritätisch besetzte Kommission erfolgen, die nicht unter staatlichem Einfluss stehen dürfte. Vertreter der Zivilgesellschaft sollten bei der Erarbeitung eines solches Codex in angemessener Weise beteiligt werden.

60

Auch ein spezifisches **Gütesiegel** als freiwilliges oder verpflichtendes Schutzzeichen kann Verbrauchern Orientierung über vertrauenswürdige algorithmische Systeme geben und gleichzeitig marktwirtschaftliche Anreize für Entwickler und Betreiber setzen, vertrauenswürdige Systeme zu entwickeln und zu verwenden.

61

Ähnlich wie schon heute Unternehmen ab einer bestimmten Größe einen Datenschutzbeauftragten benennen müssen, sollten nach Auffassung der DEK künftig auch solche Unternehmen und Behörden, die kritische algorithmische Systeme betreiben, einen **Ansprechpartner** benennen müssen. Er soll für die Kommunikation mit Behörden zur Verfügung stehen und zu einer Mitwirkung verpflichtet sein.

62

Um sicherzustellen, dass bei der behördlichen Überprüfung algorithmischer Systeme auch die Interessen der Zivilgesellschaft und betroffener Unternehmen angemessen berücksichtigt werden, sollten geeignete **Beiräte bei den sektoralen Aufsichtsbehörden** gebildet werden.

63

Die DEK stuft technische Standards **akkreditierter Normungsorganisationen** als ein grundsätzlich sinnvolles Instrument zwischen staatlicher Regulierung und rein privater Selbstregulierung an. Sie empfiehlt daher der Bundesregierung, in geeigneter Weise auf die Entwicklung und Verabschiedung technischer Standards hinzuwirken.

64

Die in Deutschland bewährten **Klagerechte von Wettbewerbern** und von **Wettbewerbs- und Verbraucherverbänden** sind ein zentraler Baustein für eine zivilgesellschaftliche Kontrolle des Einsatzes von algorithmischen Systemen. Besonders legitimierte zivilgesellschaftliche Akteure können durch solche privaten Klagerechte die Einhaltung von Rechtsvorschriften im Bereich des Vertragsrechts, des Lauterkeitsrechts oder des Antidiskriminierungsrechts sicherstellen, ohne hierbei auf das Tätigwerden von Behörden oder die Mandatierung durch einzelne Betroffene angewiesen zu sein.

Besonderes Augenmerk: Algorithmische Systeme bei Medienintermediären

65

Vor dem Hintergrund der besonderen Gefahren von Medienintermediären mit **Torwächterfunktion für die Demokratie** empfiehlt die DEK – auch mit Blick auf eine Einwirkung auf den EU-Gesetzgeber (→ siehe oben Empfehlung Nr. 43) – zu prüfen, wie den mit einer solchen Torwächterfunktion verbundenen Gefahren begegnet werden kann. Dabei sollte ein ganzes Spektrum gefahrenabwehrender Maßnahmen erwogen werden, das bis hin zu einer Ex-ante-Kontrolle (z. B. in Form eines Lizenzierungsverfahrens) reichen kann.

66

Den nationalen Gesetzgeber trifft die verfassungsrechtliche Pflicht, die Demokratie vor den Gefahren für die freie demokratische und plurale Meinungsbildung, die von Anbietern mit Torwächterfunktion ausgehen, durch **Etablierung einer positiven Medienordnung** zu schützen. Die DEK empfiehlt, die Anbieter in diesem engen Bereich zum Einsatz solcher algorithmischer Systeme zu verpflichten, die den Nutzern zumindest als zusätzliches Angebot auch einen Zugriff auf eine tendenzfreie, ausgewogene und die plurale Meinungsvielfalt abbildende Zusammenstellung von Beiträgen und Informationen verschaffen.

67

Für alle Medienintermediäre und auch bei Anbietern ohne Torwächterfunktion oder bei geringerem Schädigungspotenzial für die demokratische Meinungsbildung sollte die Bundesregierung Maßnahmen prüfen, die den charakteristischen Gefahren des Mediensektors Rechnung tragen. Dies könnte Mechanismen zur **Transparenzsteigerung** (z. B. Einblick in technische Verfahren der Nachrichtenauswahl und -priorisierung, **Kennzeichnungspflichten für Social Bots**) und ein Recht auf Gegendarstellung in Timelines umfassen.

Der Einsatz von algorithmischen Systemen durch staatliche Stellen

68

Der Staat ist im Interesse seiner Bürger zur Nutzung der besten verfügbaren Technik – einschließlich algorithmischer Systeme – verpflichtet, muss dabei jedoch im Lichte seiner Grundrechtsbindung sowie der Vorbildfunktion allen staatlichen Handelns besondere Sorgfalt walten lassen. Der Einsatz algorithmischer Systeme durch Hoheitsträger ist daher **im Allgemeinen als besonders sensibel im Sinne des Kritikalitätsmodells** einzustufen und erfordert mindestens eine umfassende Risikofolgenabschätzung.

69

Aufgaben in der **Rechtsetzung** und der **Rechtsprechung** dürfen algorithmischen Systemen allenfalls in Randbereichen übertragen werden. Insbesondere dürfen algorithmische Systeme nicht genutzt werden, um die freie Willensbildung im demokratischen Prozess und die sachliche Unabhängigkeit der Gerichte zu unterminieren. Große Potenziale für den Einsatz algorithmischer Systeme bestehen hingegen in der **Verwaltung**, vor allem in der Leistungsverwaltung. Um dem Rechnung zu tragen, sollte der Gesetzgeber verstärkt teil- und vollautomatisierte Verwaltungsverfahren zulassen. Dazu bedarf es auch einer vorsichtigen Fortentwicklung des zu engen § 35a VwVfG sowie der entsprechenden einfachrechtlichen Normen. Bei alledem gilt es, hinreichende Schutzmaßnahmen für die Bürger vorzusehen.

70

Staatliche Entscheidungen, die unter Nutzung algorithmischer Systeme zustande kommen, müssen **transparent und begründbar** bleiben. Dazu bedarf es ggf. Klarstellungen bzw. Erweiterungen der bestehenden Informationsfreiheits- und Transparenzgesetze. Ferner entbindet der Einsatz algorithmischer Systeme nicht vom Grundsatz, dass hoheitliche Entscheidungen regelmäßig im Einzelfall begründet werden müssen; im Gegenteil kann dieser Grundsatz dem Einsatz allzu komplexer algorithmischer Systeme Grenzen setzen. Schließlich trägt die Nutzung von Open-Source-Lösungen wesentlich zur Transparenz staatlichen Handelns bei und sollte daher verstärkt angestrebt werden.

71

Zwar ist aus ethischer Sicht ein generelles Recht auf Freiheit zur Nichtbefolgung von Normen nicht anzuerkennen. Gleichzeitig wirft ein automatisierter Totalvollzug des Rechts eine Reihe ethischer Bedenken auf. Daher ist regelmäßig ein technisches Design zu fordern, bei dem der Mensch im Einzelfall den **technischen Vollzug** außer Kraft setzen kann. Ferner muss stets die Verhältnismäßigkeit zwischen der potenziellen Normübertretung und der automatisierten (ggf. präventiven) Vollzugsmaßnahme gewahrt sein.

Haftung für algorithmische Systeme

72

Neben strafrechtlicher Verantwortlichkeit und Verwaltungssanktionen ist auch die Haftung auf Schadensersatz unverzichtbarer Bestandteil eines ethisch vertretbaren Ordnungsrahmens. Es ist bereits jetzt erkennbar, dass algorithmische Systeme – u. a. aufgrund der Komplexität und Dynamik der Systeme sowie aufgrund ihrer wachsenden „Autonomie" – das bestehende Haftungsrecht vor Herausforderungen stellen. Die DEK empfiehlt daher eine umfassende Prüfung und, soweit erforderlich, **Anpassung des geltenden Haftungsrechts**. Der Blick sollte sich dabei nicht allein auf bestimmte technologische Merkmale – wie etwa auf das Merkmal Maschinellen Lernens oder Künstlicher Intelligenz – verengen.

73

Der Gedanke, algorithmischen Systemen hoher Autonomie künftig Rechtspersönlichkeit zuzuerkennen und sie selbst für Schäden haften zu lassen (**„elektronische Person"**), sollte **nicht weiterverfolgt** werden. Soweit dieser Gedanke auf eine Analogie zwischen Mensch und Maschine gestützt wird, ist er schon ethisch nicht vertretbar, und soweit es schlicht um die Anerkennung einer neuen Gesellschaftsform im Sinne des Gesellschaftsrechts geht, löst er keine Probleme.

74

Dagegen ist es geboten, für den Einsatz sog. autonomer Systeme – abhängig von der Natur der dem System übertragenen Aufgaben – auch eine Zurechnung schädigender Vorgänge entsprechend den Regelungen über die Haftung für **Gehilfen** (vgl. insbes. § 278 BGB) vorzunehmen. Beispielsweise sollte eine Bank, die sich für die Prüfung der Kreditwürdigkeit eines autonomen Systems bedient, gegenüber ihrem Kunden mindestens in gleichem Maße haften, wie wenn sie sich eines menschlichen Mitarbeiters bedient hätte.

75

Daneben erscheint es nach derzeitigem Stand der Diskussion sehr wahrscheinlich, dass zusätzlich zu einer sachgerechten Anpassung der aus den 1980er Jahren stammenden **Produkthaftungsrichtlinie** und Verknüpfung mit neuen Standards der Produktsicherheit auch punktuelle Modifikationen der **Verschuldenshaftung** und/oder neue Tatbestände der **Gefährdungshaftung** erforderlich sein werden. Dabei wird jeweils zu klären sein, für welche Produkte, digitalen Inhalte und digitalen Dienstleistungen welches Haftungsregime sachgerecht und wie dieses konkret auszugestalten ist, wobei es wiederum wesentlich u. a. auf die Kritikalität des betreffenden algorithmischen Systems ankommen wird. Dabei sollten auch innovative Haftungskonzepte, wie sie derzeit auf europäischer Ebene entwickelt werden, in Betracht gezogen werden.

4

Für einen europäischen Weg

Die Fülle an Fragen, die sich der DEK im Rahmen ihrer Arbeit gestellt haben und deren Diskussion jeweils wieder neue Fragen aufgeworfen hat, lässt deutlich werden, dass dieses Gutachten lediglich einen weiteren Grundstein für einen **andauernden Zukunftsdiskurs über Ethik, Recht und Technologie** legen kann. Die DEK betont dabei, dass Ethik, Recht und Demokratie auch in der technischen Welt ihre gestaltende Kraft entfalten müssen. Dazu bedarf es eines interdisziplinären Diskurses in Politik und Gesellschaft sowie einer Gesetzgebung und Regulierung, die so offen gestaltet ist, dass sie auch bei schneller Entwicklung von Technik und Geschäftsmodellen ihre Regelungskraft und Reaktionsfähigkeit behält. Es bedarf zusätzlich der Instrumente, Verfahren und Strukturen, um die Regulierung effektiv durchzusetzen und bei Verstößen oder Fehlentwicklungen rechtzeitig einschreiten zu können.

Deutschland und Europa sehen sich im globalen Wettlauf um Zukunftstechnologien mit Wertesystemen, Gesellschaftsmodellen und Kulturen konfrontiert, die sich von unseren unterscheiden. Die DEK unterstützt den bislang eingeschlagenen **„europäischen Weg“**: Europäische Technologien sollten sich durch konsequente Ausrichtung an europäischen Werten und Grundrechten, wie sie insbesondere auch in der Charta der Grundrechte der Europäischen Union und in der Konvention zum Schutz der Menschenrechte und Grundfreiheiten des Europarats zum Ausdruck kommen, auszeichnen.

Die DEK sieht den Staat in besonderer Verantwortung, im Einklang mit unserer Werteordnung ethische Maßstäbe auch für den digitalen Raum zu formulieren und diese durchzusetzen. Um diese Garantie gegenüber den Bürgern auch einhalten zu können, bedarf es international einer Position politischer und ökonomischer Stärke: Wer von anderen übermäßig abhängig ist, wird vom „rule maker“ zum „rule taker“ und setzt seine Bürger letztlich Vorgaben aus, die von Akteuren aus anderen Regionen der Welt formuliert werden, oder von privaten Akteuren, die demokratischer Legitimation und Kontrolle weitgehend entzogen sind. Bemühungen um die **langfristige Sicherung der digitalen Souveränität Deutschlands und Europas** sind daher nicht nur ein Gebot politischer Weitsicht, sondern auch Ausdruck ethischer Verantwortung.

Mitglieder der Datenethikkommission der Bundesregierung

Co-Sprecherinnen

Prof. Dr. Christiane Wendehorst

- Professorin für Zivilrecht an der Universität Wien
- Mitglied im Vorstand des Instituts für Innovation und Digitalisierung im Recht an der Universität Wien
- Präsidentin des European Law Institute (ELI)

Prof. Dr. Christiane Woopen

- Professorin für Ethik und Theorie der Medizin und Leiterin der Forschungsstelle Ethik an der Uniklinik Köln
- Geschäftsführende Direktorin des Cologne Center for Ethics, Rights, Economics, and Social Sciences (ceres) der Universität zu Köln
- Vorsitzende des Europäischen Ethikrates (EGE)

Mitglieder

Prof. Dr. Johanna Haberer

- Leitung der Professur für Christliche Publizistik an der Friedrich-Alexander-Universität Nürnberg-Erlangen
- Geschäftsführerin des Instituts für Praktische Theologie an der Friedrich-Alexander-Universität Nürnberg-Erlangen

Marit Hansen

- Landesbeauftragte für Datenschutz Schleswig-Holstein
- Leiterin des Unabhängigen Landeszentrums für Datenschutz (ULD)

Prof. Dr. Dirk Heckmann

- Inhaber des Lehrstuhls für Recht und Sicherheit der Digitalisierung an der Technischen Universität München
- Direktor am Bayerischen Forschungsinstitut für Digitale Transformation
- Verfassungsrichter am Bayerischen Verfassungsgerichtshof

Prof. Ulrich Kelber

- Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
- Honorarprofessor an der Hochschule Bonn-Rhein-Sieg

Prof. Dieter Kempf

- Präsident des Bundesverbandes der Deutschen Industrie e. V.
- Honorarprofessor an der Friedrich-Alexander-Universität Erlangen-Nürnberg

Prof. Dr. Mario Martini

- Inhaber des Lehrstuhls für Verwaltungswissenschaft, Staatsrecht, Verwaltungsrecht und Europarecht an der DUV Speyer
- Leiter des Programmbereichs „Transformation des Staates durch Digitalisierung“ und Stellvertretender Direktor des Deutschen Forschungsinstituts für öffentliche Verwaltung

Klaus Müller

- Vorstand des Verbraucherzentrale Bundesverbands (vzbv e. V.)
- Lehrbeauftragter an der Heinrich-Heine-Universität Düsseldorf

Paul Nemitz

- Hauptberater in der EU Kommission, Generaldirektion Justiz und Verbraucherschutz

Prof. Dr. Sabine Sachweh

- Professorin für Angewandte Softwaretechnik an der Fachhochschule Dortmund
- Sprecherin und Vorstandsmitglied des Instituts für die Digitalisierung von Arbeits- und Lebenswelten (IDiAL) der Fachhochschule Dortmund
- Ko-Sprecherin im Fachbeirat „Digitalisierung und Bildung für ältere Menschen“ des Bundesministeriums für Familie, Senioren, Frauen und Jugend

Christin Schäfer

- Gründerin und Geschäftsführerin des Unternehmens acs plus, einer Boutique für Data Science
- Beirätin der Forschungsgruppe Big Data Analytics des IW Köln

Prof. Dr. Rolf Schwartmann

- Professor für Bürgerliches Recht und Wirtschaftsrecht an der Technischen Hochschule Köln
- Leiter der Forschungsstelle für Medienrecht an der Technischen Hochschule Köln
- Vorsitzender der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V.

Prof. Dr. Judith Simon

- Professorin für Ethik in der Informationstechnologie an der Universität Hamburg

Prof. Dr. Dr. h.c. mult. Wolfgang Wahlster

- Professor für Informatik, Lehrstuhl für Künstliche Intelligenz, Universität des Saarlandes
- CEO/CEA des Deutschen Forschungszentrums für Künstliche Intelligenz
- Leiter des Steuerungskreises für die KI-Normungsroadmap beim Deutschen Institut für Normung (DIN)

Prof. Dr. Thomas Wischmeyer

- Juniorprofessor (Tenure Track) für Öffentliches Recht und Recht der Digitalisierung an der Universität Bielefeld

Stand: 10. Oktober 2019

Impressum

Berlin, Oktober 2019

Gutachten der Datenethikkommission
der Bundesregierung

Herausgeber
Datenethikkommission der Bundesregierung
Bundesministerium des Innern, für Bau und Heimat
Alt-Moabit 140
10557 Berlin
Bundesministerium der Justiz und für Verbraucherschutz
Mohrenstraße 37
10117 Berlin

E-Mail
datenethikkommission_gs@bmi.bund.de
datenethikkommission_gs@bmjv.bund.de

Internet
www.datenethikkommission.de

Gestaltung
Atelier Hauer + Dörfler GmbH, Berlin

Bildnachweis
S. 28: BMI (Gruppenfoto), Studio Wilke (Christiane Wendehorst), Reiner Zensen (Christiane Woopen), BPA/Kugler (Ulrich Kelber)
S. 29: Christian Kruppa (Dieter Kempf), vzbv/Gert Baumbach (Klaus Müller), Markus Mielek (Sabine Sachweh), TH Köln/Schmülgen (Rolf Schwartmann), UHH/Nicolai (Judith Simon), Jim Rakete (Wolfgang Wahlster)

Druck
Brandenburgische Universitätsdruckerei und Verlagsgesellschaft Potsdam mbH (bud)

Ausschließlich zum Zweck der besseren Lesbarkeit wird im vorliegenden Gutachten der Datenethikkommission auf die geschlechtsspezifische Schreibweise verzichtet. Alle personenbezogenen Bezeichnungen sind geschlechtsneutral zu verstehen.

Die Langfassung des Gutachtens kann im Internet unter **www.datenethikkommission.de** heruntergeladen werden.