

# Gutachten der Datenethikkommission



daten  
ethik  
kommission



# Gutachten der Datenethikkommision



daten  
ethik  
kommission

---

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

---

# Inhaltsübersicht

<b>Executive Summary</b>	<b>12</b>
<b>A Einleitung</b>	<b>33</b>
<b>B Ethische und rechtliche Grundsätze und Prinzipien</b>	<b>39</b>
<b>C Technische Grundlagen</b>	<b>49</b>
<b>D Mehr-Ebenen-Governance komplexer Datenökosysteme</b>	<b>67</b>
<b>E Daten</b>	<b>79</b>
<b>F Algorithmische Systeme</b>	<b>159</b>
<b>G Für einen europäischen Weg</b>	<b>225</b>
<b>Anhang</b>	<b>229</b>

# Inhaltsverzeichnis

## **Executive Summary .....** **12**

1. Allgemeine ethische und rechtliche Grundsätze und Prinzipien .....	14
2. Daten .....	16
3. Algorithmische Systeme .....	24
4. Für einen europäischen Weg .....	32

## **A Einleitung .....** **33**

1. Arbeitsauftrag und Grundverständnis .....	34
2. Arbeitsweise .....	35
3. Ziele und Gegenstand des Gutachtens .....	36

## **B Ethische und rechtliche Grundsätze und Prinzipien .....** **39**

1. Der grundsätzliche Wert menschlichen Handelns .....	40
2. Verhältnis von Ethik und Recht .....	41
3. Allgemeine ethische und rechtliche Grundsätze und Prinzipien .....	43
3.1 Die Würde des Menschen .....	43
3.2 Selbstbestimmung .....	43
3.3 Privatheit .....	45
3.4 Sicherheit .....	45
3.5 Demokratie .....	46
3.6 Gerechtigkeit und Solidarität .....	46
3.7 Nachhaltigkeit .....	47

## **C Technische Grundlagen .....** **49**

1. Status Quo .....	51
2. Systemelemente .....	52
2.1 Daten .....	52
2.1.1 Begriff und Eigenschaften von Daten .....	52
2.1.2 Data Management .....	53
2.1.3 Big Data und Small Data .....	53
2.2 Datenverarbeitung .....	54
2.2.1 Algorithmen .....	54
2.2.2 Statistisches Schließen .....	55
2.2.3 Maschinelles Lernen .....	57
2.2.4 Künstliche Intelligenz .....	59
2.2.5 Algorithmische Systeme .....	62
2.3 Software .....	62
2.4 Hardware .....	63
2.5 Systemarchitektur .....	63

<b>D</b>	<b>Mehr-Ebenen-Governance komplexer Datenökosysteme .....</b>	<b>67</b>
1.	Allgemeine Rolle des Staates .....	69
2.	Unternehmerische Selbstverpflichtungen und Corporate Digital Responsibility.....	70
3.	Bildung: Stärkung digitaler Kompetenzen und kritischer Reflexion.....	72
4.	Technologieentwicklung und ethisch fundiertes Design .....	74
5.	Forschung .....	75
6.	Standardisierung .....	76
7.	Zwei Governance-Perspektiven: Daten- und Algorithmen-Perspektive .....	77
<b>E</b>	<b>Daten .....</b>	<b>79</b>
1.	Allgemeine Anforderungen an den Umgang mit Daten .....	81
1.1	Vorausschauende Verantwortung.....	81
1.2	Achtung der Rechte beteiligter Personen .....	82
1.3	Wohlfahrt durch Nutzen und Teilen von Daten.....	82
1.4	Zweckadäquate Datenqualität.....	83
1.5	Risikoadäquate Informationssicherheit .....	83
1.6	Interessenadäquate Transparenz .....	83
2.	Datenrechte und korrespondierende Datenpflichten .....	85
2.1	Allgemeine Grundsätze von Datenrechten und Datenpflichten.....	85
2.2	Konkretisierung der allgemeinen Grundsätze anhand typischer Szenarien .....	87
2.2.1	Unterlassungs-Szenarien.....	87
2.2.2	Zugangs-Szenarien .....	90
2.2.3	Korrektur-Szenarien .....	92
2.2.4	Szenarien wirtschaftlicher Teilhabe .....	93
2.3	Kollektive Aspekte von Datenrechten und Datenpflichten .....	94
3.	Anforderungen an die Nutzung personenbezogener Daten .....	95
3.1	Personenbezogene Daten und Daten juristischer Personen .....	95
3.2	Digitale Selbstbestimmung als Aufgabe für die gesamte Rechtsordnung .....	95
3.2.1	Kooperatives Verhältnis zwischen den geltenden Rechtsregimen.....	95
3.2.2	Risikoadäquate Auslegung des geltenden Rechtsrahmens.....	96
3.2.3	Bedarf nach Konkretisierung und Verschärfung des geltenden Rechtsrahmens.....	99
3.2.4	Bedarf nach einer Vereinheitlichung der Datenschutzaufsicht für den Markt .....	103
3.3	Personenbezogene Daten als Vermögensgut .....	104
3.3.1	Ökonomisierung personenbezogener Daten .....	104
3.3.2	Daten als Eigentum und die Frage eines finanziellen Ausgleichs.....	104
3.3.3	Daten als „Gegenleistung“ .....	105
3.3.4	Daten als Grundlage personalisierter Risikoeinschätzung .....	106
3.3.5	Daten als Reputationskapital .....	107
3.3.6	Daten als Handelsware .....	108

3.4	Daten und digitaler Nachlass .....	110
3.4.1	Vorrang von Verfügungen zu Lebzeiten .....	110
3.4.2	Die Rolle von Intermediären .....	110
3.4.3	Postmortaler Datenschutz .....	111
3.5	Besondere Gruppen von Betroffenen .....	112
3.5.1	Beschäftigte .....	112
3.5.2	Patienten .....	113
3.5.3	Minderjährige .....	114
3.5.4	Sonstige Pflege- und Schutzbedürftige .....	115
3.6	Datenschutz durch Technikgestaltung .....	116
3.6.1	Datenschutzfreundliches Design von Produkten und Dienstleistungen .....	116
3.6.2	Datenschutzfreundliche Produktentwicklung .....	120
	Zusammenfassung der wichtigsten Handlungsempfehlungen .....	121
<b>4.</b>	<b>Verbesserung des kontrollierten Zugangs zu personenbezogenen Daten .....</b>	<b>124</b>
4.1	Ermöglichung von Forschung mit personenbezogenen Daten .....	124
4.1.1	Vorüberlegungen .....	124
4.1.2	Rechtsklarheit und Rechtssicherheit .....	125
4.1.3	Einwilligungsprozesse bei sensiblen Daten .....	126
4.1.4	Rechtlicher Diskriminierungsschutz .....	128
4.2	Anonymisierung, Pseudonymisierung und synthetische Daten .....	129
4.2.1	Verfahren, Standards und Vermutungsregeln .....	131
4.2.2	Verbot der De-Anonymisierung .....	132
4.2.3	Synthetische Daten .....	132
4.3	Kontrollierter Datenzugang durch Datenmanagement- und Datentreuhandsysteme .....	133
4.3.1	Privacy Management Tools (PMT) und Personal Information Management Systems (PIMS) .....	133
4.3.2	Bedarf nach Regulierung von PMT/PIMS .....	133
4.3.3	PMT/PIMS als mögliche Schnittstelle zur Datenwirtschaft .....	135
4.4	Datenzugang durch Datenportabilität .....	136
4.4.1	Förderung von Datenportabilität .....	136
4.4.2	Erweiterung des Portabilitätsrechts? .....	137
4.4.3	Von Portabilität zu Interoperabilität und Interkonnektivität .....	137
4.5	Crowd Sensing zu gemeinwohlorientierten Zwecken .....	138
	Zusammenfassung der wichtigsten Handlungsempfehlungen .....	139
<b>5.</b>	<b>Datenzugangsdebatten jenseits des Personenbezugs .....</b>	<b>141</b>
5.1	Gesamtwirtschaftliche Bedeutung eines angemessenen Datenzugangs .....	141
5.2	Schaffung der erforderlichen Rahmenbedingungen .....	142
5.2.1	Bewusstseinsbildung und Datenkompetenz .....	142
5.2.2	Förderung der Infrastrukturen für eine datenbasierte Ökonomie .....	142
5.2.3	Nachhaltige und strategische Wirtschaftspolitik .....	144
5.2.4	Verbesserter Leistungsschutz .....	144
5.2.5	Datenpartnerschaften .....	145

5.3	Datenzugang in bestehenden Wertschöpfungssystemen .....	145
5.3.1	Problemstellung .....	145
5.3.2	Situation bei Bestehen eines Vertragsverhältnisses .....	146
5.3.3	Situation bei Fehlen eines Vertragsverhältnisses .....	147
5.3.4	Sektorspezifische Datenzugangsrechte .....	147
5.4	Offene Daten des öffentlichen Sektors .....	148
5.4.1	Vorüberlegungen .....	148
5.4.2	Rechtsrahmen und Infrastrukturen .....	149
5.4.3	Schutzauftrag des Staates .....	150
5.5	Offene Daten des privaten Sektors .....	151
5.5.1	Plattformen und Datennutzung .....	151
5.5.2	Anreize zum weitergehenden freiwilligen Teilen .....	151
5.5.3	Gesetzliche Datenzugangsrechte .....	152
5.5.4	Rolle des Wettbewerbsrechts .....	153
5.6	Datenzugang zugunsten von öffentlichen Stellen (B2G) und gemeinwohlorientierten Zwecken .....	154
	Zusammenfassung der wichtigsten Handlungsempfehlungen .....	155

## F

## Algorithmische Systeme ..... 159

1.	Charakteristika algorithmischer Systeme .....	160
2.	Allgemeine Anforderungen an algorithmische Systeme .....	163
2.1	Menschenzentriertes Design .....	163
2.2	Vereinbarkeit mit gesellschaftlichen Grundwerten .....	164
2.3	Nachhaltigkeit bei Gestaltung und Einsatz algorithmischer Systeme .....	165
2.4	Hohes Maß an Qualität und Leistungsfähigkeit .....	165
2.5	Gewährleistung von Robustheit und Sicherheit .....	166
2.6	Minimierung von Bias und Diskriminierung als Vorbedingung gerechter Entscheidungen .....	167
2.7	Transparenz, Erklärbarkeit und Nachvollziehbarkeit .....	169
2.8	Klare Rechenschaftsstrukturen .....	171
2.9	Ergebnis: Verantwortungsgeleitete Abwägung .....	171
3.	Empfehlung eines risikoadaptierten Regulierungsansatzes .....	173
3.1	Systemkritikalität und Systemanforderungen .....	173
3.2	Kritikalitätspyramide .....	177
3.3	Regulierung algorithmischer Systeme durch horizontale Vorgaben im Recht der Europäischen Union und sektorale Konkretisierung .....	180
	Zusammenfassung der wichtigsten Handlungsempfehlungen .....	183

<b>4. Instrumente: Pflichten des Verantwortlichen und Rechte Betroffener .....</b>	<b>185</b>
4.1 Transparenzanforderungen .....	185
4.1.1 Kennzeichnungspflichten („Ob“) .....	185
4.1.2 Informationspflichten, Erklärungspflicht und Informationszugang („Wie“ und „Was“) .....	185
4.1.3 Risikofolgenabschätzung .....	188
4.1.4 Pflicht zur Dokumentation und zur Protokollierung .....	190
4.2 Sonstige Vorgaben für algorithmische Systeme .....	190
4.2.1 Allgemeine qualitative Vorgaben an algorithmische Systeme .....	190
4.2.2 Besondere Schutzmaßnahmen beim Einsatz algorithmischer Systeme im Kontext menschlicher Entscheidungen .....	191
4.2.3 Recht auf angemessene algorithmische Schlussfolgerungen? .....	193
4.2.4 Gesetzlicher Diskriminierungsschutz .....	193
4.2.5 Präventives behördliches Zulassungsverfahren für besonders riskante algorithmische Systeme .....	195
Zusammenfassung der wichtigsten Handlungsempfehlungen .....	196
<b>5. Institutionen .....</b>	<b>198</b>
5.1 Behördliche Kompetenzen und fachliche Expertise .....	198
5.1.1 Verteilung der Aufsichtsaufgaben im sektoralen Kontrollverbund .....	198
5.1.2 Aufgabenangemessene Ausgestaltung der Kontrollbefugnisse .....	199
5.1.3 Kritikalitätsangemessene Kontrolltiefe .....	200
5.2 Unternehmerische Selbstregulierung und Ko-Regulierung .....	201
5.2.1 Selbstregulierung und -zertifizierung .....	201
5.2.2 Erarbeitung eines Verhaltenscodex .....	202
5.2.3 Gütesiegel für algorithmische Systeme .....	203
5.2.4 Ansprechpartner für algorithmische Systeme in Unternehmen und Behörden .....	203
5.2.5 Einbindung zivilgesellschaftlicher Akteure .....	203
5.3 Technische Standardisierung .....	203
5.4 Institutioneller Rechtsschutz (insbesondere Verbandsklagerechte) .....	204
Zusammenfassung der wichtigsten Handlungsempfehlungen .....	205
<b>6. Besonderes Augenmerk: Algorithmische Systeme bei Medienintermediären .....</b>	<b>207</b>
6.1 Die Relevanz für den demokratischen Prozess am Beispiel sozialer Netzwerke .....	207
6.2 Vielfalt bei Medienintermediären am Beispiel sozialer Netzwerke .....	208
6.3 Kennzeichnungspflicht für Social Bots .....	209
6.4 Maßnahmen gegen „Fake News“ .....	210
6.5 Transparenzpflichten für News-Aggregatoren .....	210
Zusammenfassung der wichtigsten Handlungsempfehlungen .....	211

<b>7. Der Einsatz algorithmischer Systeme durch staatliche Stellen .....</b>	<b>212</b>
7.1 Chancen und Risiken beim Einsatz algorithmischer Systeme durch staatliche Stellen.....	212
7.2 Algorithmische Systeme in der Rechtsetzung .....	212
7.3 Algorithmische Systeme in der Rechtsprechung .....	213
7.4 Algorithmische Systeme in der Verwaltung .....	214
7.5 Algorithmische Systeme im Sicherheitsrecht .....	214
7.6 Transparenzanforderungen beim Einsatz algorithmischer Systeme durch staatliche Akteure .....	215
7.7 Das Risiko eines automatisierten Totalvollzugs .....	217
Zusammenfassung der wichtigsten Handlungsempfehlungen .....	218
<b>8. Haftung für algorithmische Systeme.....</b>	<b>219</b>
8.1 Bedeutung .....	219
8.2 Schäden durch den Einsatz algorithmischer Systeme .....	219
8.2.1 Haftung der „Elektronischen Person“? .....	219
8.2.2 Gehilfenhaftung für „Autonome“ Systeme .....	219
8.2.3 Gefährdungshaftung .....	220
8.2.4 Produktsicherheit und Produkthaftung .....	221
8.3 Bedarf nach einer Neubewertung des Haftungsrechts .....	222
Zusammenfassung der wichtigsten Handlungsempfehlungen .....	224
<b>G Für einen europäischen Weg.....</b>	<b>225</b>
<b>Anhang.....</b>	<b>229</b>
1. Leitfragen der Bundesregierung an die Datenethikkommission .....	230
2. Mitglieder der Datenethikkommission der Bundesregierung .....	234

# Executive Summary



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 Entwicklung 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 entbehrliech 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 zu stehen, 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. **konfliktierenden 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.

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 Risiko-einschätzung** (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 abzuholen. 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 wahrnehmende 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. Interkonnectivität** 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 Drittirkung 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 Einbeugs 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) **algorithmdeterminierte** 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:

## Empfehlung eines risiko-adaptierten 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 gestiegerte 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 Systemkritikaltät 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 Systemkritikaltät 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 erhöhte 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 Anti-diskriminierungsrechts** 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 regelmäßigen (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 **sektorale 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 Verabschaffung 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 auszustalten 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 Zukundtsdiskurs 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 allerdings im globalen Wettkampf 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.

Teil A

# Einleitung



# 1. Arbeitsauftrag und Grundverständnis

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, und tun dies zum Teil schon heute. Die digitale Transformation bietet gerade für Deutschland als eng vernetzte und hoch technologisierte Volkswirtschaft enorme Chancen, übt jedoch auch zunehmenden internationalen Konkurrenzdruck auf deutsche Unternehmen aus. Gleichzeitig zeigen sich bereits jetzt die 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 steht. Wenn der digitale Wandel zum Wohl für den Einzelnen und die gesamte Gesellschaft führen soll, müssen sich Gesellschaft und Politik mit der Gestaltung datenbasierter Technologien einschließlich der KI befassen.

Die Bundesregierung hat am 18. Juli 2018 die Datenethikkommission (DEK) eingesetzt und sechzehn Mitglieder (siehe Anhang, 2.) berufen. Christiane Wendehorst und Christiane Woopen wurden gemeinsam zu Vorsitzenden bestellt. Die DEK erhielt den Auftrag, innerhalb eines Jahres ethische Maßstäbe und Leitlinien für den Schutz des Einzelnen, die Wahrung des gesellschaftlichen Zusammenlebens und die Sicherung und Förderung des Wohlstands im Informationszeitalter zu entwickeln. Die Kommission soll auch konkrete Handlungs- und Regulierungsempfehlungen unterbreiten, wie diese ethischen Leitlinien beachtet, implementiert und beaufsichtigt werden können. Dazu hat die Bundesregierung der DEK Leitfragen (siehe Anhang, 1.) an die Hand gegeben, die sich auf die drei Themenfelder: (I.) Algorithmenbasierte Prognose- und Entscheidungsprozesse, (II.) Künstliche Intelligenz und (III.) Daten konzentrieren.

Die DEK versteht **KI** in diesem Zusammenhang als Sammelbegriff für diejenigen Technologien und ihre Anwendungen, die durch digitale Methoden auf der Grundlage potenziell sehr großer und heterogener Datensätze in einem komplexen und die menschliche Intelligenz gleichsam nachahmenden maschinellen Verarbeitungsprozess ein Ergebnis ermitteln, das ggf. automatisiert zur Anwendung gebracht wird. Die wichtigsten Grundlagen für KI als Teilgebiet der Informatik sind die subsymbolische Mustererkennung, das maschinelle Lernen, die computergerechte Wissensrepräsentation und die Wissensverarbeitung, welche Methoden der heuristischen Suche, der Inferenz und der Handlungsplanung umfasst.

Die DEK hält es indessen für unangemessen, ethische und rechtliche Betrachtungen ausschließlich auf KI zu konzentrieren. Sie ist lediglich eine besondere Ausprägung und damit ein Teilbereich algorithmischer Systeme. Einige Eigenschaften, die zu ethischen Problemen führen können, teilt sie mit anderen Arten algorithmischer Systeme, so dass eine auf KI beschränkte Regulierung nur einen Teil der Probleme erfassen würde. Die bei KI im Vordergrund stehende Eigenschaft des Selbstlernens bringt zwar spezifische Herausforderungen mit sich, die bei einer Risikobestimmung besonders zu berücksichtigen sind, sie ist aber nicht die einzige Eigenschaft, die besonderer Aufmerksamkeit bedarf. Insofern beziehen sich die folgenden Ausführungen auf **alle Arten algorithmischer Systeme**.

Anwendungen beruhen selten auf einem einzigen Algorithmus, und eine isolierte Betrachtung von Algorithmen hat selten Aussagekraft. Für die ethische 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.

## 2. Arbeitsweise

Die DEK trat zwischen September 2018 und September 2019 monatlich zusammen. Die DEK diskutierte exemplarische Anwendungsbeispiele neuer Technologien („Use Cases“) in verschiedenen Sektoren, die im Hinblick auf ihre technischen Grundlagen sowie unter ethischen und juristischen Gesichtspunkten analysiert wurden. Die daraus und aus grundlegenden Diskussionen gewonnenen Erkenntnisse erlaubten die Identifizierung von übergeordneten Themen und Fragestellungen, um Eckpunkte zur ethischen Einordnung sowie konkrete Empfehlungen für künftiges politisches und gesetzgeberisches Handeln zu entwickeln. Bereits im Oktober 2018 unterbreitete die DEK auf der Grundlage eines Eckpunktepapiers der Bundesregierung zwei konkrete Empfehlungen für die Ausgestaltung der „Strategie Künstliche Intelligenz“, die von der Bundesregierung aufgegriffen wurden. Im November 2018 gab die DEK noch eine weitere Empfehlung ab, in der sie sich für eine partizipative Entwicklung der elektronischen Patientenakte aussprach.<sup>1</sup>

Die Öffentlichkeit wurde im Rahmen von zwei öffentlichen Tagungen mit einbezogen. Die erste Tagung fand am 7. Februar 2019 im Bundesministerium der Justiz und für Verbraucherschutz (BMJV) zu dem Thema „Selbst- und Fremdbestimmung im Zeitalter künstlicher Intelligenz“ statt. Die zweite Tagung wurde am 9. Mai 2019 als International Round Table mit dem Titel „Für eine ethische Gestaltung unserer digitalen Zukunft“ („Towards Shaping of Our Digital Future“) im Bundesministerium des Innern, für Bau und Heimat (BMI) ausgerichtet. Beide Veranstaltungen erlaubten einen intensiven Austausch der DEK mit Experten, Stakeholdern sowie der Öffentlichkeit und interessierten Bürgerinnen und Bürgern.<sup>2</sup>

Am 14. November 2018 fand anlässlich der Digitalklau-  
sur der Bundesregierung ein Austausch zwischen der  
Bundeskanzlerin sowie allen Mitgliedern der Bundes-  
regierung und den beiden Vorsitzenden der DEK statt.  
Darüber hinaus wurden anlassbezogen Gespräche mit  
einzelnen Mitgliedern der Bundesregierung geführt. Zu-  
dem wurden Experten angehört und Konsultationstreffen  
mit anderen Institutionen und Gremien durchgeführt,  
die sich verwandten Themen widmen – darunter etwa  
die Enquête-Kommission „Künstliche Intelligenz“, die  
Kommission Wettbewerbsrecht 4.0, der Digitalrat der  
Bundesregierung, der Sachverständigenrat für Verbrau-  
cherfragen, u.v.m.

Es gehörte zu den wesentlichen Merkmalen der DEK,  
dass sie in völliger Unabhängigkeit und frei von jeg-  
licher externen politischen Einflussnahme beraten und  
arbeiten konnte. Die in diesem Gutachten niedergelegten  
Standpunkte geben ausschließlich die persönliche Über-  
zeugung der *ad personam* berufenen Mitglieder sowie die  
interne Meinungsbildung der institutionellen Mitglieder  
wieder. Die DEK hat alle Empfehlungen dieses Gutach-  
tens im Konsens verabschiedet.

1 Beide Dokumente stehen auf der Internetseite der DEK (abrufbar unter: [www.datenethikkommision.de](http://www.datenethikkommision.de)).

2 Weitergehende Informationen zu den öffentlichen Tagungen, inklusive der Videoaufnahmen, auf der Internetseite der DEK (abrufbar unter: [www.datenethikkommision.de](http://www.datenethikkommision.de)).



### 3. Ziele und Gegenstand des Gutachtens

Die DEK möchte mit diesem Gutachten einen Beitrag dazu leisten, unseren ethischen und rechtlichen **Ordnungsrahmen** angesichts der Herausforderungen durch digitale Technologien weiter zu entwickeln. Im Vordergrund stehen dabei die Gewährleistung der essenziellen Bedingungen für die freiheitlich-demokratische Grundordnung sowie die Nutzung der Potenziale für die Verwirklichung nachhaltigkeitsorientierter Ziele und das Gedeihen unserer sozialen Marktwirtschaft.

Angesichts der zunehmenden Erfassung personenbezogener Daten und ihrer automatisierten Verarbeitung zu unterschiedlichen Zwecken ist es ein wichtiges Anliegen der DEK, die **grundlegenden Rechte und Freiheiten des Individuums** einschließlich des Schutzes seiner Selbstbestimmung und Integrität mit dem Fortschritt, dem Wohlstand, der Sicherung der Demokratie und der Gestaltung einer zukunftsfähigen Gesellschaft zusammen zu denken. Es ist die Aufgabe des Rechtsstaats, den Einzelnen vor Datenmissbrauch und vor Diskriminierung zu schützen und für die Sicherheit aller Akteure zu sorgen. Dafür muss er wirksame Regularien und Institutionen schaffen. Gleichzeitig sollte er innovative Geschäftsmodelle ermöglichen, die den zukünftigen Wohlstand für alle sichern.

Die DEK sieht in der Digitalisierung – insbesondere in Form der zunehmenden Verfügbarkeit von Daten und des Einsatzes komplexer algorithmischer Systeme einschließlich Künstlicher Intelligenz – **große Potenziale** für technische und soziale Innovationen sowie für die Verwirklichung der Nachhaltigkeitsziele der Vereinten Nationen. Das betrifft unter anderem die Förderung der Gesundheit, die Humanisierung der Arbeitswelt, die Gestaltung nachhaltiger Städte und Gemeinden, angemessene Bildung sowie Maßnahmen für einen wirksamen Klimaschutz. Gleichzeitig sind **hohe Risiken** zu bedenken, die sich, getrieben durch den umfassenden Einsatz digitaler Technologien, für den Einzelnen, für die Gesellschaft und für die freiheitlich-demokratische Grundordnung ergeben können. Dazu gehört beispielsweise die Möglichkeit der Erstellung feingranularer Persönlichkeitsprofile (von Online Tracking über die Analyse der Stimme im Rahmen fernkommunikativer Bewerbungsgegenden bis hin zur Diagnostik von pathologischen

psychischen Zuständen anhand der Beiträge in sozialen Medien), die Möglichkeit der Ausnutzung dieser zur Steuerung und Manipulation (von individueller Preissetzung bis hin zur Manipulation demokratischer Meinungsbildungsprozesse im Rahmen des sog. Microtargeting), die Diskriminierung gesellschaftlicher Gruppen sowie die Delegation menschlicher Verantwortung an Maschinen. Die DEK ruft in diesem Zusammenhang zu einer aktiven Mitgestaltung unserer Zukunft auf, die Potenziale verwirklicht und Risiken vermeidet.

Der Weg zur Verwirklichung dieser Ziele durchläuft aus Sicht der DEK mehrere Ebenen. Er beginnt mit der ethischen Reflektion über den Wert menschlichen Handelns in einem technologiegeprägten Umfeld und der Bekräftigung **zentraler ethischer Grundsätze und Prinzipien**, auf denen unsere Gesellschaft aufgebaut ist (→ Teil B). Die Leitfragen enthalten aus Sicht der DEK eine datenfokussierte Perspektive („Daten-Perspektive“) und eine auf algorithmische Systeme fokussierte Perspektive („Algorithmen-Perspektive“) als zwei sich wechselseitig ergänzende und bedingende ethische Diskurse, die sich auch in jeweils unterschiedlichen **Governance-Instrumenten** widerspiegeln (→ Teil D).

Unter der Daten-Perspektive (→ Teil E) entwickelt die DEK allgemeine ethische Prinzipien für den **Umgang mit Daten** (→ E 1) und vor allem ethische Grundsätze von **Datenrechten und Datenpflichten** (→ E 2), um diese in eine Reihe konkreter Handlungsempfehlungen betreffend die Nutzung von Daten und den Datenzugang münden zu lassen (→ E 3 bis 5). Unter der Algorithmen-Perspektive (→ Teil F) formuliert die DEK allgemeine ethische Anforderungen an das **Design algorithmischer Systeme** (→ F 2) und an deren **risikoadaptierte Regulierung** (→ F 3). Sie leuchtet sodann im Detail die Instrumente und Institutionen einer solchen Regulierung aus, wie sie dem Gesetzgeber als Empfehlung unterbreitet werden (→ F 4 bis 8). Voraussetzung für diese Überlegungen ist ein gemeinsames Grundverständnis technischer Gegebenheiten und Zusammenhänge (→ Teil C). Das Gutachten endet mit einem Plädoyer für einen „europäischen Weg“ (→ Teil G).

Die Empfehlungen der DEK richten sich dem Auftrag gemäß primär an die deutsche **Bundesregierung** und die mit ihr verbundenen Institutionen. An einigen Stellen sind indessen auch andere Akteure angesprochen, etwa Länder und Gemeinden, Forschungseinrichtungen oder Unternehmen. Solche Empfehlungen sind insofern immer auch an die Bundesregierung gerichtet, als der Bundesregierung empfohlen wird, die anderen Akteure in ihren Bemühungen zu ermutigen und zu unterstützen. Alle Empfehlungen sind ferner im Kontext der europäischen und internationalen Entwicklungen und dort bereits bestehenden oder zu entwickelnden Institutionen und Regulierungen zu verstehen. Soweit eine Empfehlung der DEK auf **europäischer oder internationaler Ebene** umgesetzt werden sollte, ist sie als Empfehlung an die deutsche Bundesregierung zu verstehen, sich kraftvoll und zukunftsorientiert in Europa und international einzubringen.





Teil B

# Ethische und rechtliche Grundsätze und Prinzipien



# 1. Der grundsätzliche Wert menschlichen Handelns

Im Zuge der rasant fortschreitenden Entwicklung digitaler Technologien einschließlich selbstlernender algorithmischer Systeme („Künstliche Intelligenz“), die bestimmte Funktionen menschlichen Handelns in ihrer Leistungskraft übersteigen, stellt sich die **grundlegende Frage, ob das Handeln eines Menschen einen ethisch relevanten Wert an sich darstellt**, der sich jenseits von Effektivität und Effizienz verwirklicht, und der dem Funktionieren maschineller Systeme vorzuziehen ist. Die Frage stellt sich umso dringender, als der internationale Wettbewerb eine Dynamik und Eigengesetzlichkeit entfaltet, die strikt auf im Wesentlichen ökonomische Effizienz ausgerichtet ist.

Das menschliche Handeln bezieht seinen grundsätzlichen Wert aus seiner moralischen Bedeutung. Der Mensch kann Gründe für sein Handeln angeben, sich für oder gegen ein bestimmtes Handeln entscheiden, und er muss sein Handeln verantworten. Im Handeln verwirklicht und entfaltet sich der Mensch gemäß seinen Möglichkeiten, seinen Präferenzen und seinen Vorstellungen von einem sinnvollen Leben. Diese **Sinndimension des Handelns** macht es zu einem Wert, den das Funktionieren technischer Systeme niemals erhalten kann. Technik ist stets nur Mittel zu einem Zweck, den Menschen gesetzt haben. Auch wenn Menschen – hypothetisch gesprochen – entscheiden sollten, dass sich algorithmische Systeme selbst Zwecke setzen können, ist die Ermöglichung technischer Zwecksetzung ein menschlich gesetzter Zweck. Insofern kann der Einsatz technischer Systeme zwar ein Element menschlichen Handelns sein – das in bestimmten Fällen sogar ethisch geboten sein mag – technische Systeme können aber menschliches Handeln in seiner moralischen Dimension niemals vollständig ersetzen. Menschen handeln und entfalten sich als Lebewesen in mehreren Dimensionen. Auch wenn Menschenbilder in unterschiedlichen Kulturen und aufgrund unterschiedlicher religiöser Überzeugungen erhebliche Unterschiede aufweisen, enthalten sie doch alle die Dimension des Lebendigen und der moralischen Verantwortung, und sie umfassen bei aller Unterschiedlichkeit der jeweiligen Antworten die Frage nach dem Sinn des Lebens – wohingegen technische Systeme lediglich funktionieren.

Ist nun zu entscheiden, wo menschlichem Handeln der Vorzug zu geben ist vor dem Einsatz algorithmischer Systeme, so spielen viele Kriterien eine Rolle. Grundsätzlich gebürtig der höheren Effektivität der Vorrang, wenn es um die Erfüllung bestimmter begrenzter Funktionen geht. **Effektivität ist aber nicht der höchste Wert**. Sie darf die Entfaltung des Menschen in seinem eigenen Handeln nicht substanzuell einschränken, und sie muss hinter der grundlegenden ethischen Dimension des sinnvollen und gelingenden Lebens als Einzelner und in der Gemeinschaft zurückstehen. Selbst wenn also beispielsweise ein Roboter einen Menschen effektiver pflegen könnte, dürfte die menschliche Zuwendung und Sorge für den pflegebedürftigen Menschen dadurch nicht ersetzt werden. Gleichwohl kann der Einsatz von Robotern in der Pflege zusätzlich zur menschlichen Zuwendung geboten sein, wenn dadurch die Sicherheit der zu pflegenden Person wesentlich erhöht wird. Wenn aber etwa ein Arbeitnehmer durch technische Systeme dazu gezwungen wird, seine gesamten Arbeitsabläufe in den Dienst maximaler Effektivität zu stellen und dabei seine Privatsphäre oder seine persönliche Integrität verletzt werden, hat die Effektivität zurückzustehen. Menschen dürfen nicht zu Objekten von Maschinen werden, sondern müssen ihre Subjektivität erhalten können.

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 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.

## 2. Verhältnis von Ethik und Recht

Das Leben jedes einzelnen Menschen und alle Bereiche des gesellschaftlichen Zusammenlebens werden durch die exponentielle technische Entwicklung bei der Erhebung und Verwendung digitaler Daten sowie dem Einsatz algorithmischer Systeme und Künstlicher Intelligenz zunehmend geprägt. Dadurch entstehen weit reichende und tief greifende Fragen, deren Beantwortung sich an den **rechtlichen und ethischen Grundsätzen**, auf die sich die Gesellschaft in einer Demokratie verpflichtet hat, orientieren muss.

Die Maßstäbe und leitenden Prinzipien, anhand derer die Gesellschaft ihre unterschiedlichen Bereiche wie etwa die Wirtschaft, die Bildung, die Gestaltung des öffentlichen Raums, das Gesundheitswesen, den Finanzsektor, den Verkehr und die Energieversorgung gestaltet und zu gestalten hat, sind grundlegend ethischer Natur. Bei allem moralischen Pluralismus, der für ein freiheitliches System charakteristisch ist, gibt es dennoch einen gemeinsamen ethischen Ordnungsrahmen, der rechtlich in der Verfassung, und, betreffend das Verhältnis zwischen Staat und Individuum, insbesondere in den Grundrechten niedergelegt ist. Für die Frage, was dieser ethische und rechtliche Ordnungsrahmen bezogen auf einen Einzelfall und im Falle eines Konfliktes zwischen unterschiedlichen Werten oder Grundrechten bedeutet, gibt es nicht immer eindeutige Antworten. Das relativiert aber nicht die verbindliche Funktion und **konstitutive Bedeutung der ethischen Fundierung unseres Gemeinwesens**. Es betont vielmehr einmal mehr die unverzichtbare Bedeutung einer offenen und kontinuierlichen Debatte über die Gestaltung unserer Gesellschaft und ist die Grundlage demokratischer Entscheidungsprozesse, die ja gerade anerkennen, dass unterschiedliche Antworten im Rahmen der Verfassung denkbar sind.

**Ethik geht nicht im Recht auf.** Nicht jedes Detail, das ethisch relevant ist, kann und sollte rechtlich reguliert werden. Umgekehrt gibt es Aspekte rechtlicher Regulierung, die pragmatischer Art und ethisch nicht zwingend sind. Rechtssetzung muss aber immer mögliche ethische Implikationen reflektieren und ethischen Ansprüchen genügen – den verfassungsrechtlichen Vorgaben ohnehin.

Die Datenethikkommission ist der Ansicht, dass ethische Prinzipien und Leitlinien rechtliche Regulierung nicht entbehrlich machen können, wo es der verfassungsgerichtlich entwickelte **Wesentlichkeitsgrundsatz** erforderlich macht, demokratisch legitimierte und gegenüber jedermann durchsetzbare Regeln im Wege parlamentarischer Gesetzgebung zu erlassen. Internetpolitik ist auch Gesellschaftspolitik. Mit zunehmender Allgegenwärtigkeit algorithmischer Systeme einschließlich der Künstlichen Intelligenz werden auch Regeln für das gesellschaftliche Zusammenleben zu gestalten und zu sichern sein. Dies erfordert nicht nur eine fortwährende öffentliche, sondern insbesondere dort, wo Grundrechte betroffen sind, auch eine parlamentarische Debatte und gesetzgeberische Initiative. Auf durchsetzbare Regeln zugunsten von Freiwilligkeit systematisch zu verzichten erscheint angesichts der Erfahrungen mit der Rechtsdurchsetzung im Internet und der Beobachtung, dass Märkte, die durch digitale Technologien gekennzeichnet sind, in bestimmten Bereichen stärker zu einer Machtzentrale neigen, nicht sinnvoll.

**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. Andererseits können und müssen regulative Rahmenbedingungen wesentliche Rechte und Freiheiten schützen und Rechtssicherheit schaffen. Dies ist die Grundlage dafür, dass Bürgerinnen und Bürger, Unternehmen und Institutionen auf eine ethisch ausgerichtete gesellschaftliche Transformation vertrauen können. Zudem bietet das Rechtssystem mit der Möglichkeit von Regulierung auf unterschiedlichen Ebenen – vom Gesetz über Verordnungen bis hin zu Kodizes, Selbstverwaltung und Selbstverpflichtung – einen Instrumentenkasten, um anpassungsfähige und dem technologischen Fortschritt gerecht werdende Rahmenbedingungen zu gestalten.



Der **Bedarf an Orientierung geht jedoch über Regulierung weit hinaus**. Vor diesem Hintergrund haben in einer Zeit vielgestaltiger Umbrüche viele unterschiedliche Akteure wie etwa Berufsgruppen, Unternehmen und beratende Gremien auf nationaler, regionaler und internationaler Ebene Ethik-Kodizes oder Sets an leitenden ethischen Prinzipien formuliert und teilweise zur öffentlichen Diskussion gestellt.

Die Datenethikkommission begrüßt die Vielfalt des Engagements und der Diskussion über eine ethisch fundierte Gestaltung der Digitalisierung, die verdeutlicht, wie unverzichtbar die öffentliche Debatte und das **Ein-stehen aller für das Gelingen unseres Zusammenlebens** sind. In diesem Sinne orientiert sich die Datenethik-kommission – wie im Koalitionsvertrag aufgetragen – bei ihren Empfehlungen für „einen Entwicklungsrahmen für Datenpolitik, den Umgang mit Algorithmen, künstlicher Intelligenz und digitalen Innovationen“ in Verbindung mit den verfassungsrechtlichen Grundsätzen an ethischen Querschnittsprinzipien, die in unterschiedlichen Gewichtungen in allen gesellschaftlichen Bereichen relevant sind und im Folgenden in aller Kürze skizziert werden.<sup>1</sup>

<sup>1</sup> Die DEK bezieht sich mit diesem Ansatz auf dieselben Grundlagen, auf die sich auch die European Group on Ethics in Science and New Technologies (EGE) in ihrer Stellungnahme bezogen hat: EGE: Statement on Artificial Intelligence, Robotics and “Autonomous” Systems, 2018 (abrufbar unter: [http://ec.europa.eu/research/ege/pdf/ege\\_ai\\_statement\\_2018.pdf](http://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018.pdf)).

### 3. Allgemeine ethische und rechtliche Grundsätze und Prinzipien

#### 3.1 Die Würde des Menschen

Allem voraus und zugrunde liegt die Würde des Menschen, die in ethischer Hinsicht für den unbedingten Wert jedes menschlichen Lebewesens steht und als „tragendes Konstitutionsprinzip“ in der Verfassungsordnung verankert ist. Die Würde gebietet es anzuerkennen, dass jedem Menschen unabhängig von seinen Eigenschaften und Leistungen Respekt gebührt. Der **Schutz des dem Menschen inhärenten und nicht erst zu erwerbenden Wertes** beinhaltet, dass er nicht über alle seine Lebensbereiche und Tätigkeiten hinweg in ein klassifizierendes System eingeordnet („Super-Score“) oder wie ein Gegenstand mit einem Preis versehen und dementsprechend behandelt wird. Auch dort, wo menschliches Verhalten durch algorithmische Systeme gemessen und verarbeitet wird, ist stets zu berücksichtigen, dass jeder Mensch ein Individuum und kein Muster aus Datenpunkten ist. Algorithmische Systeme müssen daher stets so gestaltet sein, dass sie diesem Individualitätsanspruch des Einzelnen gerecht werden können.

Die Anerkennung der Menschenwürde erfordert, dass der Mensch immer „über der Technik“ steht, d.h. technischen Systemen nicht vollständig oder unwiderruflich unterworfen werden darf. Im konkreten Anwendungsfall kann sich dies auf unterschiedliche Ebenen der Gestaltungs- und Eingriffsmöglichkeiten beziehen, gleichwohl muss der **Grundsatz der menschlichen Gestaltungshoheit** gewahrt bleiben. Der Mensch ist in der Mensch-Maschine-Interaktion verantwortlicher Akteur und darf nicht als fehlerhaftes Wesen betrachtet werden, das von der Maschine optimiert oder perfektioniert werden muss. Vielmehr nutzt der Mensch algorithmische Systeme, um seine Ideen und Ziele besser, schneller und weniger fehlerbehaftet zu erreichen.

Der Würdeschutz umfasst darüber hinaus, dass der **Mensch als Beziehungswesen** technologisch nicht über die Art der Beziehung in die Irre geführt wird, wie es etwa der Fall sein könnte, wenn er mit einem Bot spricht und ihm systematisch vorgetäuscht wird, er spreche mit einem Menschen. Insbesondere schützt die Menschenwürde auch die **psychische Integrität der Einzelnen**. Untersagt ist daher die Nutzung von datengetriebenen Systemen zu manipulativen Zwecken, insbesondere wenn dies auf der Basis umfassender und feingranularer Persönlichkeitsprofile beruht. Gleichermaßen gilt, wo algorithmische Systeme **Einzelne oder Gruppen systematisch diskriminieren**, also etwa herabstufen oder aus ethisch unvertretbaren Gründen von der Inanspruchnahme bestimmter Leistungen ausschließen oder bei der Beteiligung am demokratischen Diskurs systematisch täuschen.

#### 3.2 Selbstbestimmung

Mit der Würde des Menschen ist die Möglichkeit der Selbstbestimmung eng verbunden. Die Bestimmung seiner Lebensziele und seiner Lebensweise und damit die Bestimmung, Entfaltung und Darstellung seines Selbst sind **Ausdruck der Freiheit** des Menschen. Eine Gesellschaft, die Freiheit ernst meint, schafft Rahmenbedingungen, in denen sich die Bürgerinnen und Bürger in allen ihren Unterschiedlichkeiten frei entfalten können und gegenseitig die Freiheit des oder der jeweils Anderen respektieren. Entfaltungsbedingungen für ein selbstbestimmtes Leben in Freiheit bedeuten beispielsweise, dass technische Systeme den Handlungsspielraum des Menschen nicht ohne einen ethisch bedeutsamen Grund einschränken und beherrschen dürfen. Selbstbestimmung ist nicht ausschließlich individualistisch auszurichten. Der Mensch ist ein Beziehungswesen und entfaltet sein Leben in einem sozialen Miteinander mit vielfältigen wechselseitigen Verbindungen und Einflussnahmen.



Die Regeln dieses Miteinanders werden durch **kulturelle und sozialnormative Rahmenbedingungen** im gesellschaftlichen Zusammenleben über die Zeit geprägt. Zudem werden sie durch Recht gestaltet, in einer demokratischen Gesellschaft vor allem dort, wo Macht- und Informationsungleichgewichte herrschen.

Je mehr Informationen Dritte über den Einzelnen gesammelt haben, desto schwieriger wird es, in sozialen Situationen unbefangen zu agieren oder sich gar als Individuum ganz neu zu erfinden. Verhindert werden muss, dass Praktiken der Datensammlung und -auswertung persönliche und soziale Profile routinemässig an vielen Stellen erstellen und dauerhaft „zementieren“. Insofern umfasst Selbstbestimmung auch ein **Recht, die eigene Identität auszubilden und zu ändern** und damit auch die Möglichkeit eines neuen Anfangs. Auch die Entscheidung darüber, wie ein Individuum in der Öffentlichkeit auftritt sowie der Schutz gegen eine falsche Darstellung in der Öffentlichkeit sind daher vom Recht auf Selbstbestimmung umfasst.

Selbstbestimmung bedeutet auch, dass Menschen nicht nur **Verantwortung** übernehmen dürfen, vielmehr müssen sie sie übernehmen und müssen ihr auch gerecht werden. Verantwortung liegt nie bei einer Maschine, sondern immer beim Menschen, gegebenenfalls im Rahmen von institutioneller Verantwortung. Auch wenn ein technisches System eingesetzt wird, um im Rahmen einer automatisierten Datenauswertung Schlussfolgerungen wie die Gewährung eines Kredites anzuwenden, ist es die Verantwortung des Menschen, dieses System in einer ethisch vertretbaren Weise zu entwickeln und einzusetzen.

Eine wichtige Ausprägung der Selbstbestimmung ist die **informationelle Selbstbestimmung**. Sie umfasst das Recht des Einzelnen zu bestimmen, wer wann und zu welchem Zweck welche personenbezogenen Daten erheben und verwenden darf. Durch die informationelle Selbstbestimmung kann der Einzelne seine Handlungsfreiheit und Privatheit in dem Umfang schützen, wie es ihm wichtig ist, und er kann auch im öffentlichen Raum bestimmen, als welche Persönlichkeit er wahrgenommen und behandelt werden möchte.

Im Zeitalter der Digitalisierung kommt dem Einzelnen über seine informationelle Selbstbestimmung hinaus als selbstbestimmtem Akteur in der Datengesellschaft eine besondere Bedeutung zu. Hierauf wird durch den Begriff der **digitalen Selbstbestimmung** Bezug genommen. Diese schließt die Kompetenz ein, selbst zu bestimmen, mit welchen Inhalten jemand in Beziehung zu seiner Umwelt tritt und wie jemand die eigene Persönlichkeit interaktiv entfaltet. Sie umfasst unter bestimmten Bedingungen etwa auch die selbstbestimmte wirtschaftliche Verwertung der eigenen Datenbestände sowie den selbstbestimmten Umgang mit nicht-personenbezogenen Daten, die durch den Betrieb eigener Geräte generiert werden. Digitale Selbstbestimmung geht dabei immer auch mit digitaler Selbstverantwortung einher.

Nach Auffassung der DEK gilt ein Recht auf digitale Selbstbestimmung auch für **Unternehmen und juristische Personen**. Juristische Personen können sich nicht auf die im Rahmen des allgemeinen Persönlichkeitsrechts über Art. 1 Abs. 1 GG geschützte Menschenwürde und somit nicht auf den damit verbundenen absolut geschützten Kernbereich der Persönlichkeitsentfaltung berufen. Allerdings verfügen juristische Personen über ein durch Art. 2 Abs. 1 GG in Verbindung mit Art. 19 Abs. 3 GG geschütztes Persönlichkeitsrecht, das auch ein informationelles Selbstbestimmungsrecht beinhaltet.

Im Hinblick auf Verbraucher sind ihre Selbstbestimmung und die Ermöglichung bewusster Konsumententscheidungen Voraussetzungen einer optimalen Ressourcenallokation und Wohlfahrtsmaximierung innerhalb der Volkswirtschaft. Ein Erodieren der für die Selbstbestimmung erforderlichen **Kompetenzen von Verbrauchern**, etwa durch einen übermäßigen Einsatz von Entscheidungsassistenten und damit verbundene Habituationseffekte, wirft ethische Fragen zur Fremdbestimmung und Entscheidungsfreiheit von Individuen, aber auch gesellschaftlicher Steuerung durch einzelne marktmächtige Akteure auf.

### 3.3 Privatheit

In enger Verbindung mit dem **Schutz der Menschen-würde und der Selbstbestimmung** steht wesentlich auch der Schutz der Privatheit. Die ethisch hochrangige Bedeutung, die eigene Privatsphäre bewahren zu können und sich in der Gewissheit der geschützten Privatheit auch in der Öffentlichkeit bewegen zu können, begründet das Recht des Einzelnen, darüber zu bestimmen, wer welche persönlichen Informationen zu welchem Zeitpunkt und zu welchem Zweck erhalten darf (→ informationelle Selbstbestimmung, oben 3.2). Die gesetzliche Regelung eines verantwortungsvollen Umgangs mit persönlichen Daten gehört zum Schutz der Würde des Menschen.

Privatheit umfasst darüber hinaus die **Wahrung der Integrität der persönlichen Identität**. Diese kann beispielsweise verletzt werden, wenn algorithmische Systeme anhand von Daten, die zu ganz anderen Zwecken entstanden sind, die Persönlichkeit eines Menschen, seine Präferenzen und Neigungen gleichsam ausrechnen, um dies unabhängig von oder sogar gegen seinen Willen zu eigenen Zwecken zu nutzen.

In einer Gesellschaft, deren unterschiedlichen Bereiche zunehmend durch datengetriebene Technologien geprägt werden, gilt es, die **Aufmerksamkeit zunehmend auf die Verwendung der Daten zu richten**. Viele Menschen geben auch personenbezogene Daten der Öffentlichkeit oder Teilen davon preis, da sie bestimmte Produkte und Services genießen oder einen Beitrag zum öffentlichen Wohl leisten wollen. Sie nur darauf zu verweisen, dass sie sparsam mit der Freigabe ihrer Daten umgehen sollen, hilft hier nicht weiter. Vielmehr müssen sie sich durch eine wirksame Regulierung darauf verlassen können, dass mit ihren Daten verantwortungsvoll umgegangen wird und ethisch unzulässige Verwendungen verboten sind.

### 3.4 Sicherheit

Algorithmische Systeme werfen zudem wichtige Fragen der Sicherheit auf. Je nach Anwendungskontext kann die Sicherheit der Nutzer gefördert oder gefährdet werden. Die ethische und rechtliche Relevanz von Sicherheit besteht in ihrer **Funktion, hochrangige Güter zu schützen**, wie etwa die körperliche und psychische Gesundheit und die Privatheit von Individuen oder auch die öffentliche Sicherheit, den Frieden sowie die Freiheit und Gleichheit demokratischer Wahlen.

Sicherheit kann sich auf die Datenerhebung und -verwendung beziehen und betrifft damit auch den **Schutz der Privatheit**. Datenskandale großen Ausmaßes, die in den letzten Jahren bekannt wurden, haben deutlich gemacht, dass sich die Verletzung der Privatheit und die Verwendung personenbezogener Daten zu manipulativen Zwecken bis in den Bereich der Politik mit weitreichenden Folgen auswirken kann.

Auch die **körperliche und emotionale Sicherheit** des Menschen bei der Bedienung und bei der Anwendung algorithmischer Systeme ist zu bedenken. Dies führt zu hohen Anforderungen beispielsweise in der Mensch-Maschine-Interaktion. So ist etwa beim Einsatz eines Pflegeroboters sicherzustellen, dass sowohl die zu pflegende als auch die pflegende Person dadurch in ihrer körperlichen sowie psychischen Integrität nicht geschädigt werden.

Darüber hinaus kann die **Sicherheit der Umwelt** berührt sein. Bei algorithmisch gesteuerten öffentlichen Infrastrukturen wie etwa dem Verkehr oder der Energie- und Wasserversorgung kann es bei Fehlfunktionen zu massiven Schädigungen kommen.

Zudem können algorithmische Systeme in sich unsicher sein und damit Fehlfunktionen verursachen oder sogar **Einfallsstore für Angriffe und Manipulationen** in bösartiger Absicht bieten. Auch über eine solche systeminterne Anfälligkeit hinaus ist die Problematik des Missbrauchs eines algorithmischen Systems für schädliche Zwecke zu bedenken.



### 3.5 Demokratie

Digitale Technologien sind auf komplexe Art und Weise für die Entfaltung der Grundrechte (insbesondere die Meinungs- und Informationsfreiheit, das (informationelle) Selbstbestimmungsrecht und das Fernmeldegeheimnis, die Versammlungs- und Vereinigungsfreiheit sowie die Berufsfreiheit und das Eigentumsrecht), für die Demokratie, für die Sicherung von Vielfalt, für eine offene gesellschaftliche Debatte sowie für freie und gleiche Wahlen **systemrelevant**. Beispielsweise ermöglichen soziale Medien eine niedrigschwellige und grundsätzlich begrüßenswerte Beteiligung aller Bürgerinnen und Bürger an einer Debatte über die Gestaltung unserer Zukunft. Sie können aber auch Gefahren im Hinblick auf Manipulation und Radikalisierung mit sich bringen. Dem sollte der Staat durch Regeln und Institutionen, die Fehlentwicklungen und missbräuchliche Verwendung verhindern, entschieden entgegentreten.

Auch ist nicht zu verkennen, dass mit der Verbreitung des Internets der wirtschaftliche Niedergang des Journalismus und seiner privat finanzierten Pluralität einhergeht. Die elektronische Öffentlichkeit ersetzt aber in keiner Weise die für die Demokratie wichtige Funktion des Journalismus als „vierte Gewalt“ bzw. als „Wachhund der Demokratie“, also der Kontrolle von Macht und Wahrheitsanspruch durch systematische und unabhängige Nachforschung und Kritik. Die Gefahr des steuernden Einflusses machtvoller **Medienintermediäre mit Torwächterfunktion** für die demokratische Willensbildung kann unter bestimmten Umständen eine erhebliche Bedrohung für die Demokratie darstellen, der aus ethischen und verfassungsrechtlichen Gründen gesetzlich entgegenzuwirken ist.

Auch **Erziehung und Bildung** spielen bei der Sicherung einer freiheitlich-demokratischen Grundordnung eine herausragende Rolle, da sie auf vielfältige Weise die für eine Demokratie konstitutive, kritische Beteiligung der Bürgerinnen und Bürger an der Gestaltung der Gesellschaft, das Verständnis und die Einschätzung gesellschaftlich relevanter Zusammenhänge und Entwicklungen und damit auch letztlich das Vertrauen in eine wertebasierte, gestaltbare Zukunft beeinflusst. Durch Erziehung und Bildung zu vermittelnde Kompetenzen betreffen sowohl technische und mathematische als auch ethische, rechtliche, ökonomische und sozialwissenschaftliche Aspekte.

### 3.6 Gerechtigkeit und Solidarität

Für ein freiheitlich-demokratisches Zusammenleben in Frieden und Wohlstand ist unter anderem konstitutiv, dass die Gesellschaft und ihre Institutionen die Prinzipien der Gerechtigkeit umsetzen. Angesichts der massiven daten- und technologieinduzierten Anhäufung von wirtschaftlicher und damit auch gesellschaftlicher Gestaltungsmacht bei wenigen großen Unternehmen stellen sich neue Fragen einer gerechten Wirtschaftsordnung. Aber auch weitere Fragen von **Zugangs- und Verteilungsgerechtigkeit**, etwa bei Einkommen und im Gesundheitswesen, können durch die Verfügbarkeit großer Datens Mengen und die Digitalisierung von Prozessen wie in der Arbeitswelt und der medizinischen Versorgung betroffen sein – im Sinne einer gerechteren Verteilung knapper Ressourcen, aber auch im Sinne einer Benachteiligung oder Diskriminierung bestimmter Personengruppen.

Gerechtigkeit ist zudem eng verbunden mit der Möglichkeit zur Beteiligung. Durch die – auch digital unterstützte – **Stärkung partizipativer Prozesse** kann bei technologieinduzierten sozialen Umbrüchen ein wichtiger Beitrag zur Beförderung sozialer Innovationen geleistet werden. Ein gerechtigkeitsrelevantes Problem besteht nicht zuletzt in einer Diskriminierung von Personen oder Personengruppen, die – insbesondere bei Anwendung selbstlernender algorithmischer Systeme – ohne rechtfertigende Gründe benachteiligt werden.

Die klare **Zuordnung von Verantwortung und Rechenschaftspflichten** ist in einem demokratischen Rechtsstaat unverzichtbar. Es bedarf einer ausreichenden Transparenz und Erklärbarkeit, um eine Überprüfbarkeit algorithmischer Systeme in Abhängigkeit von ihrem konkreten Schädigungspotenzial zu gewährleisten. Zudem muss es Möglichkeiten geben, unter bestimmten Voraussetzungen den Rechtsweg zu beschreiten und jemanden gegebenenfalls in die Verantwortung nehmen zu können, also haften zu lassen.

Der **Zugang zu digitalen Ressourcen** über das Internet ist heute eine elementare Voraussetzung digitaler und damit auch sozialer Teilhabe. Den Staat trifft als Teil seines Gewährleistungsauftrages die Pflicht, dafür zu sorgen, dass Bürgerinnen und Bürger flächendeckend sowohl stationär als auch mobil in angemessenem Umfang auf eine zeitgemäße Internetinfrastruktur zugreifen können. Sein Bildungsauftrag ist es, die Bürgerinnen und Bürger zu befähigen, sich selbstbestimmt in der digitalen Welt zu bewegen und Chancen sowie Risiken der Internetnutzung richtig einzuschätzen zu können.

Teilhabemöglichkeiten fördern auch den **sozialen Zusammenhalt**. Dieser basiert zudem auf einer Grundhaltung und einer institutionellen Verankerung von gesellschaftlicher Solidarität. Digitale Technologien können zu ihrer Stärkung beitragen, sie können sie aber auch schwächen oder zerstören. Bei der Anwendung von algorithmischen Systemen in bestimmten gesellschaftlichen Bereichen wie etwa im Versicherungswesen oder in der Vermittlung von sozialen Teilhabechancen ist auf zum Teil subtile Effekte mit der Folge einer systemischen Schwächung von Solidarität zu achten. So können nachvollziehbare und individuell gerechtfertigt erscheinende datengetriebene Differenzierungen und Ungleichbehandlungen durchaus in der Summe zu einer Entsolidarisierung mit bestimmten Personengruppen führen – auch solchen, die auf eine gesellschaftliche Unterstützung in besonderem Maße angewiesen sind.

### 3.7 Nachhaltigkeit

Digitale Technologien bringen große Chancen für eine effizientere Ressourcenbewirtschaftung und innovative Geschäftsmodelle mit sich. In der allgemeinen Diskussion steht dieser ökonomische Aspekt meist im Vordergrund. Weniger diskutiert wird aber bislang, ob die digitalen Technologien auch zu ökonomischer Nachhaltigkeit beitragen. Zusätzlich sind die Aspekte ökologischer und sozialer Nachhaltigkeit zu bedenken. Die Vereinten Nationen haben **17 Ziele für nachhaltige Entwicklung auf ökonomischer, sozialer und ökologischer Ebene** formuliert, die für alle Staaten gelten und bis 2030 umgesetzt sein sollen. Digitale Technologien können dazu beitragen, diese nachhaltigen Ziele zu verwirklichen, wie es etwa von der International Telecommunication Union (ITU) mit „AI for good“ verfolgt wird. So hat jüngst der Wissenschaftliche Beirat der Bundesregierung Globale Umweltveränderungen (WBGU) die Vision einer KI-basierten feingranularen Umweltsensorik entworfen, die ein bisher ungekanntes „umfassendes und echtzeitnahe Monitoring der natürlichen Erdsysteme, ihrer Zustände und ihrer Entwicklung“ ermöglichen und damit einen zentralen Baustein für eine künftige digitale Nachhaltigkeitspolitik bilden soll.

Digitale Technologien fördern allerdings nicht nur Ressourcen, sie erfordern auch Ressourcen etwa durch einen immer stärker anwachsenden Bedarf an elektrischer Energie und durch die Angewiesenheit digitaler Produkte auf bestimmte „seltene Erden“, die nur noch begrenzt und nur in bestimmten Staaten verfügbar sind. Zudem geht ihr Abbau mit massiven ökologischen Schäden einher. Das wirft Fragen in Bezug auf nachhaltige ökonomische und ökologische Entwicklung auf und berührt zusätzlich **Fragen der internationalen Gerechtigkeit** beim Umgang mit natürlichen Ressourcen sowie der globalen Verantwortung für künftige Generationen.



Nachhaltigkeit ist auch gefordert, was die Ressource menschlichen Wissens und menschlicher Kompetenz betrifft: In dem Maße, wie sich digitale Technologien entwickeln und dem Menschen Aufgaben abnehmen, werden nicht nur neue Kompetenzen hinzugewonnen, sondern es gehen auch **Kompetenzen des Menschen** verloren. Dies erfordert eine Diskussion, welche Verantwortlichkeit gegenüber der nächsten Generation besteht, und Maßnahmen, bestimmte Kompetenzen und Unabhängigkeiten zu bewahren und zu entwickeln.

Die umfassende und regelmäßige **Technikfolgenabschätzung**, wie sie dieses Gutachten an mehreren Stellen einfordert, wird auch die Aspekte der Nachhaltigkeit der neuen Technologien in ihren verschiedenen Ausformungen mit einbeziehen müssen. Der Gesetzgeber ist hier gefordert, Verantwortung für Nachhaltigkeit in die Regulierung der Datenwirtschaft und der algorithmischen Systeme einzubauen, beispielsweise durch die Einführung einer Pflicht zur Offenlegung der gesamten Energiebilanz eines energieintensiven Blockchain-Systems.

Zudem sollten **öffentliche Investitionen** in Datenwirtschaft und algorithmische Systeme insbesondere darauf ausgerichtet sein, Nachhaltigkeitsziele zu verfolgen, wie sie die Vereinten Nationen formuliert haben. Die Entwicklung von Daten und algorithmischen Systemen etwa zur Erfassung und Kontrolle von Umwelteinwirkungen und Entwicklungen in der Umwelt wie auch Systeme zur Optimierung und Reduzierung von Energie- und Ressourcenverbrauch sollten im Vergleich zu nur kurzfristigen wirtschaftlichen Gewinnen vorrangig Gegenstand öffentlicher Förderung sein. Auch sollten nachhaltigkeitsorientierte soziale Innovationen verstärkt gefördert werden, die gesellschaftliche Kreativität und Partizipation stärken.

Teil C

# Technische Grundlagen



Datenintensive IT-Anwendungen haben unser Zusammenleben, unsere Arbeitswelt, Wirtschaft, Wissenschaft und Gesellschaft nachhaltig beeinflusst. Smartphones sind allgegenwärtige Begleiter, wir nutzen täglich Suchmaschinen, verlassen uns auf Empfehlungssoftware, schicken Text- oder Sprachnachrichten an Familie und Freunde, regulieren die Temperatur im Haus von der Ferne oder lassen uns durch Navigationsgeräte von einem Ort zum anderen leiten. Diese Möglichkeiten beruhen auf einer Reihe technologischer Entwicklungen der letzten Jahrzehnte. Im Folgenden sollen wichtige technologische Grundlagen beschrieben werden. Ziel ist hierbei nicht eine vollumfängliche Darstellung, sondern das Herausarbeiten zentraler Elemente, um resultierende Probleme und Ansatzpunkte für mögliche Governance identifizieren zu können.

## 1. Status Quo

Die Leistungssteigerung und Verkleinerung der physischen Komponenten von IT-Systemen (Hardware) zur Speicherung und Verarbeitung von Daten, zusammen mit einer sich stets verbessernden Konnektivität – sowohl kabelgebunden als auch über Funk – eröffnen die **Erschließung ganz neuer Anwendungsbereiche**. Smartphones, Tablets, Wearables durchdringen zusammen mit Sensoren, Aktuatoren und teilweise „autonom“ agierenden Systemen, wie z.B. Robotern, die Arbeits- und Lebenswelt. So ist in weiten Teilen eine permanente und mobile Nutzung des Internets möglich, die beispielsweise in Kombination mit umfangreicher Sensorik in Smartphones (Geolokalisierung, Gyrosensoren, Kameras, Mikrofon usw.) neben Texteingaben auch Bild-, Video- und Audioaufnahmen fast von jedem Ort zu jedem Zeitpunkt im Internet bereitstellen kann. Neben der sozialen Vernetzung und Kommunikation ermöglicht diese technologische Durchdringung darüber hinaus die Vernetzung von Geräten zum sog. Internet der Dinge (engl. Internet of Things, IoT).

Die analoge Welt und die digitale Welt lassen sich nicht mehr genau trennen: Die analoge Welt enthält zunehmend Komponenten, die Informationen aus der analogen Welt in die digitale Welt weitergeben, doch ebenso werden auch digitale Informationen in der analogen Welt zur Verfügung gestellt, so dass beide Welten mehr und mehr zu einer **hybriden Welt** verschmelzen.

Bedingt durch umfangreiche Sensorik, durch das IoT und immer günstigere Datenspeicher ergibt sich ein **exponentiell ansteigendes Datenaufkommen**. Die Verarbeitung dieser großen Datenmengen erfordert spezialisierte Werkzeuge. Gleichzeitig hat dieses Datenaufkommen zusammen mit der leistungsfähigen Hardware die breitflächige Anwendung von Verfahren des maschinellen Lernens befördert. Diese Verfahren erzielen teilweise beeindruckende Ergebnisse, z.B. im Bereich des Sprach- und Bilderkennens.

Die Leistungssteigerung in der Spracherkennung und Videoverarbeitung reicht aber mittlerweile auch so weit, dass die **Grenzen zwischen der Wirklichkeit und computergenerierten Informationen** verschwimmen können. Dann ist es für Menschen nicht mehr klar, ob sie mit einem Sprach-Bot reden oder ob sie ein generiertes Video anschauen, in dem Menschen Worte in den Mund gelegt wurden, die diese nie gesagt haben (sog. Deep Fakes).



## 2. Systemelemente

### 2.1 Daten

#### 2.1.1 Begriff und Eigenschaften von Daten

Aufgrund des Arbeitsauftrags der DEK liegt der Fokus des Gutachtens auf Daten, die **digital und maschinenlesbar** sind. Die Basis dieser Daten sind binäre, elektrische Impulse. Diese Impulse können nur für den Augenblick als Signal existieren, etwa als ein Steuerungsimpuls für ein technisches System, oder auch persistieren, d.h. auf einem Medium gespeichert sein.

**Daten sind vielfältig.** Der Begriff „Daten“ versammelt eine immense Diversität von Erscheinungsformen unter einem Begriffsdeckel. So lassen sich Daten etwa anhand des Datentyps (z.B. binäre, nominale, ordinale, metrische und textuelle Daten), des datengenerierenden Prozesses (z.B. Umfragedaten, Sensordaten), des Erhebungsbereichs (z.B. Finanzdaten, Wetterdaten) oder ihrer Funktion in einem digitalen System (z.B. Log-in-Daten, Trainingsdaten) einteilen. Eine weitere Einteilung setzt am Grad der Verarbeitung (Veredelung) an: Ohne eine weitere Verarbeitung spricht man auch von „Rohdaten“, je nach dem Grad der Strukturierung (Normalisierung) von „strukturierten“ oder „unstrukturierten“ Daten. Daten können der Input in ein System sein oder auch der Output, der wiederum der Input in das nächste System sein mag. Daten können zugleich digitale Vermögensgüter (digital assets) repräsentieren, wie multimediale Inhalte oder Einheiten von Kryptowährungen. Von erheblicher juristischer Bedeutung ist zudem die Differenzierung zwischen personenbezogenen und nicht-personenbezogenen Daten.

**Daten sind nicht immer Information.** Um die **binären, elektrischen Impulse**, welche die Basis für digitale Daten darstellen, zu verstehen, d.h. um aus Daten „Information“ werden zu lassen, ist es erforderlich, den **Kontext** und die **Semantik** (Bedeutung) zu kennen. Der Kontext kann durch den Ursprung der Signalerzeugung gegeben sein, beispielsweise die Kenntnis, von welchem Sensor ein Signal gesendet wird. Die Semantik gibt an, welche Information in einer gewissen Abfolge von binären Signalen liegt, z.B. kann bei einer Umfrage die Ziffer 4 die Anzahl der Kinder im Haushalt oder genauso gut die Anzahl der im letzten Halbjahr gekauften Zahnpastatuben sein. Kontext und Semantik findet man in Metadaten, Domaintabellen, Ontologien, Identifikatoren und weiteren die Datenwerte ergänzenden technischen Spezifikationen. In diesem Gutachten ist mit dem Begriff Datum immer auch die Kenntnis von Kontext und Semantik gemeint.

**Daten sind von unterschiedlicher Qualität.** Die meisten Daten – oder besser gesagt die in ihnen enthaltene Information – sollen die Realität möglichst getreu abbilden, indem etwa den richtigen Entitäten (Informationsobjekten) diejenigen Attribute zugeordnet werden, die diese Entitäten auch in der Realität aufweisen. Dabei kann es zu Fehlern kommen. Es gibt auch viele Daten, die eine Wahrscheinlichkeit für die Realität, oder für eine künftige Realität, zum Ausdruck bringen sollen, oder auch Daten, die eine hypothetische Realität konstruieren sollen oder gar keinen Bezug zur Realität haben. In allen Fällen kann der Datenbestand **fehlerbehaftet** sein. Davon zu unterscheiden sind Situationen, in denen Daten das leisten, was sie vorgeben zu leisten, diese Leistung aber **ungeeignet** ist, um ein bestimmtes Ziel zu erreichen, etwa eine bestimmte Analyse durchzuführen (z.B. die Daten sind nicht granular genug oder zu alt oder nicht vollständig genug).

Entscheidend für datengetriebene Systeme ist die Qualität der verwendeten Daten: Selbst ein perfekter Algorithmus wird keine Qualität liefern, wenn er schlechte, d.h. ungenaue oder inadäquate Daten als Eingabe erhält. Datenqualität ist kein absoluter Wert, die relevanten Datenqualitätsdimensionen und deren Qualitätslevel sind abhängig von der spezifischen Verwendung (→ s. Abb. 1).



Abbildung 1: Beispiel für unterschiedliche Qualitätsanforderungen je nach Verwendung

### 2.1.2 Data Management

**Daten sind nicht gegeben, sondern gemacht.** Im Prozess der Erhebung, Aufbereitung und Verarbeitung von Daten treffen Menschen vielfältige Entscheidungen, welche Konsequenzen für die weitere Datennutzung haben. Fehlt beispielsweise zu einem Datensatz Kontext oder Semantik, kann das Potenzial dieser Daten unwiederbringlich verloren sein. Um dies zu vermeiden, ist sorgfältiges **Data Management** erforderlich.

Möchte man Daten aus unterschiedlichen Quellen zusammenführen, ist sicherzustellen, dass sowohl auf technischer als auch auf semantischer Ebene eine solche Zusammenführung möglich ist. Dies bezeichnet man als Interoperabilität. Es gilt, eine Abbildung der Daten aus diesen Quellen aufeinander zu finden, die der jeweiligen Semantik der Daten gerecht wird. Ist die Interoperabilität von besonderer Bedeutung, sollte eine **Standardisierung** bezüglich der technischen Spezifikationen (Formate, Metadaten zur Beschreibung usw.) angestrebt werden. Dabei spielen etwa Referenzdaten eine wichtige Rolle, also standardisierte Schemata oder Ontologien, die beispielsweise von nationalen oder internationalen Institutionen verantwortet werden (z.B. die von der WHO herausgegebene internationale Klassifikation von Krankheiten).

### 2.1.3 Big Data und Small Data

Nicht um einen eigenen Datentyp, sondern um einen neuen methodischen Ansatz zum Auffinden von Zusammenhängen handelt es sich bei **Big Data**. Eine besonders bekannte, frühe Definition von Big Data geht auf Laney<sup>1</sup> zurück, welcher Big Data durch drei Vs charakterisiert: *volume, velocity und variety* – eine große Menge an vielfältigen Daten aus potenziell unterschiedlichen Quellen, die mit hoher Geschwindigkeit (oft in Echtzeit) generiert werden. Um in der Lage zu sein, vielfältige, in ihrer Qualität variierende, sich schnell verändernde große Datenmengen zu bearbeiten, bedarf es besonderer Technologien. Besonders geeignet ist die Analyse großer Datensätze (Big Data), wenn aus einer Vielzahl möglicher Zusammenhänge Hinweise auf diejenigen ermittelt werden sollen, die vielversprechend sind. Beispielsweise ist es für die medizinische Forschung hilfreich, aus der Vielzahl von Umweltfaktoren, die eine Krankheit möglicherweise begünstigen, mit Hilfe von Big Data zunächst einige wahrscheinliche Kandidaten zu identifizieren und sodann nur für diese aufwändige und exakte Experimente oder Studien durchzuführen. Ein besonderes Problem dieses Ansatzes ist es, dass er zunächst einmal nur **Korrelationen**, aber keine Kausalitäten aufzeigt. Es können daher auch ganz falsche Kandidaten identifiziert werden.

1 Doug Laney: 3D Data Management. Controlling data Volume, Velocity and Variety, META Group Inc., 2001.

In vielen Bereichen werden niemals ausreichend große Datenmengen vorliegen, die mit den Big-Data-Methoden analysiert werden können (z.B. mag der Kundenstamm eines mittelständischen Unternehmens nie größer als 200 Kunden werden, die Anzahl an Parteien in einem Land ist selten dreistellig). Auch für den Bereich der **Small Data** kann mit geeigneten Analysemethoden viel Wissen und Information aus den Daten extrahiert werden. Nicht die Menge an Daten ist entscheidend. Es gilt vielmehr, Daten mit adäquater Qualität und in für die Fragestellung ausreichender Menge mit geeigneten Werkzeugen zu kombinieren, um gute Datenanalysen zu ermöglichen.

## 2.2 Datenverarbeitung

### 2.2.1 Algorithmen

Während im Datenschutz unter **Verarbeitung** die Gesamtheit des Prozesses von der Datengenerierung über die Extraktion zur Speicherung und jedwede Transformation der Daten selbst bezeichnet wird (Art. 4 Nr. 2 DSGVO), verwenden die mathematisch-technischen Disziplinen den Begriff in erster Linie, um die Nutzung der Daten zu bezeichnen. Dieses Verständnis liegt auch den folgenden Ausführungen zu Grunde.

Jede digitale Datenverarbeitung folgt dem **EVA (Eingabe-Verarbeitung-Ausgabe)-Prinzip**: Daten gehen als Eingabe (Input) ein, werden verarbeitet und als Ergebnis ausgegeben. Jede interne Verarbeitung in einem EVA-System beruht auf einem Algorithmus: einer operativen Verarbeitungsvorschrift, die einen Ablaufplan als eine Folge von Verarbeitungsschritten spezifiziert, um ein angestrebtes Ergebnis durch die schrittweise Transformation der Eingangsdaten zu erzielen. Schon Euklid spezifizierte einen Algorithmus als Rechenanleitung zum einfachen Auffinden des größten gemeinsamen Teilers zweier natürlicher Zahlen. Der Begriff leitet sich aus dem Namen des arabischen Mathematikers al-Chawarizmi (latinisiert Algorismi) ab, der um 830 n. Chr. eine Sammlung von Rechenvorschriften für das Lösen algebraischer Gleichungen veröffentlicht hat.

Insbesondere in der modernen Informatik ist der Begriff „Algorithmus“ von fundamentaler Bedeutung. Wenn man eine gegebene Fragestellung mittels Datenverarbeitung beantworten möchte, muss man einen Algorithmus sowohl korrekt implementieren als auch produktiv einsetzen. Dies setzt die Kenntnis des Algorithmus voraus. In vielen Situationen ist der zum Ziel führende Algorithmus allerdings noch nicht bekannt und die Kernaufgabe besteht zunächst darin, **einen geeigneten Algorithmus zu finden**. Für viele praktisch relevante Situationen können die Verarbeitungsvorschriften aus Fachwissen, bekannten Modellen oder auch Rechtsvorschriften direkt abgeleitet, d.h. deduziert werden. In anderen Situationen ist unser Verständnis des Zusammenhangs noch nicht weit genug ausgereift, um diesen in mehr oder weniger einfachen mathematischen Formeln beschreiben zu können.

Fehlt dieser Kenntnisrahmen, gibt es diverse Strategien, um einen Algorithmus zu finden, wie z.B. per Zufall, Versuch und Irrtum oder durch **Schließen** (auch Ableiten) aus Daten. Letztere Herangehensweise folgt dem Prinzip der Induktion: Aus Einzelfällen wird versucht, auf eine übergeordnete Regel zu schließen. Hierbei dienen die Daten als Einzelfälle. Findet man eine übergeordnete Regel, die zur Lösung der Fragestellung geeignet ist, hat man damit einen geeigneten Algorithmus gefunden. Dabei ist zu beachten, dass es durchaus mehrere zur Lösung geeignete Regeln geben kann. Des Weiteren ist eine Induktion nicht zwingend korrekt. Es ist möglich, aus vorliegenden Einzelfällen zu einem Schluss zu kommen, der teilweise oder vollständig falsch ist.

### 2.2.2 Statistisches Schließen

Das Schließen aus Daten ist das Kerngebiet der Statistik. Die **Verfahren des statistischen Schließens** aus Daten können sowohl zur Bearbeitung von Fragestellungen angewandt werden, deren inhärente Logik unbekannt ist, als auch insbesondere in Situationen, in denen der Zufall ein Teil des zu modellierenden Prozesses ist, beispielsweise um die Regenwahrscheinlichkeit für den Folgetag abzuschätzen oder Personen zu identifizieren, die mit einer hohen Wahrscheinlichkeit ein Produkt kaufen. Es gibt viele Methoden des statistischen Schließens: Die Spanne reicht von diversen Formen der Regression (lineare, logistische oder regularisierte Ridge Regression) über Support Vector Machines (SVM), Bayesian Networks und Regel-lernern (z.B. Aprioiri, CART und Random Forest) bis hin zu Neuronalen Netzen (NN). Alle diese Verfahren eignen sich zur Extraktion von Information aus vorliegenden Daten. Einige sind darauf spezialisiert, Regressionsfragestellungen zu lösen, etwa die Frage nach der erwarteten Körpergröße eines Kindes in Anbetracht der Größe der Eltern. Andere – zum Beispiel SVM, CART, NN – werden eingesetzt, wenn es sich um Klassifikationsfragestellungen handelt: z.B. schwanger oder nicht schwanger, Hund oder Katze. Ihre Eignung für den Einsatz zur Bearbeitung einer Fragestellung hängt dabei von vielen Faktoren ab, unter anderem dem Umfang und der Art der Daten.

Neben den Methoden zur Induktion verfügt die Statistik über ein breites Spektrum an **Verfahren und Maßen, um die Qualität des Ergebnisses zu bewerten**. Mithilfe dieser Maßzahlen ist es möglich, etwaige Fehler sowohl abzuschätzen als auch während des Einsatzes zu kontrollieren. Die Frage nach der erwarteten Körpergröße eines Kindes kann so mit 175 cm +/- 4 cm beantwortet werden. Die Sicherheit, dass das Ergebnis eines Schwangerschaftstests positiv ist, kann bei 93 % liegen. Kontrollieren lässt sich – am Beispiel des Schwangerschaftstests – die Anzahl von Fehlalarmen, bei denen die Frau nicht schwanger ist, und fehlenden Alarmen, bei denen eine schwangere Frau ein negatives Ergebnis erhält. Ein perfektes statistisches Verfahren würde zu keinem dieser Fehler führen. In der Praxis muss abgewogen werden, welcher Fehler schwerwiegender und daher exakt zu kontrollieren ist. Ist es kritischer, eine tatsächlich schwangere Frau zu spät zu informieren, oder ist es kritischer, Frauen fälschlicherweise eine Schwangerschaft anzudeuten? Es ist nicht möglich, beide Fehlerarten gleichzeitig zu minimieren: je kleiner der eine, desto größer in aller Regel der andere. Die „Balance“ wird je nach Kontext unterschiedlich gewählt werden.



Die Bewertung der Qualität der Ergebnisse leitet sich aus Qualitätsmerkmalen der Methoden selbst ab. Für einige Methoden können sogar **Qualitätsgarantien** gegeben werden. So gibt es eine Gruppe von Schätzverfahren, die als UMVUE (Uniformly Minimum Variance Unbiased Estimator, gleichmäßig bester erwartungstreuer Schätzer) bezeichnet werden. Verwendet man einen solchen Schätzer, stellt man sicher, bei gegebener Datenlage das bestmögliche Ergebnis zu erhalten. Liefert eine Regression, deren Parameter durch Verwendung eines UMVUE-Schätzers ermittelt wurde, die erwartete Körpergröße des Kindes 175 cm +/- 4 cm, gibt es keinen anderen Schätzer, der einen kleineren Fehlerbereich liefert. Ein anderes Beispiel ist die Garantie bei einer Support Vector Machine, dass es sich bei einem aus den Daten ermittelten Modell um das bestmögliche für die Methode handelt, sofern sich ein solches finden lässt. Für manche Verfahren liegen zur Zeit weder für das Modell an sich noch für die Schätzungen, die mit dem Modell erzeugt werden, fundierte Verfahren zur Bewertung der Qualität vor. Dies gilt insbesondere für die Methodenklasse der NN. Aber auch für NN können Qualitätsangaben gemacht werden. Besonders wichtig sind Maßzahlen, die angeben, wie gut ein Modell auf Grundlage bisher unbekannter Daten funktioniert. Das Modell wird auf einem Datensatz (Trainingsdaten) gelernt und auf einem anderen in seiner Güte bewertet (Testdaten). Mit dieser Herangehensweise können Modelle

identifiziert werden, die nicht die übergeordnete Regel abbilden, sondern ihre Trainingsdaten auswendig gelernt haben. Man spricht in einem solchen Fall von overfitting. Ein überangepasstes Modell wird auf den Trainingsdaten wesentlich bessere Qualitätswerte erzielen als auf den Testdaten.

Viele Verfahren der Statistik können analytisch gelöst werden. Das bedeutet, dass die Fragestellung als eine mathematische Gleichung oder ein Gleichungssystem formuliert und durch – häufig geschicktes – Transformieren aufgelöst werden kann. Eine Vielzahl von Methoden lassen sich dagegen nicht direkt analytisch auflösen (bspw. wenn Zusatzbedingungen wie ein Regularisierungsterm hinzukommen, s.u.). In diesen Fällen kann man auf **Optimierungsverfahren** zurückgreifen, die sich in vielen kleinen Schritten an die Lösung herantasten. Optimierungsverfahren sind nicht notwendigerweise optimal, so kann es sich bei dem berechneten Ergebnis gegebenenfalls nur um ein lokales Optimum und nicht das (oder eines der) globale/n Optimum/a handeln.

## Verschiedene Lösungsansätze: Analytische Verfahren und Optimierungsverfahren

Eine direkte analytische Lösung ist für Aufgaben möglich wie „Gesucht ist der Wert von y für die Gleichung mit  $y=4 \cdot x+3$  mit  $x=3$ “.

Dies ist nicht möglich für die Aufgabenstellung:  
„Gesucht ist die Lösung für die lineare Gleichung  $a \cdot x_1 + b \cdot x_2 + \dots + h \cdot x_8 = y$ , bei der möglichst viele Parameter a, b, ..., g, h gleich 0 sind“.

Dafür wird ein Regularisierungsterm hinzugenommen:  
 $\min((a \cdot x_1 + b \cdot x_2 + \dots + h \cdot x_8 - y) + (\text{Anzahl Parameter} \neq 0))$ .

Um Lösungen zu finden, verwendet man Optimierungsverfahren.

### 2.2.3 Maschinelles Lernen

Die Abgrenzung zwischen klassischer Statistik und dem erstmals durch Mitchell<sup>2</sup> definierten **Maschinellen Lernen** ist schwierig. Spätestens wenn Optimierungsverfahren (→ dazu soeben unter ) für das Lösen des induktiven Schließens verwendet werden, bietet es sich an, von Maschinellem Lernen zu sprechen.

Die Ansätze für **Schätz- bzw. „Lern“strategien** des Maschinellen Lernens unterscheiden sich durch die Formulierung des zu lösenden Optimierungsproblems. Es wird zwischen verschiedenen Lernverfahren differenziert:

- Überwachtes Lernen: Für überwachtes Lernen ist es erforderlich, zu jeder Eingabeinformation (das „E“ im EVA-Prinzip) die korrekte Ausgabe (das „A“) zu kennen. Ein klassisches Beispiel ist die Körpergröße: Möchte man von der Körpergröße der Eltern (Eingabe) auf die Körpergröße der Kinder (Ausgabe) schließen, so muss für jedes Kind die Größe vorab bekannt sein. Bei Schwangerschaftstests muss das korrekte Ergebnis, bei Wettervorhersagen das Wetter, bei Bodenanalysen die Bodenbeschaffenheit usw. gegeben sein. In der Praxis besteht die Herausforderung oft in der Beschaffung und Qualitätssicherung dieser korrekten Ausgabeinformation. Diese Ausgabeinformation wird häufig als **Label** bezeichnet. Aktuell wird die Mehrzahl aller im Einsatz befindlicher durch Maschinelles Lernen spezifizierter Algorithmen mittels überwachten Lernens trainiert.

- Es ist entscheidend für diese Lernverfahren, wie das eigentliche Optimierungsproblem formuliert ist, welche Regularisierungen verwendet werden und wie die Verlustfunktion definiert ist (d.h. werden alle Fehler gleich behandelt oder gibt es unterschiedliche Gewichte, Schweregrade, z.B. im Vergleich von als False Negatives nicht erkannten Krebserkrankungen zu als False Positives fälschlich ausgewiesenen Krebs-erkrankungen?).

### Qualität von Labeln

Label können ebenfalls fehlerbehaftet sein. Man kann mehrere Komplexitätsstufen für die Feststellung der Labels definieren:

1. Label, deren Korrektheit zum Erhebungszeitraum überprüfbar ist. – Beispiel: Bei physikalischen Systemen oder Eigenschaften, der Geschwindigkeit eines Objektes, der Raumtemperatur, aber auch dem Geburtsdatum jedes Menschen, existiert nur ein richtiger zugehöriger Wert. Diese Werte können daher prinzipiell als Label durch einen Algorithmus ermittelt werden.
2. Label, deren Korrektheit zum Erhebungszeitpunkt und gegebenenfalls auch später nicht überprüfbar ist.
3. Label mit einem konstruierten und nicht überprüfbaren Bezug zur realen Welt. – Beispiel: Um Menschen und ihr Verhalten besser verstehen und analysieren zu können, wurden etwa Konzepte wie soziale Milieus oder Charaktertypen entwickelt. Diese Konzepte sind Abstraktionen, die eine Wahrheit – sofern diese existiert – nicht notwendigerweise korrekt abbilden.

<sup>2</sup> Tom Mitchell: Machine Learning, McGraw-Hill, 1997.



## Festsetzung des Optimierungsziels

Ein ÖPNV-Unternehmen plant, die Linienführung von Bussen der Stadtentwicklung anzupassen, weil viele Einwohner in die Randbereiche abgewandert sind, große innerstädtische Brachflächen erschlossen wurden und sich die Bevölkerungszusammensetzung in den Bezirken durch Gentrifizierung stark verändert hat. Der Projektleiter hat Daten zu Fahrgast- und Nutzungszahlen erhoben und arbeitet an einer Optimierung, um eine bedarfsgerechte Linienführung der Buslinien zu erreichen, ohne dass der Einsatz zusätzlicher Busse nötig wird. Für die Optimierung kommen verschiedene Ziele oder Nebenbedingungen infrage, z.B. Einsparung von Bussen, Einsatz von weniger Fahrerinnen und Fahrern, kein Schaffen neuer Routen. Abhängig von der Formulierung des Optimierungsproblems könnte es sein, dass beispielsweise dichtbesiedelte Stadtteile im Vergleich besser versorgt werden, dafür aber alle Bewohner von Außenbezirken etwas längere Fahrzeiten oder geringere Frequenzen in Kauf

nehmen. Da der Projektleiter selbst im Speckgürtel wohnt, ist ihm die Optimierung lieber, bei der die längste Fahrzeit minimiert wird. Dies führt dazu, dass schnellere Verbindungen auch in die Randbezirke entstehen. Seinem Vorgesetzten gefallen beide Modelle nicht. Er möchte, dass so viele Passagiere wie möglich transportiert werden. Dies führt dazu, dass gute Kurzstreckenverbindungen verstärkt werden, längere Fahrten über mehr als vier Stationen jedoch im Nachteil sind. Hier zeigt sich, dass die Entscheidung über die Optimierungsfunktion gesellschaftliche Auswirkungen haben kann. Es stellen sich u.a. folgende Fragen: Wer entscheidet über das Ziel der Optimierung? Wer sollte (mit)entscheiden? Wie kann der notwendige/sinnvolle gesellschaftliche Diskurs geführt werden? Welchen Rechtsschutz (z.B. Klagemöglichkeiten) genießen Gruppierungen/Stadtteile, die sich anderen gegenüber benachteiligt fühlen?

- Beim **Reinforcement Learning** werden Handlungen eines Agenten durch eine Bestrafung (Penalty) bzw. durch eine Belohnung (Bonus) bewertet. Ein Agent kann aus einer Menge von Handlungen auswählen und eine Handlung durchführen. Sein Handeln verändert den Zustand des Systems. Als Eingabe zur Optimierung dient die Handlung des Agenten. Zusammen mit dem Zustand bzw. der Zustandsänderung des Systems, die von der Handlung des Agenten herbeigeführt wird, muss eine eindeutige Bonusfunktion existieren. Während beim überwachten Lernen zu jeder Eingabe die korrekte, optimale Lösung vorliegt, ist dies bei Reinforcement Learning nicht unbedingt gegeben. Die Optimierung hat dabei die Aufgabe, diejenigen Handlungsstrategien zu finden, die zum besten Endzustand bezogen auf das Optimierungsproblem führen. Dabei kann es erforderlich sein, auf Handlungen, die eine kurzfristige Verbesserung liefern, verzichten zu müssen. Für diese Lernstrategie spielt neben dem eigentlichen Optimierungsproblem und der relevanten Verlustfunktion insbesondere die Bonusfunktion eine entscheidende Rolle.

- **Unüberwachtes Lernen** nutzt eine Menge von Eingabedaten und sucht in diesen Daten nach Strukturen. Die Kenntnis von korrekten Strukturen oder einer Bonusfunktion ist nicht erforderlich. Dagegen ist es notwendig, genau zu definieren, nach welcher Struktur gesucht werden soll. Beispielsweise kann nach Clustern, d.h. Gruppen in den Daten, gesucht werden, wobei die Anforderung darin besteht, dass alle Datenpunkte eines Clusters sich so stark wie möglich ähneln, wohingegen der Unterschied zwischen den Clustern maximiert werden soll. Daraus ergibt sich das Optimierungsproblem für das unüberwachte Lernen. Das unüberwachte Lernen wird auch als **Data Mining** bezeichnet.

Neben den Lernverfahren spielt die Bereitstellung der Daten eine entscheidende Rolle, da diese in hinreichendem Umfang, einer guten Qualität und angemessenen Breite zur Verfügung stehen müssen, um eine gute Näherung des Optimierungsziels zu erreichen. In vielen Fällen stehen Daten leider nicht im erforderlichen Umfang, der Breite oder Qualität zur Verfügung, so dass andere Wege eingeschlagen werden müssen, um dennoch gute Ergebnisse durch Maschinelles Lernen zu erzielen.

So ist es möglich, **synthetische Daten**, d.h. Daten, die künstlich generiert und nicht unmittelbar in der echten Welt erhoben wurden, zu verwenden. Sie haben mehrere Vorteile gegenüber den echten Daten:<sup>3</sup> Synthetische Daten können in beliebiger Menge produziert werden; dies ist besonders wichtig für Simulationen, wenn die echten Daten noch gar nicht angefallen sein können. Bei der Erzeugung kann dafür gesorgt werden, dass gesamte Wertespektrum möglichst vollständig abzubilden, z.B. um das Verhalten eines technischen Systems auch bei ungewöhnlichen Datenkonstellationen zu testen. Die Qualität der synthetischen Daten ist messbar; je nach Bedarf kann im Einzelfall gewährleistet werden, dass die Eigenschaften eines Referenzdatenbestands aus der echten Welt erhalten bleiben, oder es können gezielt Verzerrungen, die in Echtbeständen vorkommen können, im Sinne einer Diskriminierungsvermeidung herausgenommen werden. Solange der synthetische Datenbestand keinen Personenbezug aufweist, ist er anonym, und die DSGVO ist nicht anwendbar. Synthetische Daten können für ein Training von Algorithmen oder ein Test von Systemen hilfreich sein. Jedoch besteht das Risiko, dass Eigenschaften der generierten Daten den Algorithmus beeinflussen, die keine Entsprechung in der Realität haben. Daher sind vor dem praktischen Einsatz gesonderte Funktionstests erforderlich.

Ein häufig genutzer Mittelweg ist die sogenannte **Augmentation**. Hierbei werden echte Daten so erweitert, dass im Training eine größere Menge an Konstellationen abgedeckt werden kann. Somit bleibt einerseits der Bezug zu echten Daten erhalten und andererseits wird eine Verbreiterung der Datenbasis erzielt. Augmentation beschreibt den Prozess, neue Daten zu generieren, die leicht von den Ursprungsdaten abweichen. Beispielsweise zeichnet sich ein augmentiertes Bild dadurch aus, dass es verschoben, rotiert oder verzerrt worden ist.

## 2.2.4 Künstliche Intelligenz

Im aktuellen Sprachgebrauch wird Maschinelles Lernen, weiter verengt auf Neuronale Netze, als **Künstliche Intelligenz (KI)** bezeichnet. Diese Bezeichnung kann durchaus für Verwirrung sorgen: Maschinelles Lernen ist nur ein spezielles Verfahren innerhalb der „schwachen KI“, welche wohlspezifizierte Aufgaben löst. Im Gegensatz dazu wird von der „starken KI“ erwartet, nicht nur eine Aufgabe, sondern ein breites Spektrum von Aufgaben, womöglich ohne Eingriffe eines Menschen, zu bewältigen. Dies leistet das Maschinelle Lernen entgegen der Erwartung, die der Begriff Künstliche Intelligenz weckt, nicht.

Historisch bezeichnet der Begriff Künstliche Intelligenz ein breites Forschungsgebiet innerhalb der Informatik, das bereits 1956 in den USA unter dem Namen **Artificial Intelligence** begründet wurde (Dartmouth Proposal).<sup>4</sup> Seit Gründung hat das Gebiet mehrfache Zyklen überzogener Erwartungen und folgender Ernüchterung erlebt. Der Sprung aus der Forschung in Wirtschaft und (Lebens-)Alltag gelang spätestens in den 1970er und 1980er Jahren durch die sogenannten Expertensysteme. In Deutschland setzte die verstärkte Forschung in den 1980er Jahren ein.

Neben dem Maschinellen Lernen hat das Forschungsgebiet der KI eine Vielzahl weiterer wichtiger Methoden hervorgebracht, beispielsweise Verfahren zur **Mustererkennung**, zur **Wissensrepräsentation**, zur **automatischen Inferenz** und **Handlungsplanung** sowie zur **Benutzermodellierung**. Diese Verfahren werden bspw. in **Sprach-, Bild- und Dialogverständen**, in der **Robotik** und bei **Multiagentensystemen** eingesetzt.

3 Jörg Drechsler / Nicola Jentzsch: Synthetische Daten: Innovationspotential und gesellschaftliche Herausforderungen, Stiftung Neue Verantwortung, 2018 (abrufbar unter: <https://www.stiftung-nv.de/de/publikation/synthetische-daten-innovationspotential-und-gesellschaftliche-herausforderungen>).

4 John McCarthy / Marvin Minsky / Nathaniel Rochester / Claude Shannon: A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, 1955.

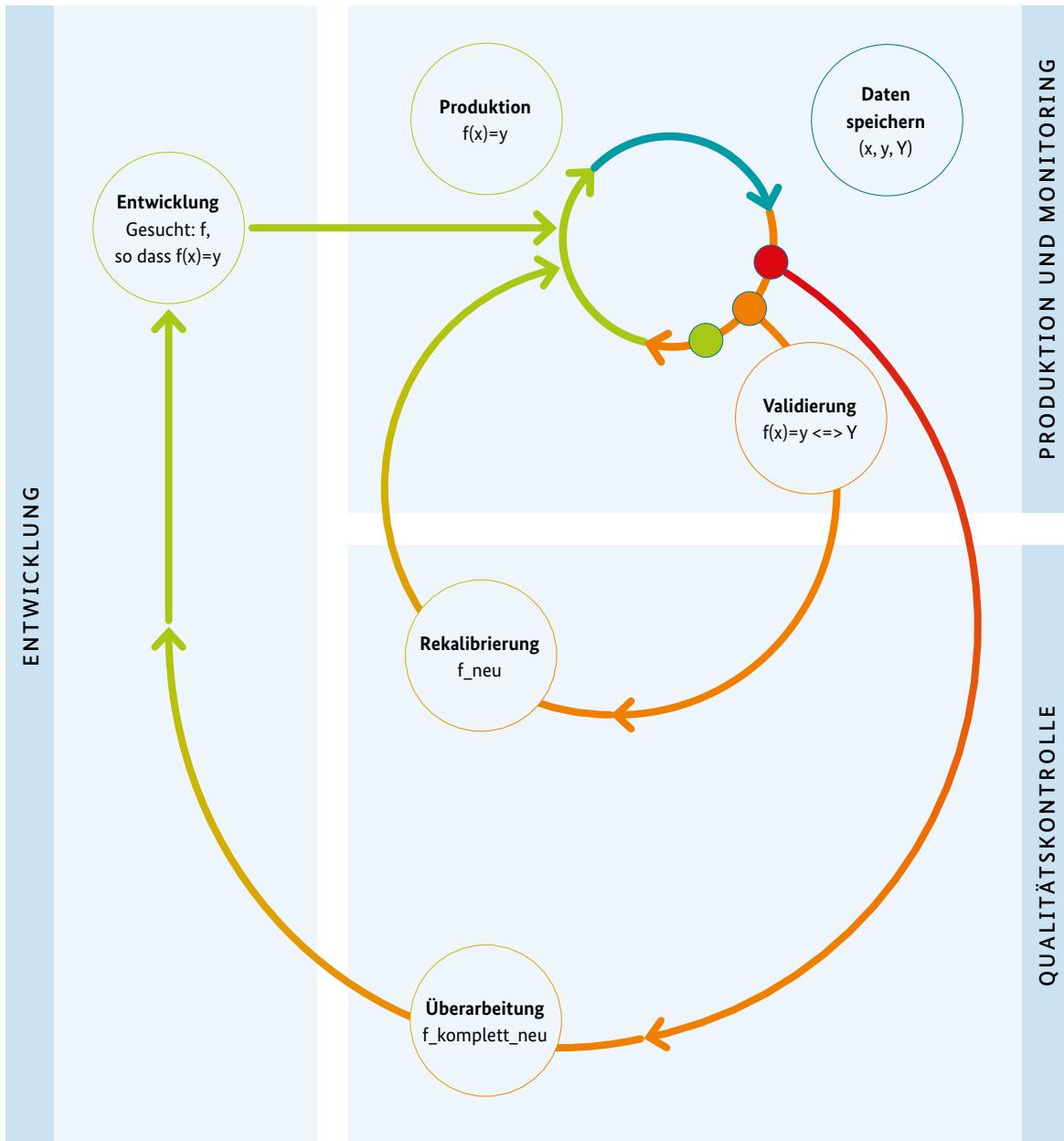
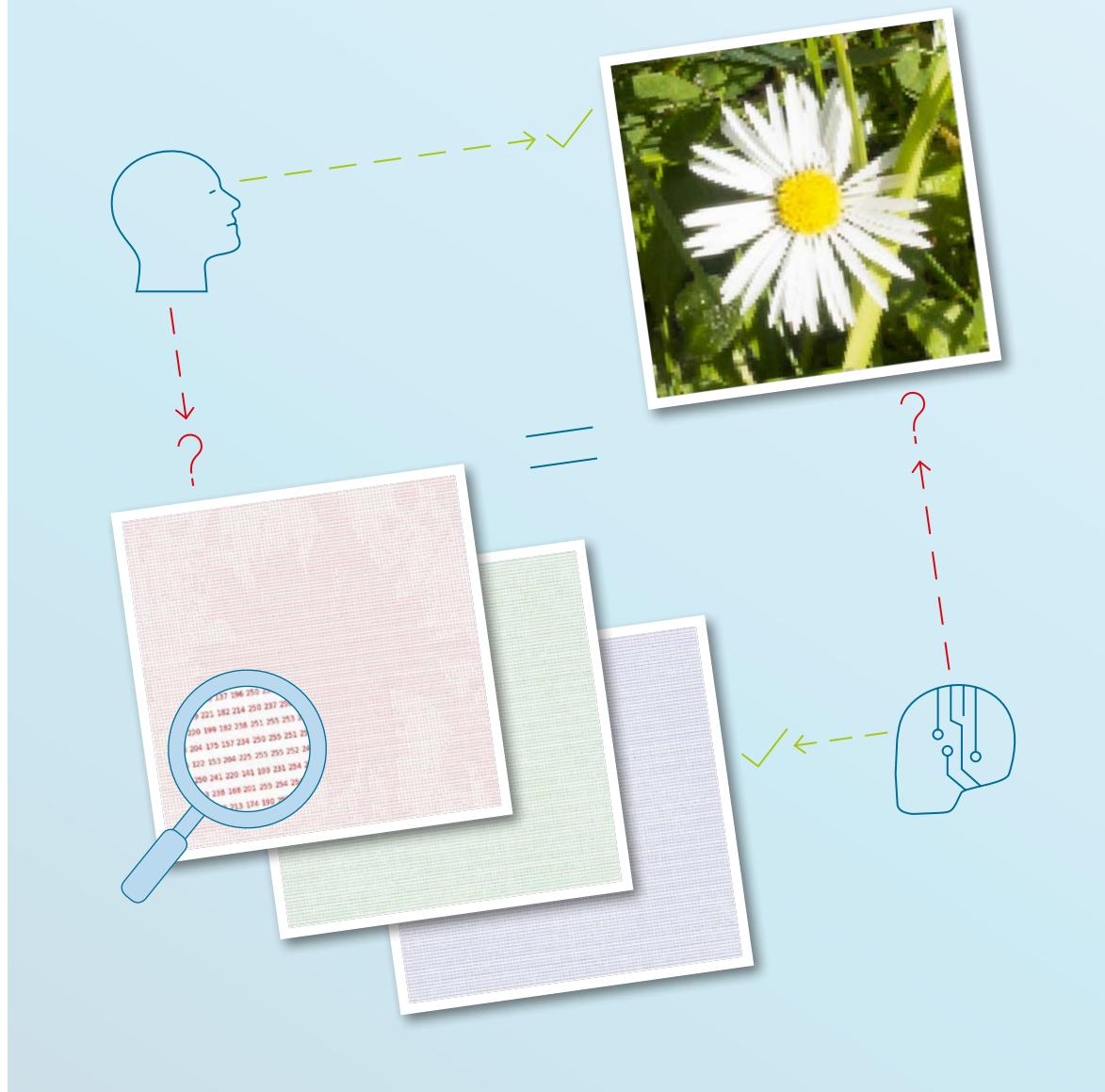


Abbildung 2: Prozessmodell eines auf Maschinellem Lernen basierenden Algorithmus: Fortlaufende Beobachtung und Bewertung. Der Prozess beginnt mit der Entwicklung des Algorithmus  $f$  auf den Trainingsdaten. Ist ein Algorithmus gefunden worden, der die angestrebten Qualitätsstandards erfüllt, wird dieser in Produktion gebracht. Um die Möglichkeit zum Monitoring und zur Qualitätskontrolle zu haben, muss in Produktion der Input  $x$  in den Algorithmus, der Output  $y$  des Algorithmus und der zugehörige korrekte Wert  $Y$  gesichert werden. Auf der Basis dieser Information kann eine Kontrolle des Algorithmus im produktiven Umfeld etabliert werden. Hierzu wird verglichen, in welchem Maß die Outputs  $y$  des Algorithmus den erwarteten Wert  $Y$  reflektieren. Sind die Abweichungen unkritisch, kann der Algorithmus ohne Veränderung weiterbetrieben werden. Bei signifikanten Abweichungen kann es erforderlich werden, die Parameter des Algorithmus neu zu schätzen, d.h. zu rekalibrieren. Bei kritischen Abweichungen empfiehlt sich eine Überarbeitung.

## Verständlichkeit und Nachvollziehbarkeit als Problem

Ein intuitives Verstehen von mathematisch oder technisch abgebildeten Methoden ist für Menschen häufig schwierig oder unmöglich. Dies betrifft selbst Experten im Bereich der Modellierung. Sogar bei mathematisch gut verstandenen, verhältnismäßig einfachen Klassifikationsmethoden wie der logistischen Regression, weiß kaum jemand intuitiv, welches Ergebnis sie für welche Eingabewerte liefert.

Ein Beispiel sind Neuronale Netze (NN) in der Bilderkennung: Während ein Mensch auf einem Foto meist sofort erkennt, was abgebildet ist, ist dies kaum möglich bei dem Betrachten der Datenstrukturen desselben Fotos, die Eingabe für ein NN sind. Das bedeutet: Selbst wenn man alle digitalen Eingabewerte kennt und alle Schritte in einem NN nachvollziehen kann, folgt daraus nicht, dass Menschen den Erkennungsprozess verstehen und etwa im Fehlerfall feststellen können, warum eine Fehlerkennung passiert und wie diese behoben werden kann. Menschliche und maschinelle Objekt- und Mustererkennung funktioniert also nach unterschiedlichen Regeln, die nicht leicht übersetzbare sind.



### 2.2.5 Algorithmische Systeme

Ein algorithmisches System besteht in der Regel nicht aus einem einzigen Algorithmus, sondern aus einer Vielzahl von Algorithmen, die zusammenarbeiten können. Eine Komponente beschreibt einen ausführbaren Teil eines solchen Systems. Ein Algorithmus kann in unterschiedlichen Komponenten technisch verschieden umgesetzt sein, beispielsweise im Bereich der Microservice-Architekturen. Es ist zu berücksichtigen, dass die einzelnen Komponenten eines solchen Systems in Produktion unterschiedlichen Anforderungen in Bezug auf rechtliche Vorgaben oder Schutzziele unterliegen können. Hinzu kommt, dass in einem algorithmischen System verschiedene Akteure, beispielsweise in Form von Zulieferern, Betreibern oder Herstellern, für verschiedene Komponenten des Systems verantwortlich sein können. Dabei ist zu beachten, dass an die einzelnen Komponenten unterschiedliche Anforderungen gestellt werden bzw. dass unterschiedliche Regularien greifen, z.B. für Datenqualität, Diskriminierungsfreiheit oder Vertragsfreiheit.

### 2.3 Software

Wird ein Algorithmus nicht in natürlicher Sprache, sondern in einer Programmiersprache (formale Sprache) formuliert, so wird er als **Programm** (oder **Software**) automatisch auf einem Rechner ausführbar. Die Funktionsweise einer Software ist nicht allein abhängig von den Daten, die sie verarbeitet, sondern auch vom Ausführungskontext (vgl. u.a. Technologie-Stack, der sämtliche Hard- und Softwarekomponenten beinhaltet, die für die Ausführung verwendet werden) und von ihrer Parametrisierung. Mit Hilfe von Parametern kann eine Software quasi von außen eingestellt werden. Auf diese Weise können einfache Informationen wie beispielsweise Darstellungsoptionen oder Pfadangaben bis hin zu komplexen Modellen an die Software übergeben werden. Je stärker eine Software parametrisierbar ist, desto flexibler ist sie einsetzbar, desto komplexer ist sie in der Regel zu entwickeln und desto relevanter werden die Parameter. So kann parametrisierbare Software relativ leicht an verschiedene Kontexte adaptiert werden, ohne erneut den Quelltext, d.h. die eigentliche Umsetzung, verändern zu müssen. Eine spezielle Variante sind adaptive Systeme, die sich über die Zeit automatisch an ihren Kontext, beispielsweise die Person des Nutzers oder die Einsatzumgebung, anpassen.

Um die Entwicklung qualitativ hochwertiger Software in einem gleichzeitig immer komplexer werdenden Umfeld effizient(er) zu gestalten und Kommunikationsprobleme im Entwicklungsprozess zu reduzieren, werden seit vielen Jahren erfolgreich **modellgetriebene Entwicklungsansätze** verfolgt. Hierbei wird eine generische Softwarekomponente mit einem komplexen Modell auf eine den Anwendungskontext bezogene Sprache parametrisiert. Einen Spezialfall stellen dabei mathematisch-statistische Modelle dar, die sich von domänenpezifischen Sprachen dadurch abgrenzen, dass hier nicht ein Modell explizit spezifiziert oder programmiert, sondern das mathematisch-statistische Modell (**implizit**) auf Basis von Daten angelernt bzw. trainiert wird (→ siehe oben 2.2.3 zum Maschinellen Lernen).

## 2.4 Hardware

Die Software wird von Hardware und speziell von sog. **Prozessoren** ausgeführt, deren Leistungsfähigkeit in der Vergangenheit stets zunahm, während die Geräte selbst kontinuierlich kleiner wurden, so dass sich das Feld der Einsatzszenarien stets erweiterte. Die Steigerung der Leistungsfähigkeit nach der sog. Moore'schen Gesetzmäßigkeit (Hundertfache Leistungssteigerung in 10 Jahren) unterliegt jedoch physikalischen Grenzen. Mit der Annäherung von Chipkomponenten an die Größe einzelner Atome wird es zunehmend kostspieliger und technisch aufwändiger, die Vorhersagen von Moore mit Silizium als Transistormaterial zu erfüllen. Es wird daher heute mit alternativen Materialien, wie Graphen, in Verbindung mit neuen Berechnungskonzepten, wie photonischen Quantencomputern, geforscht, wobei eine Alltagstauglichkeit noch offen ist. Bereits etablierte Lösungen, die stark auf Parallelität setzen, sind dagegen Multi- und Many-Core-Prozessoren oder der Einsatz von Grafikprozessoren (GPU = Graphic Processing Unit). Für die Beschleunigung des Maschinellen Lernens über Massendaten wurden auch anwendungsspezifische Chips wie die Tensor-Prozessoren (TPU = Tensor Processing Units) entwickelt, die auf das hochparallele Addieren und Multiplizieren von Matrizen für neuronale Netze optimiert sind.

Durch die immer stärkere Parallelisierung der Berechnungen entsteht das Problem, dass für Menschen Fehler in solchen Prozessoren sehr schwer zu finden und auch die durchgeföhrten Berechnungen auf der Hardwareebene **kaum reproduzierbar und nachvollziehbar** sind.

## 2.5 Systemarchitektur

Heute laufen Anwendungen selten auf einem einzelnen Rechner; es handelt sich dagegen um viele Software-Komponenten auf verschiedenen Rechnern, die miteinander interagieren, um eine Aufgabe zu erfüllen. Aufgrund der Verteilung auf unterschiedliche Hardware-Knoten spricht man von einem **verteilten System**. Ein verteiltes System setzt sich aus unterschiedlichen Software- und Hardware-Komponenten zusammen, die in einem Netz interagieren. Die Netzketten kommunizieren miteinander über Funk oder Kabelverbindungen.

Für die Netzkommunikation existieren vielfältige **Protokolle und Standards**. Mittels dieser werden Daten auf den Netzknoten verarbeitet und über das Netz weitergeleitet bzw. zu anderen Knoten transportiert. Die Spezifikation für Anfragen, die an einen Server gestellt werden dürfen, wird beispielsweise in einer sog. Programmierschnittstelle (API = Application Programming Interface) veröffentlicht, wobei der Zugriff über diese Schnittstelle in der Regel gegen fehlerhafte Nutzung oder Angriffe abgesichert werden muss.

IT-Infrastrukturen, die über das Internet erreichbar sind, werden als **Cloud** bezeichnet. Cloud-Anwendungen können Milliarden von Nutzern erreichen. Bestimmte verwandte Cloud-Anwendungen werden oft als **Digitale Plattform** bezeichnet und haben einen hohen Bekanntheitsgrad wie beispielsweise die sog. Big Four oder GAFA (Google, Apple, Facebook, Amazon) bzw. GAFAM (wenn Microsoft mit dazu genommen wird).



Während zu Beginn des Internets der Dinge die meisten Daten direkt in die Cloud geschickt wurden, um dort auf großen digitalen Plattformen verarbeitet zu werden, werden derzeit vermehrt Lösungen entwickelt, bei denen die Daten direkt und möglichst nah an dem Erhebungspunkt, also gleichsam „am Rande“ (on the edge) des Internets, verarbeitet oder zumindest vorverarbeitet werden. Die Verarbeitung nah am Erhebungspunkt wird im Gegensatz zur Verarbeitung in der Cloud (Cloud-Computing) als **Edge-Computing** bezeichnet. Gerade die Vorverarbeitung von Daten ermöglicht es, die Kommunikationsaufwände zu minimieren, aber auch datenschutzfreundlichere Systeme zu erstellen, indem bereits an dieser Stelle, nämlich nahe des Erhebungspunktes, ein nicht erforderlicher Personenbezug entfernt werden kann.

Die mittlerweile entstandene komplexe Systemlandschaft einschließlich Internet, Edge-Computing und IoT führt dazu, dass Einzelsysteme wegen einer starken Verschränkung nur schwer voneinander abgrenzbar sind.

Die Ausgestaltung der Architektur verteilter Systeme hat durch die Entscheidung, welche Technologie eingesetzt wird, auf welchen Netzwerknoten die Software läuft, mit wem über welche Schnittstellen und Protokolle kommuniziert wird, auch signifikanten **Einfluss auf die Geschäftsprozesse**, die das System unterstützt. Wenn beispielsweise Hersteller von Hardware Daten, die ihre Geräte erfassen, nutzen wollen, um diese langfristig zu verbessern, so können sie eine eigene Kommunikationsinfrastruktur aufbauen, gegebenenfalls die Infrastruktur des Anwenders nutzen oder aber den Anwender bitten, die Daten über eine Schnittstelle zur Verfügung zu stellen. Der Umgang mit solchen Daten in kooperativen Prozessen sollte transparent gestaltet werden und muss gegebenenfalls vertraglich geregelt werden. Die vertragliche Gestaltung des Datenaustauschs kann dabei durch die technischen Gegebenheiten eingeschränkt sein.

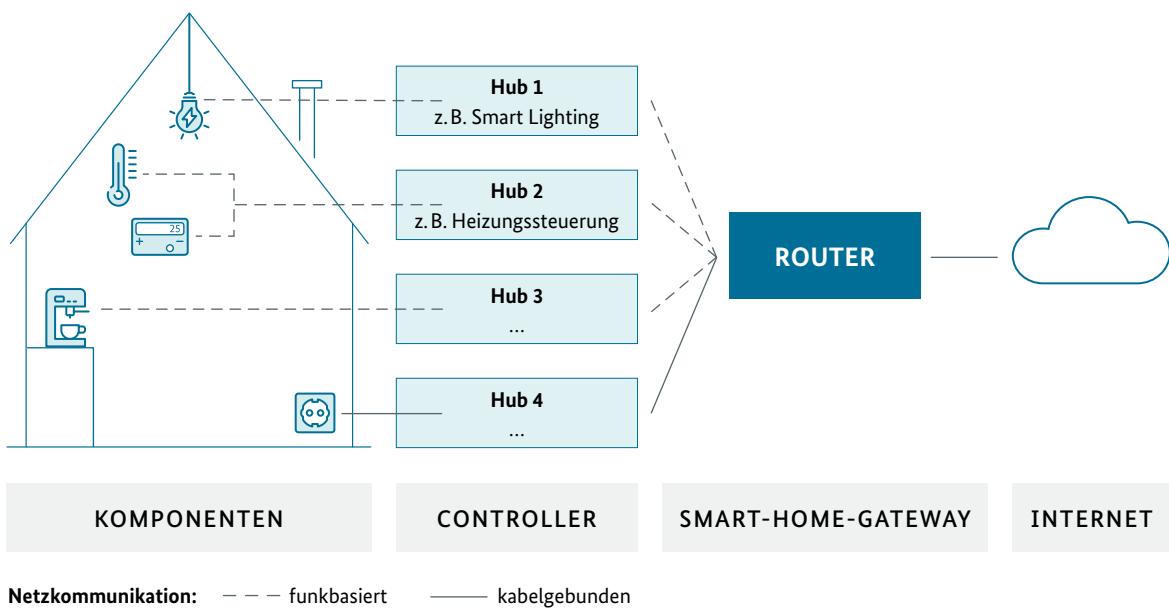


Abbildung 3: Beispiel der Systemarchitektur im Smart Home

## Blockchain und andere Distributed Ledger Technologien

Die signifikanten Verbesserungen im Bereich der verteilten Systeme ermöglichen den Einsatz von **Distributed Ledger Technologien** (DLT), die auf dem Konzept verteilter Kassenbücher basieren. Statt einer zentralen Verwaltung werden dabei viele grundsätzlich gleichgestellte Kopien eines sog. Kassenbuchs von unterschiedlichen Partnern verwaltet. Neue Einträge werden in allen Kopien ergänzt und der aktuelle Stand durch einen Konsensus (eine Übereinkunft) geklärt. Die zugrundeliegende Architektur solcher Systeme variiert je nach Verwendungszweck und Transaktionsgestaltung von linearen Ansätzen zu verschiedensten graphbasierten Systemen. Auch eine Übereinkunft kann auf verschiedene Arten erzielt werden, die durch ein sog. Konsensusprotokoll festgelegt wird.

Einer der bekanntesten Vertreter einer DLT-Architektur ist die **Blockchain**, zu der es Implementierungen wie Bitcoin oder Ethereum gibt. In einer Blockchain werden Daten in einer Liste von Datensätzen („Blöcken“) gespeichert. Die Blöcke sind miteinander kryptographisch verknüpft, so dass eine Transaktion, die als Block gespeichert wird, implizit die Richtigkeit früherer Transaktionen, d.h. der gesamten Kette (Chain), bestätigt und somit Manipulationen wie Veränderungen oder Löschungen von Einträgen erschwert. Durch das dezentrale Konsensusprotokoll ist keine zusätzliche Instanz zur Integritätsbestätigung von Transaktion erforderlich.





Teil D

# Mehr-Ebenen-Governance komplexer Datenökosysteme



Die konkrete Umsetzung des von der DEK zugrunde gelegten ethischen und rechtlichen Ordnungsrahmens stellt die Regulierung, die Steuerung und das Design von Datenökosystemen in Anbetracht der hohen Komplexität und Dynamik dieser Systeme vor neue Herausforderungen und erfordert das Zusammenwirken verschiedener Akteure und unterschiedlicher Governance-Instrumente auf mehreren Regulierungsebenen (Mehr-Ebenen-Governance). Der folgende Teil zeigt zunächst **relevante Governance-Instrumente und Akteure** auf. Weitere Spezifizierungen, auch zum Zusammenspiel verschiedener Instrumente und Akteure, finden sich in den beiden anschließenden Kapiteln zu Daten und algorithmischen Systemen.

# 1. Allgemeine Rolle des Staates

Diejenigen, die ethisch begründete Rechte wahrnehmen und korrespondierende Pflichten befolgen müssen – seien es etwa Bürger, Unternehmen oder staatliche Stellen – müssen dazu auch in der Lage sein. Hieraus ergeben sich zahlreiche Aufgaben für den Staat. Zunächst ist der Staat verantwortlich für die **rechtlichen Rahmenbedingungen**, in denen sich eine gemeinwohlorientierte Datengesellschaft entwickeln kann. Die Geschwindigkeit, in der sich algorithmische Systeme fortentwickeln und mit der sie in immer mehr Lebensbereiche vordringen, führt zu großen Herausforderungen für die Gesetzgebung und die konkretisierende Gerichtspraxis. Der Staat hat sicherzustellen, dass Regulierung in einem solchen Umfeld einerseits hinreichend Steuerungskraft entfaltet und andererseits die nötige Flexibilität aufweist, um ihre Aufgabe auch unter geänderten technologischen Bedingungen erfüllen zu können. Dafür bedarf es **technik-neutraler Formulierung** von Rechtsnormen und **innovativer Regulierungsmodele**.

Zudem bedarf es **angemessener infrastruktureller und technischer Voraussetzungen**, etwa befähigender Technologien, Institutionen und Intermediäre, unter Einschluss eines breiten Spektrums zivilgesellschaftlicher Akteure. Auch insofern kommt dem Staat nach Auffassung der DEK eine entscheidende Garantie- und Gewährleistungsfunktion im Rahmen der Daseinsvorsorge zu.

Durch die neuen Möglichkeiten der Datengesellschaft entsteht zudem eine umfassende **Bildungsaufgabe**. Hier stellt sich die Frage, welche Kompetenzen für den kreativen sowie gleichzeitig reflektierten Umgang mit digitalen Technologien notwendig sind und welche Rahmenbedingungen geschaffen werden sollten, um adäquate Bildungsangebote für vielfältige Zielgruppen umsetzen zu können. Die Bildungsaufgabe des Staates ist in einem umfassenden Sinn zu verstehen und schließt eine entsprechende Bewusstseinsbildung durch **Öffentlichkeitsarbeit** mit ein.

Ferner kommt dem Staat allgemein die Aufgabe zu, **Forschung und Entwicklung** zu fördern. Von besonderer Wichtigkeit ist hier, Forschung und Entwicklung ethisch fundierter Technologien bspw. zu Nachvollziehbarkeit, zu Transparenz oder zum Schutz vor Diskriminierung zu unterstützen. Die Berücksichtigung von ethischen und rechtlichen Grundsätzen und Prinzipien erfordert intensive Forschungs- und Entwicklungsarbeit, die verstärkt gefördert werden sollte.

Der Staat muss zwar nicht alle Mittel selbst oder durch staatsnahe Institutionen bereitstellen, aber er muss die **rechtlichen und sonstigen Rahmenbedingungen** für eine Datengesellschaft schaffen, in welcher Einzelne sich ebenso wie Unternehmen auf der Grundlage ethischer Werte und Prinzipien selbstbestimmt und zugleich ausreichend geschützt bewegen können und in welcher Potenziale von Daten und algorithmischen Systemen für die Gestaltung einer lebenswerten Zukunft genutzt werden.

Im Sinne einer ethisch fundierten Governance auf mehreren Ebenen sollte sich Deutschland auch kraftvoll in einen **europäischen und internationalen Diskurs** einbringen. Die globale Dimension der technologischen Entwicklung kann nicht von einem einzigen Nationalstaat und allein durch nationale Regulierung angemessen adressiert werden. Deswegen begrüßt die DEK die bereits bestehenden europäischen und internationalen Initiativen (z. B. der Europäischen Kommission und der OECD) für eine ethisch fundierte Gestaltung unserer Zukunft. Der Gewährleistung der **digitalen Souveränität** Deutschlands und Europas im internationalen Kontext (näher Teil G) kommt hierbei eine herausragende Bedeutung zu.



## 2. Unternehmerische Selbstverpflichtungen und Corporate Digital Responsibility

Sich um die Risiken der Digitalisierung zu sorgen und zu kümmern, aber auch deren erhebliche Potenziale wahrzunehmen, ist nicht nur eine Frage staatlicher Verantwortung und Regulierung. Ebenso tragen jene Akteure, die Technologien entwickeln, verbreiten und einsetzen, eine solche **Verantwortung**, und dies auch **jenseits gesetzlicher Vorgaben**. Auch wenn der Staat, nicht zuletzt infolge seiner Schutzpflichten zur Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme sowie weiterer Grundrechte, eine hervorgehobene Verantwortung hat, sind Instrumente der Selbstregulierung gerade im Kontext der Digitalen Transformation unverzichtbar.

Die Wahrnehmung einer jeweils eigenen Verantwortung für die Folgen der Digitalisierung wird, bezogen auf Unternehmen als Hersteller und Betreiber digitaler Technologien, unter dem Begriff der **Corporate Digital Responsibility (CDR)** diskutiert und praktiziert. CDR wird – in Anlehnung an Corporate Social Responsibility (CSR) – als Teilbereich der Unternehmensverantwortung verstanden, hier bezogen auf freiwillige unternehmerische Aktivitäten im digitalen Bereich, die über das heute gesetzlich Vorgeschriebene hinausgehen und die digitale Welt aktiv zum Vorteil der Gesellschaft im Allgemeinen und der Kunden und Mitarbeiter im Besonderen mitgestalten. In diesem Sinne hat das Bundesministerium der Justiz und für Verbraucherschutz (BMJV) im Mai 2018 eine Initiative zur Etablierung von Grundsätzen und Konzepten einer unternehmerischen digitalen Verantwortung gestartet ([www.bmjjv.de/cdr](http://www.bmjjv.de/cdr)). CDR kann demnach viele Themenbereiche umfassen<sup>1</sup>, unter anderem den Schutz personenbezogener Daten, die Sicherung der Inklusion in der digitalen Sphäre, die Transparenz etwa von Algorithmen oder im Datenschutz, die Entwicklung digitaler Innovationen, die zur Erreichung von Nachhaltigkeitszielen beitragen, den gemeinwohlorientierten Einsatz von Algorithmen, Open Data und die Gewährleistung von Informationssicherheit.

Eine verantwortungsvolle Entwicklung digitaler Produkte und Dienstleistungen muss bei allen unternehmerischen Entscheidungen und auf allen Ebenen des Unternehmens eine zentrale Rolle einnehmen. Ethische Fragestellungen dürfen dabei nicht allein den Rechtsabteilungen und Compliance-Beauftragten zugewiesen werden. Sie ist vielmehr als **Querschnittsaufgabe in sämtliche Prozesse zu integrieren**. Alle Beteiligten müssen sich verantwortlich fühlen, ethische Werte wie Teilhabe, Fairness, Gleichbehandlung, Selbstbestimmung und Transparenz zu berücksichtigen. So sollen die negativen sozialen und gesellschaftlichen Effekte der Digitalisierung und digitaler Geschäftsmodelle auf Mitarbeiter, Lieferanten, Kunden sowie die Gesellschaft und Umwelt insgesamt minimiert und die neuen Möglichkeiten der Digitalisierung zur Verwirklichung gesamtgesellschaftlicher Ziele genutzt werden. Richtig eingesetzt kann CDR zu Verbraucherschutz, digitaler Teilhabe und einer **nachhaltigen Entwicklung der Digitalwirtschaft** beitragen.

Im Kern ist CDR, genauso wie Corporate Social Responsibility (CSR), eine Selbstverpflichtung auf freiwilliger Basis. Dementsprechend kann die Umsetzung insbesondere durch interne Strategien wie unternehmensinterne oder branchenspezifische Wertekodizes abgesichert werden. Die DEK begrüßt insoweit die vermehrte Ausbildung professionsethischer Standards und Verhaltenskodizes (Codes of Conduct) durch Verbände und Unternehmen der datenverarbeitenden Wirtschaft, soweit diese zur Konkretisierung der Vorgaben beitragen. Maßnahmen im Rahmen von CDR dürfen nicht bloß ein „Feigenblatt“ sein, um dem Unternehmen einen „Anstrich digitaler Ethik“ zu geben.

1 Corporate Digital Responsibility-Initiative: Digitalisierung verantwortungsvoll gestalten – Eine gemeinsame Plattform, 2018 (abrufbar unter: [https://www.bmjjv.de/SharedDocs/Downloads/DE/News/Artikel/100818\\_CDR-Initiative.pdf?\\_\\_blob=publicationFile&v=4](https://www.bmjjv.de/SharedDocs/Downloads/DE/News/Artikel/100818_CDR-Initiative.pdf?__blob=publicationFile&v=4)).

Aus Sicht der DEK sollte schon in der Entwicklungsphase eines digitalen Produkts nicht nur gegebenenfalls eine Datenschutz-Folgenabschätzung nach der DSGVO, sondern im Sinne der Übernahme vorausschauender Verantwortung eine darüber hinausgehende, allgemeine **Risiko-Folgenabschätzung** für die Gesellschaft (einschließlich der von der Digitalen Transformation besonders betroffenen Mitarbeiter und Kunden eines Unternehmens) durchgeführt werden, die auch die gesellschaftlichen Langzeitwirkungen datengetriebener Geschäftsmodelle berücksichtigt. Dabei könnte für marktmächtige Unternehmen empfohlen werden, nach dem Vorbild von Verbraucher- oder Kundenbeiräten einen Beirat mit den Vertretern der je nach Geschäftsmodell spezifisch betroffenen Personengruppen einzurichten, welcher an einer solchen Folgenabschätzung beteiligt werden könnte.



### 3. Bildung: Stärkung digitaler Kompetenzen und kritischer Reflexion

Digitale Selbstbestimmung setzt digitale Kompetenz voraus. In diesem Zusammenhang sind die Bemühungen der Bundesregierung, von Verbraucherschutzverbänden, von juristischen Berufsvereinigungen sowie seitens anderer Stellen um eine **Sensibilisierung der Bevölkerung für den selbstbestimmten Umgang mit Daten und digitalen Technologien** – von Konfigurationsmöglichkeiten auf dem eigenen Smartphone bis hin zur digitalen Nachlassplanung – und um einfache und verständliche Informationen über die Gestaltungsmöglichkeiten nebst praktischen Hilfestellungen uneingeschränkt zu begrüßen. Das betrifft auch Bemühungen, bei Verbrauchern ein Bewusstsein für das Potenzial der Daten zu wecken und sie verstärkt über ihre Rechte und über die tatsächlichen Chancen und Risiken, ihre Daten wirtschaftlich zu nutzen, aufzuklären. Die DEK empfiehlt, all diese Bemühungen aufrecht zu erhalten und noch zu intensivieren.

Auch in den Schulen sollte möglichst früh ein Bewusstsein für die Digitalisierung geschaffen werden. Digitale Kompetenz sollte in die **Lehrpläne** integriert werden und Lehrkräfte müssen regelmäßig und umfassend geschult werden. Nur so können neue Generationen zu kompetenten „Digital Natives“ heranwachsen, die sowohl Chancen als auch Risiken neuer digitaler Anwendungen einschätzen, informierte Entscheidungen treffen und ihre Rechte effektiv einfordern können.

Daneben bedarf es einer **lebenslangen Bildung** zum Umgang mit Daten und digitalen Technologien, die für alle Altersstufen und gesellschaftlichen Gruppen gewährleistet werden muss. Hierbei ist zu berücksichtigen, dass digitale Kompetenz nicht nur grundlegende Kenntnisse technischer Aspekte voraussetzt, für die fortlaufend technisch-mathematische Kompetenzen vermittelt werden müssen, sondern auch ausreichende Kenntnisse ökonomischer, rechtlicher, ethischer und sozialwissenschaftlicher Art. Die Vielfalt an Kenntnissen ist erforderlich, um unterschiedliche Chancen und Risiken in ihrer Komplexität erfassen, diskutieren und bewerten zu können.

Von besonderer Relevanz ist hier die Ausbildung in Informatik, Softwareentwicklung und Datenwissenschaft (Data Science). Hier bedarf es einerseits grundlegender Lehrveranstaltungen zu ethischen und rechtlichen Fragen sowie andererseits weiterführende Ausbildung zu Statistik, Methodologie und Wissenschaftstheorie. Insbesondere die Verankerung daten- und forschungsethischer Fragestellungen in der fachspezifischen Methodenausbildung ist hier von zentraler Bedeutung und sollte deutlich vorangetrieben werden, damit diejenigen, die digitale Produkte und Dienstleistungen entwickeln oder über ihre Entwicklung entscheiden, ethische und rechtliche Gesichtspunkte frühzeitig in ihre Überlegungen mit einbeziehen.

Um diese Ziele zu verwirklichen, bedarf es zunächst des Zusammenwirkens einer **Vielzahl staatlicher, staatsnaher und privater Akteure** auf Bundes- wie auf Landesebene und in den Kommunen. Aufbau und langfristige Sicherstellung digitaler Kompetenz der Bevölkerung ist eine zu große Aufgabe, und die Herausforderungen in einzelnen Lebenszusammenhängen sind zu vielfältig, um dies zentralisiert in die Hände einer einzigen Stelle zu legen. Jedenfalls dürfte den Aufsichtsbehörden (Datenschutzbehörden und/oder jeweilige Fachaufsichtsbehörden), der Stiftung Datenschutz und den Verbraucherzentralen sowie den für die Bildung zuständigen Stellen eine zentrale Rolle zukommen. Auch den Medien und den Institutionen der Medienregulierung kommt in diesem Zusammenhang eine wichtige Funktion zu. Diese besteht nicht nur in der Aufklärung der Gesellschaft über neue Technologien und in der kritischen Begleitung des technischen Fortschritts, sondern auch in der Bereitstellung neuer Foren für Debatten.

Digitale Kompetenz der Bevölkerung lässt sich allerdings trotz der primären Verantwortlichkeit staatlicher Stellen nicht umfassend verwirklichen ohne den Aufbau entsprechender **zivilgesellschaftlicher Strukturen**, wie des digitalen Ehrenamts, des sog. Tech-Accountability-Journalismus und der verbraucherorientierten Marktbeobachtung. Die DEK empfiehlt daher der Bundesregierung, den Aufbau derartiger Strukturen nachhaltig zu fördern.

Auch innerhalb von **Unternehmen** ergeben sich Bildungsaufgaben. So kann ein Unternehmen nur dann hohen ethischen Standards genügen, wenn diejenigen, die im Unternehmen tätig sind, insbesondere im Management und in der Produktentwicklung, eine hinreichende Sensibilität für ethische und rechtliche Fragen aufweisen. Im Bereich der Aus- und Fortbildung sollten Fragestellungen rund um Datenethik und Datenrecht ferner bei einer **breiten Palette akademischer und beruflicher Ausbildungswägen** sowie in der betrieblichen Fortbildung berücksichtigt werden. Dabei ist insbesondere an technische und betriebswirtschaftliche Berufsrichtungen zu denken, damit diejenigen, die digitale Produkte und Dienstleistungen entwickeln oder über ihre Entwicklung entscheiden, ethische und rechtliche Gesichtspunkte frühzeitig in ihre Überlegungen mit einbeziehen.



## 4. Technologieentwicklung und ethisch fundiertes Design

Die Bemühungen, digitale Kompetenzen in der Bevölkerung zu verbessern, dürfen keine Verschiebung von Verantwortung weg von Produzenten und digitalen Dienstleistern hin zu den Nutzern bedeuten, zumal die Nutzer nur begrenzte Möglichkeiten haben, alle Verarbeitungsschritte ihrer Daten und die dahinterliegenden Geschäftsmodelle nachzuvollziehen und zu verstehen. Die Übernahme von Verantwortung ist vielmehr zuvörderst auf der Seite derjenigen erforderlich, welche Einfluss auf die Entwicklung von Produkten und Dienstleistungen haben. Solche Verantwortung äußert sich insbesondere in ethisch fundiertem Design (sog. **Ethics by Design** bzw. **Ethics in Design**) und ist bspw. in Bezug auf Privatsphäre- und Datenschutz bereits in der DSGVO unter den Stichworten Datenschutz „by design“ und Datenschutz „by default“ enthalten. Die Orientierung der Entwicklung von Technologien und Produkten (einschließlich Diensten und Anwendungen) an den zuvor dargelegten ethischen Werten und Prinzipien ist zudem geeignet, Vertrauen und Akzeptanz der Bevölkerung in digitale Produkte zu stärken.

Dabei muss allerdings jedes Produktdesign **auf die adressierten Nutzergruppen abgestimmt** sein, wobei **partizipative Produktentwicklung**, die Nutzergruppen und ihre Bedürfnisse bereits im Stadium der Produktentwicklung mit einbezieht, hilfreich sein kann. Insbesondere dort, wo ein Produkt auch wenig digital affine und/oder vulnerable Nutzergruppen adressiert, sollte Design, einschließlich der datenschutzfreundlichen Voreinstellungen, **inklusiv gestaltet** sein, sodass auch diese Nutzergruppen in ihrer digitalen Selbstbestimmung geschützt sind. Damit können Hersteller und Betreiber der besonderen grundrechtlichen Verankerung der informationellen Selbstbestimmung in Art. 1 Abs. 1 GG (Menschenwürde) gerecht werden, die es verbietet, den Schutz von den individuellen Fähigkeiten und der individuellen Lebenssituation des Einzelnen abhängig zu machen.

Typische Technikentwicklungsmethoden und -plattformen, weitverbreitete Bibliotheken oder andere Code-Komponenten unterstützen bisher kaum die Anforderungen von Ethics by Design. Gleichzeitig führen Komponenten, die mit einer aus ethischer oder datenschutzrechtlicher Sicht besseren Gestaltung aufwarten, allenfalls ein Nischendasein. In diesen Bereichen sind Änderungen nötig, damit der Einbau ethischer Prinzipien im Allgemeinen und Datenschutzprinzipien im Speziellen die Regel wird, statt weiterhin eine Ausnimmeeigenschaft darzustellen. Ethics by Design erfordert einen Brückenschlag zwischen verschiedenen Gemeinschaften („Communities“) und hat Auswirkungen auf die betroffenen Berufsbilder. Hilfreich für die Umsetzung wären neben Informationen zu Methoden und Katalogen **Best-Practice-Konzepte, unterstützende Werkzeuge, Entwicklungs-Frameworks und (Open-Source-)Code-Komponenten**. Über Plattformen mit Repositoryn für solche Komponenten sowie verwendbare Datenbestände, die gegebenenfalls Überprüfungen erst möglich machen, könnten die besonderen Eigenschaften herausgestellt, nötige Dokumentationen gleich mitgeliefert und Möglichkeiten zum Austausch von Erfahrungswissen bereitgestellt werden.

Auch wenn Ethics by Design ein wichtiges Governance-Instrument ist, um Produkte, Prozesse und Dienstleistungen von Beginn an im Interesse des Individuums und des Gemeinwohls zu gestalten, ist es kein Garant für ethische Produkte und Dienstleistungen. Ethische Prinzipien können und sollen die Technologieentwicklung positiv beeinflussen, **Ethik lässt sich aber nicht an Technik delegieren**. Zudem sollten Entscheidungen darüber, welche ethischen Prinzipien wie umgesetzt werden, z. B. ob, und wenn ja, welche Fairnessmaße für algorithmische Systeme verwendet werden, nicht Entwicklern alleine überlassen werden, sondern kontextspezifisch und ggf. unter Einbeziehung Betroffener ausgehandelt werden.

## 5. Forschung

Während in der Forschung häufig Lösungsansätze für eine ethisch besser fundierte Gestaltung von datenverarbeitenden Systemen entwickelt und exemplarisch umgesetzt werden, besteht zwischen Wissenschaft und Praxis eine gewisse Kluft. Dies könnte darauf zurückzuführen sein, dass einige der technischen Lösungen, bspw. auf Basis von kryptographischen Mechanismen, kontraintuitive Eigenschaften aufweisen, die im Vergleich zu herkömmlichen Methoden für viele Menschen schwer verständlich sind (wie ein Ausweis, der bei jedem Vorzeigen anders aussieht und damit die Verknüpfbarkeit von beobachteten Aktionen verhindert). Die vorhandenen **mentalen Modelle**, die viele Menschen aus der (analogen) Welt haben, reichen nicht aus, um ein **Verständnis** für solche innovativen Technologien zu erzeugen oder den Mehrwert zu vermitteln. Solange aber Schwierigkeiten im Verständnis oder in der Verwendung bestehen, ist die Verbreitung solcher Technologien schwierig, selbst wenn sie Vorteile bezüglich ihrer ethischen oder datenschutzrechtlichen Eigenschaften mit sich bringen.

Vielfach erfordern das Verstehen von Implikationen neuer Entwicklungen und das ethisch fundierte Gestalten eine übergreifende und damit auch interdisziplinäre Zusammenarbeit, welche von den disziplinären Metriken für gute Wissenschaft und Forschung nicht erfasst wird. Hier ist ein Umdenken in unterschiedlichen Bereichen (z.B. Hochschulen, Publikationsbewertung, Gutachterweisen) erforderlich, damit interdisziplinäre Forschung eine angemessene Würdigung erhält. Forschungsförderungen sollten die interdisziplinäre Zusammenarbeit, die zu Ergebnissen führt, die in den Einzeldisziplinen gar nicht hätten erreicht werden können, besonders honorieren und langfristige Karrierepfade sowie geeignete institutionelle Rahmenbedingungen vorsehen.

Im Forschungsbereich sind bereits vielfach gute und vielversprechende technische Lösungen vorhanden, die jedoch noch zu wenig nachgefragt werden. Außerdem fehlt es an Methodiken oder Technologien, die es ermöglichen, vom jetzigen Realisierungsstand einen **Migrationspfad zu einem verbesserten Status** der Technologie zu erreichen. Auch dieser Aspekt verdient eine besondere **Entwicklungs- und Innovationsförderung**, um tatsächlich bessere Lösungen in die Realität zu bringen. Statt lediglich punktuell Spitzenleistungen zu fördern, muss auch ein Fortschritt in der Breite zum ethisch fundierten Design Anerkennung finden.



## 6. Standardisierung

Spätestens als vor 20 Jahren Lawrence Lessig „Code is Law“<sup>2</sup> postulierte und damit die Relevanz der technischen Realität heraushob, sollte klar geworden sein, dass technische Standardisierung essentiell für die Umsetzung rechtlicher und ethischer Vorgaben ist. Für **technische Standardisierung** im Bereich von Kommunikationsnetzen sind bspw. die weltweit aktiven Gremien ISO/IEC, IEEE, IETF, ITU, ETSI oder W3C zuständig, für Europa ferner CEN und in Deutschland neben weiteren spezifischen Standards für öffentliche Stellen v.a. DIN. Zwar hat ein technischer Standard allein keine Gesetzeskraft, und Anwender technischer Systeme müssen auch dann das geltende Recht einhalten, wenn dieses den Anforderungen eines globalen technischen Standards widerspricht. Dennoch beeinflusst die Standardisierung das Angebot auf dem Markt massiv, sodass möglichst vermieden werden muss, dass sich Standards etablieren, die gegen geltendes Recht verstößen.

Der Prozess der Standardisierung steht häufig in der Kritik, weil ihm die demokratische Legitimation fehlt und faktisch **keine repräsentative Mitwirkung** der betroffenen Teile der Gesellschaft eröffnet ist. So sind Nichtregierungsorganisationen oder andere Vertreter der Zivilgesellschaft selten an der Standardisierung beteiligt. Auch Datenschutzbehörden können in der Regel nur in Einzelfällen an der Standardisierung technischer Systeme mitwirken. Dies kann im schlechtesten Fall dazu führen, dass der Betrieb von standardkonformen technischen Systemen nicht gleichzeitig rechtskonform wäre. Kritisiert wird auch, dass einige internationale Standards, an die sich Hersteller oder Betreiber halten sollen, **nicht öffentlich und kostenlos** zur Verfügung stehen, sondern erst erworben werden müssen.

Standardisierung in der Informationssicherheit hat in der Vergangenheit großteils dazu beigetragen, verstärkt Sicherheitsfunktionalität einzubauen und allmählich das Sicherheitsniveau zu erhöhen, bspw. beim Online-Banking. Allerdings haben die Snowden-Enthüllungen ans Tageslicht befördert, dass einige Geheimdienste und Regierungsbehörden gezielt Sicherheitslücken oder Hintertüren in Standards einzubringen versuchen, um sich zukünftige Zugriffsmöglichkeiten zu verschaffen. Es ist zu erwarten, dass die technische Standardisierung künftig einen größeren Stellenwert einnimmt, bspw. durch die Anforderung der DSGVO, den Stand der Technik zu berücksichtigen, oder als Konsequenz des IT-Sicherheitsgesetzes. Ebenso ist zu erwarten, dass die politische Einflussnahme aus vielen, auch außereuropäischen, Ländern zunehmen wird.

Eine **Folgenabschätzung** bezüglich existierender oder diskutierter Standards muss über rein technische und ökonomische Perspektiven hinausgehen und um ethische und gesellschaftliche Aspekte **erweitert** werden. Beim Standardisierungsprozess sollte der Staat Sorge dafür tragen, dass sich Akteure der Zivilgesellschaft, Datenschutzbehörden, Verbraucherschützer oder Vertreter von Betroffenenorganisationen ebenso in die Standardisierung einbringen können wie die bisher primär vertretenen Stakeholder.

2 Lawrence Lessig: Code and other Laws of Cyberspace, 1999.

## 7. Zwei Governance-Perspektiven: Daten- und Algorithmen-Perspektive

In den folgenden beiden Kapiteln werden die zuvor ausgeführten Überlegungen mittels zweier komplementärer Perspektiven auf datenbasierte, algorithmische Systeme angewendet. Die von der DEK zugrunde gelegten **allgemeinen ethischen Grundsätzen und Prinzipien** (oben Teil B) müssen zum einen handlungsleitend sein für den Umgang mit Daten, insbesondere für die ethisch fundierte Gestaltung der Sammlung von Daten, des Zugangs zu Daten und der Datennutzung. Zum anderen müssen sie handlungsleitend sein für die Gestaltung datenverarbeitender, auf Algorithmen beruhender Systeme, einschließlich der vielfach so bezeichneten „Künstlichen Intelligenz“. Bei der primär datenfokussierten Perspektive („Daten-Perspektive“) und der primär auf algorithmische Systeme fokussierten Perspektive („Algorithmen-Perspektive“) handelt es sich dabei weder um miteinander konkurrierende Sichtweisen noch um verschiedene Seiten einer derselben Medaille, sondern um **sich wechselseitig ergänzende und bedingende ethische Diskurse**, welche sich typischerweise auch in unterschiedlichen Governance-Instrumenten, einschließlich unterschiedlichen Rechtsakten, widerspiegeln.

Die **Daten-Perspektive** richtet den Blick auf die Daten, welche zum Training algorithmischer Systeme, als Datenbasis für algorithmisch geprägte Entscheidungen oder auch für eine Fülle weiterer Zwecke verwendet werden, die in spezifischer Weise mit **Bedeutungskontext und Semantik von Daten** (→ Teil C, 2.1) verbunden sind. Sie betrachtet die Daten vor allem in Bezug auf deren Herkunft sowie auf die möglichen Konsequenzen der Datenverarbeitung für bestimmte Personen, welche mit Kontext und Semantik der Daten zu tun haben. Aus ethischer wie aus rechtlicher Perspektive geht es einerseits um objektive Anforderungen an den Umgang mit Daten, noch mehr aber typischerweise um **subjektive Rechte**, welche diese Personen gegenüber einer bestimmten anderen Person oder auch gegenüber jedermann geltend machen können. Eine zentrale Unterscheidung ist diejenige zwischen personenbezogenen und nicht-personenbezogenen Daten, welche über die Anwendbarkeit der datenschutzrechtlichen Betroffenenrechte entscheidet. Aktuelle Debatten, die hier zu verorten wären, sind etwa diejenigen um ein „Dateneigentum“ oder um Open Data.

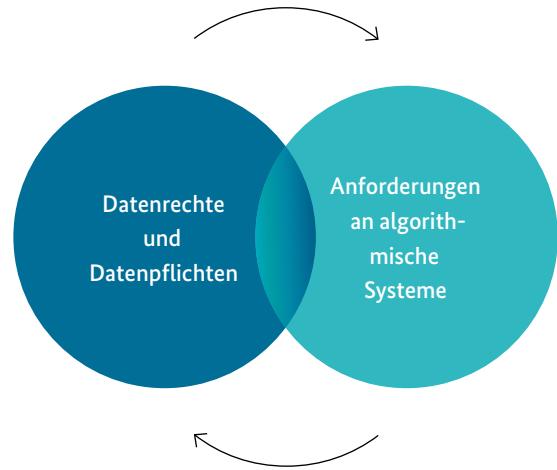


Abbildung 4:  
Daten- und Algorithmenperspektive

Die **Algorithmen-Perspektive** richtet den Blick dagegen auf die Architektur und Dynamik des datenverarbeitenden algorithmischen Systems, 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, 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, und wenn sie doch etwas mit diesen Daten zu tun haben, liegt dort bei der System-Perspektive nicht der Schwerpunkt der Betrachtung. Im Kern geht es um **objektive Anforderungen**, deren Beachtung möglicherweise eingefordert und an deren Missachtung Haftung und Sanktionen geknüpft werden können. Eine zentrale aktuelle Debatte, die hier zu verorten wäre, ist diejenige um eine sog. Algorithmenkontrolle.



Teil E

# Daten



Daten bedeuten Zugang zu Information, Information kann zu Wissen führen, und Wissen verleiht Einfluss und Macht. Durch neue Möglichkeiten automatisierter Datenverarbeitung und den exponentiellen Anstieg von Speicherkapazitäten und Rechenleistung ist der mit dem Zugang zu Daten verbundene Zuwachs an Macht und Handlungsmöglichkeiten enorm. Dabei bringt die Verfügungsmacht über wichtige Ressourcen an sich schon ein besonderes Maß an Verantwortung mit sich. So dürfen Daten – wie andere Ressourcen auch – nur zu rechtmäßigen und ethisch vertretbaren Zwecken eingesetzt werden, und bei ihrer Nutzung sind – wie bei anderen Ressourcen auch – stets die Auswirkungen mit zu bedenken, welche die Nutzung für Einzelne oder die Allgemeinheit mit sich bringen kann. Daten weisen aber auch bestimmte Charakteristika auf, die sie von anderen Ressourcen unterscheiden.

Auf Grundlage der spezifischen Charakteristika von Daten konkretisiert die DEK daher zunächst – ohne Anspruch auf Vollständigkeit – die in Teil B genannten Grundsätze und Prinzipien zu allgemeinen Anforderungen an den Umgang mit Daten ([→ unten 1.](#)) sowie zu Datenrechten und korrespondierenden Datenpflichten ([→ unten 2.](#)). Sie entwickelt sodann konkrete Handlungsempfehlungen betreffend Anforderungen für die Nutzung personenbezogener Daten ([→ unten 3.](#)), für die Verbesserung eines kontrollierten Zugangs zu personenbezogenen Daten ([→ unten 4.](#)) und für den allgemeinen Zugang zu Daten, insbesondere nicht-personenbezogenen Daten ([→ unten 5.](#)).

# 1. Allgemeine Anforderungen an den Umgang mit Daten

Ausgangspunkt für die Formulierung spezieller Prinzipien für den Umgang mit Daten sind die Unterschiede zwischen Daten und klassischen Ressourcen wie z. B. Öl oder Waren. Die spezifischen Charakteristika von Daten kommen vor allem darin zum Ausdruck, dass:

- Daten in einem **verteilten, dynamischen und prinzipiell nie völlig abgeschlossenen Prozess** durch das Zusammenwirken mehrerer Personen – welche in sehr verschiedenen Rollen auftreten (z. B. als Subjekt, über das Informationen erhoben werden, als Betreiber eines datengenerierenden Systems, als Entwickler) – entstehen und weiterverarbeitet werden;
- Daten ein **nicht-rivales Gut** sind, d. h. beliebig vervielfältigt und von einer Vielzahl von Personen parallel und in verschiedener Weise genutzt werden können;
- Daten **multifunktional und quer über alle Lebensbereiche einsetzbar** sind, wobei die Potenziale und Risiken von Daten in außergewöhnlichem Maße abhängig sind von den konkreten Zielen und Möglichkeiten eines Akteurs, insbesondere von der Verknüpfbarkeit mit anderen Daten, auch unter Berücksichtigung von Skaleneffekten.

## 1.1 Vorausschauende Verantwortung

Die Charakteristika von Daten, wie die außergewöhnlich hohe Dynamik und Abhängigkeit der Chancen und Risiken von der konkreten Konstellation, führen bei der Abwägung über die Sammlung, Nutzung oder Weitergabe von Daten zu einem besonderen Bedarf an vorausschauender Verantwortung. Bei der Abschätzung der Folgen, einschließlich der Möglichkeit einer Verletzung von Rechten anderer, sind insbesondere die folgenden Punkte zu bedenken und zu berücksichtigen:

- **Umfang** der entstehenden Datensammlungen, mit besonderem Augenmerk auf etwaigen Akkumulations-, Netzwerk- und Skaleneffekten;
- **Technologische Mittel** der Datenverarbeitung, wobei besonders an die derzeit zur Verfügung stehenden und zukünftigen technologischen **Möglichkeiten** durch größere Unternehmen und staatliche Einheiten (v. a. auch in Bezug auf die Rekombination und Entschlüsselung von Daten) zu denken ist;
- **Zweck** der Datenverarbeitung, unter besonderer Berücksichtigung möglicher Änderungen des Anwendungskontexts und der Akteurskonstellationen (z. B. durch Zugriff staatlicher Stellen oder durch Konzernübernahmen).

Bei personenbezogenen Daten hat das Prinzip vorausschauender Verantwortung in den von der DSGVO betonten Grundsätzen der Datenminimierung und der Speicherbegrenzung in typisierter Weise Ausdruck gefunden. Aber auch eine Fülle von Pflichten, angefangen von der Pflicht zu einer Datenschutzfolgenabschätzung bis hin zu Anforderungen an Vereinbarungen mit Auftragsverarbeitern, sind unmittelbar Ausfluss dieses Prinzips.



## 1.2 Achtung der Rechte beteiligter Personen

Die Nutzung von Daten muss stets die Rechte anderer respektieren. Handlungen und Unterlassungen, die ganz allgemein ethisch nicht vertretbar oder rechtswidrig sind, weil sie **Rechte anderer** verletzen, bleiben ethisch nicht vertretbar oder rechtswidrig, wenn sie mit Hilfe von Daten begangen werden (Beispiel: Betrug ist mit oder ohne Nutzung von Daten strafbar). Die Tatsache, dass Daten in einem verteilten Prozess und durch das Zusammenwirken mehrerer Personen generiert werden, kann aber auch dazu führen, dass Personen, welche an der Generierung der Daten in irgendeiner Weise beteiligt waren – etwa als Subjekt der Information oder als Eigentümer einer daten-generierenden technischen Vorrichtung – aus ethischer und möglicherweise auch aus rechtlicher Sicht **genuine datenspezifische Rechte (Datenrechte)** in Bezug auf diese Daten zustehen (→ näher unten 2). Diese Datenrechte müssen bei jeder Nutzung von Daten geachtet werden.

Achtung von Datenrechten anderer heißt dabei deutlich mehr, als nicht in fremde Rechtssphären – etwa ein fremdes Urheberrecht – einzudringen. Verlangt ist vielmehr aus ethischer Sicht eine umfassende **Rücksichtnahme** auf die datenbezogenen Interessen von Personen, die in spezifischer Weise mit den Daten verbunden sind und denen daher ein Recht auf Mitsprache und Teilhabe zukommt. Diese Pflicht zur Rücksichtnahme kann auch eine Pflicht zu aktivem Handeln, etwa zur Gewährung von bestimmten Formen des Datenzugangs, beinhalten.

Bei personenbezogenen Daten hat das Prinzip der Achtung der Datenrechte anderer vor allem Ausdruck gefunden in den von der DSGVO betonten **Grundsätzen der Rechtmäßigkeit, der Verarbeitung nach Treu und Glauben sowie der Zweckbindung**. In der DSGVO selbst normierte Datenrechte sind die Betroffenenrechte, etwa auf Auskunft, Berichtigung, Einschränkung der Verarbeitung, Löschung oder Datenübertragung (Portabilität).

## 1.3 Wohlfahrt durch Nutzen und Teilen von Daten

Ressourcen, die zum Wohl wichtiger Rechtsgüter Einzelner (z.B. Gesundheit) oder zum Wohl der Allgemeinheit – insbesondere zur Förderung einer der 17 Ziele der Vereinten Nationen für nachhaltige Entwicklung auf ökonomischer, sozialer und ökologischer Ebene – eingesetzt werden können, sollten nicht brachliegen. Ihre Nutzung ist dort, wo dies der umfassend verstandenen Wohlfahrt dient und keine überwiegenden Interessen – insbesondere keine Datenrechte anderer – entgegenstehen, grund-sätzlich **ethisch geboten**.

Daten zeichnen sich durch das besondere Charakteristikum aus, nicht-rivale Güter zu sein. Sie nutzen sich bei ihrer parallelen Nutzung durch viele verschiedene Akteure zu vielen verschiedenen Zwecken nicht ab und sind nahezu beliebig vervielfältigbar. Durch das **Teilen von Daten** kann ein Zustand eintreten, bei dem die teilende Partei zumindest nicht schlechter, alle anderen im weiteren Sinne Beteiligten dafür aber besser stehen als wenn das Teilen der Daten unterblieben wäre. Diesem Umstand sollte ein ethisch verantwortlicher Umgang mit Daten Rechnung tragen. Teilen von Daten hat zudem immense Bedeutung für die Sicherstellung eines **fairen und effizienten Wettbewerbs**.

Allerdings kann das Prinzip der Nutzung und des Teilens von Daten in einem Spannungsverhältnis mit dem Prinzip vorausschauender Verantwortung und dem Prinzip der Achtung der Datenrechte anderer stehen, ebenso wie mit Erwägungen zu einem angemessenen Leistungsschutz. Daher sollten Anreize zum **freiwilligen Teilen** stets Vorrang genießen und eine gesetzliche Pflicht zum Teilen die Ausnahme sein.

## 1.4 Zweckadäquate Datenqualität

Daten – zusammen genommen mit ihrem Kontext und der Semantik – sind gespeicherte Information. Information geht regelmäßig mit dem Anspruch einher, ein möglichst getreues Abbild der gegenwärtigen Realität oder eine möglichst treffsichere Voraussage einer künftigen Realität zu sein. Während es jenseits der automatisierten Verarbeitung von Daten durch algorithmische Systeme für alle offenkundig ist, dass Fehlinformationen nicht nur wertlos, sondern schädigend sein können, kommt es durch die Automatisierung oft zu einer verführerischen **Schein-objektivität** und einer gefährlichen Bereitschaft, sich trotz einer falschen oder unvollständigen Datenbasis auf ein Berechnungsergebnis zu verlassen, das genauso schlecht ist wie seine Datenbasis („*Garbage in, garbage out*“).

Ein verantwortungsvoller Umgang mit Daten in der Datengesellschaft setzt daher im Interesse aller auch das Bemühen um eine **dem Einsatzzweck angemessene Datenqualität** voraus (→ siehe oben Teil C, 2.1.1). Die Bestimmung dessen, was jeweils eine „angemessene“ Datenqualität bedeutet, muss jedoch stets **kontextspezifisch** erfolgen. Beispielsweise ist zu berücksichtigen, dass Daten gesellschaftliche Vorannahmen, Stereotypen und Diskriminierungen abbilden können, welche in Folge die Funktionsweise eines algorithmischen Systems bestimmen, das mit Hilfe dieser Daten trainiert wird (→ näher unten Teil F, 2.6). Insofern kann es geboten sein, das getreue Abbild eines bestehenden Defizits, das etwa für statistische Zwecke qualitativ hochwertig sein kann, gerade nicht als Datengrundlage für andere Zwecke zugrunde zu legen.

In diesem Zusammenhang ist auch zu berücksichtigen, dass Daten über verschiedene Lebensbereiche hinweg und zu unterschiedlichen Zwecken einsetzbar sind. In diesem Zusammenhang kann daher auch das sog. **FAIR-Prinzip** (*Findable, Accessible, Interoperable, Reusable*) relevant sein, welches etwa die Modi der Speicherung und Kodierung von Daten betrifft. Danach sollten Daten möglichst so aufbereitet und gespeichert sein, dass sie auffindbar und zugänglich sind, dass sie in einem gängigen Format kodiert sind und in einer Weise, die kontextabhängig möglichst vielen Akteuren die weitere Nutzung der Daten ermöglicht.

Bei personenbezogenen Daten hat das Streben nach einem hohen Maß an Datenqualität in dem von der DSGVO betonten **Prinzip der Richtigkeit** Ausdruck gefunden.

## 1.5 Risikoadäquate Informationssicherheit

Daten können beliebig vervielfältigt werden. Sind sie einmal in andere Hände gelangt, können sie **kaum zurückgeholt** werden. Sie sind zudem aufgrund zahlreicher und vielfach unbemerkt bleibender **Angriffsmöglichkeiten** von außen besonders verletzlich gegenüber Verfälschung und Zerstörung. In unmittelbarem Zusammenhang mit dem Prinzip vorausschauender Verantwortung ebenso wie dem Prinzip der Achtung von Rechten beteiligter Personen steht daher in technischer Hinsicht ein hohes und dem jeweiligen Risikopotenzial angemessenes Maß an **Informationssicherheit**. Ausreichende Informationssicherheit, die eine breite Palette von Maßnahmen auf unterschiedlichen Ebenen umfasst, ist eine notwendige Voraussetzung für vertrauensvolles Handeln in der Datengesellschaft.

Bei personenbezogenen Daten hat Informationssicherheit in dem von der DSGVO betonten **Prinzip der Integrität und Vertraulichkeit** Ausdruck gefunden.

## 1.6 Interessenadäquate Transparenz

Die Tatsache, dass die faktische Kontrolle und die Nutzung von Daten auch Einfluss und Macht bedeuten kann, bedingt, dass derjenige, der Daten faktisch kontrolliert und nutzt, prinzipiell bereit und in der Lage sein muss, für sein Handeln **Rechenschaft** abzulegen. Das gilt auch und gerade zum Schutze derjenigen, deren Datenrechte potenziell betroffen oder gar verletzt sind. Damit diese Personen, oder aber auch Stellen, die zur Wahrnehmung der Datenrechte anderer berufen sind, überhaupt feststellen können, ob und inwieweit Datenrechte tatsächlich betroffen oder gar verletzt sind und wem gegenüber sie Ansprüche geltend machen können, bedarf es einer **den potenziell betroffenen Interessen angemessenen Transparenz**.



Bei personenbezogenen Daten ist die Transparenz im Sinne der **Nachvollziehbarkeit der Datenverarbeitung** für betroffene Personen ebenso ein festes Grundprinzip der DSGVO wie die **Rechenschaftspflicht**. Eine Vielzahl von Regelungen der DSGVO, etwa betreffend Information, Dokumentation oder Auskunftsrechten, sollen Transparenz gewährleisten.

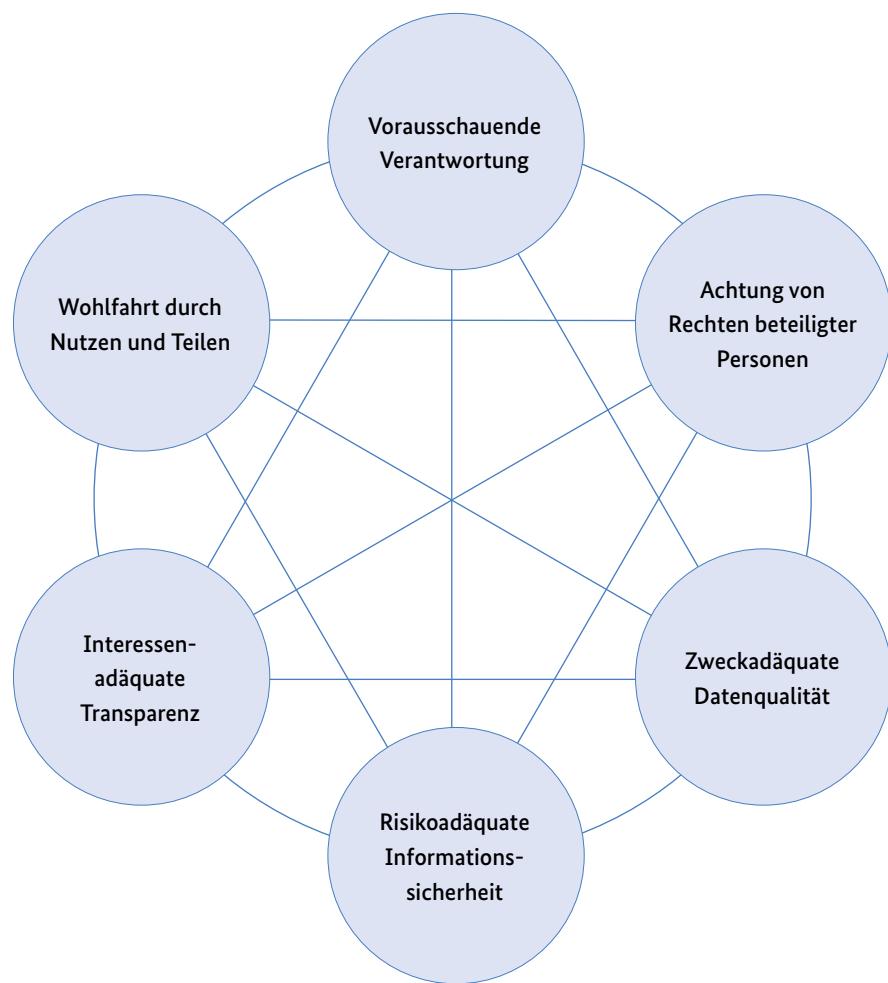


Abbildung 5: Anforderungen an den Umgang mit Daten

## 2. Datenrechte und korrespondierende Datenpflichten

Das ethische Prinzip digitaler Selbstbestimmung begreift den Einzelnen nicht nur als passiv, schutzbedürftig und aktuell oder potenziell bedroht, sondern als **selbstbestimmten Akteur in der Datengesellschaft**. Um sich als Akteur in der Datengesellschaft selbstbestimmt bewegen zu können, bedarf es subjektiver Rechte, die dem Einzelnen 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 prinzipiell auch für Unternehmen und **juristische Personen** und – zumindest in Ansätzen – für Gruppen von Personen (Kollektive). Vor diesem Hintergrund sieht die DEK allgemeine, über Datenschutz hinausgehende, Grundsätze von Datenrechten und Datenpflichten.<sup>1</sup>

### 2.1 Allgemeine Grundsätze von Datenrechten und Datenpflichten

In komplexen Prozessen der Generierung von Daten – verstanden in einem weiteren Sinne, einschließlich verschiedener Phasen der Datenherstellung, Datenanreicherung und Datenveredelung – interagieren häufig unterschiedliche Akteure mit unterschiedlichen Zielen miteinander und tragen dabei in unterschiedlichen Rollen zur Generierung von Daten bei. Ein relevanter **Beitrag eines Akteurs** (natürliche oder juristische Person) zur Generierung von Daten kann darin bestehen, dass

- a) sich die in den Daten gespeicherten Informationen in ihrer Bedeutung auf diesen Akteur, oder auf einen mit diesem Akteur verbundenen (z.B. ihm gehörenden) Gegenstand, beziehen;

- b) die Daten durch eine Aktivität dieses Akteurs, oder durch Verwendung eines ihm gehörenden Gegenstands (z.B. eines Sensors), generiert wurden; oder
- c) die Daten durch Software oder eine andere Komponente (z.B. Sensoren) generiert wurden, welche dieser Akteur geschaffen hat oder in welche er investiert hat.

Dabei kommt der unter a) genannten Situation, dass ein Akteur Subjekt der in den Daten gespeicherten Information ist, bei natürlichen Personen eine herausgehobene Bedeutung zu, ist sie doch zugleich Anknüpfungspunkt für das verfassungsrechtlich geschützte Recht auf informationelle Selbstbestimmung und Datenschutz.

Ein Beitrag zur Generierung von Daten führt angesichts der spezifischen Charakteristika von Daten sowie – bei personenbezogenen Daten – angesichts der untrennbarer Verknüpfung mit Persönlichkeitsrechten nach Auffassung der DEK jenseits des geltenden Immaterialgüterrechts nicht zu exklusiven Eigentumsrechten an Daten (→ siehe und 5.2.4). Vielmehr folgen aus einem solchen Beitrag Datenrechte eines Akteurs in Gestalt von **Mitspracherechte- und Teilhaberechten**, mit denen korrespondierende Pflichten anderer Akteure einhergehen. Zwischen einem Akteur, der an der Generierung von Daten beteiligt war, und einem Akteur, der diese Daten faktisch kontrolliert, entsteht aus ethischer Sicht daher eine **dynamische Sonderbeziehung**. Diese Beziehung kann mehr oder minder langfristig sowie stärker oder schwächer ausgeprägt sein. Bezüglich personenbezogener Daten ist sie weitgehend durch das geltende Datenschutzrecht determiniert.

Die **Anerkennung und Ausgestaltung** von Datenrechten und korrespondierenden Datenpflichten in dynamischen Umgebungen hängt aus ethischer Sicht von den folgenden allgemeinen Faktoren ab, die dort, wo Datenrechte und Datenpflichten bereits gesetzlich konkretisiert wurden, regelmäßig auch der rechtlichen Beurteilung zugrunde liegen:

<sup>1</sup> Modell der Datenrechte und Datenpflichten in Anlehnung an Vorentwürfe Nr. 2 (Februar 2019) und Nr. 3 (Oktober 2019) der Principles for a Data Economy des European Law Institute (ELI) und des American Law Institute (ALI), die der DEK zur Verfügung gestellt wurden. Die Vorentwürfe sind bislang weder von ALI noch von ELI verabschiedet worden und stellen noch nicht die offizielle Position einer oder beider Organisationen dar.



- a) Umfang und Art des **Beitrags zur Datengenerierung** desjenigen Akteurs, der ein Datenrecht geltend macht;
- b) **Gewicht des Individualinteresses** desjenigen Akteurs, der das Datenrecht geltend macht, an der Gewährung des Datenrechts (insbesondere an Unterlassung/Zugang/Korrektur/wirtschaftlicher Teilhabe);
- c) Gewicht von ggf. **konfliktierenden Individualinteressen** desjenigen Akteurs, dem gegenüber das Datenrecht geltend gemacht wird, oder Dritter, unter Berücksichtigung von Ausgleichsmöglichkeiten (z.B. Schutzmaßnahmen, Vergütung);
- d) Gewicht von **Interessen der Allgemeinheit**;
- e) **Machtverteilung** zwischen dem Akteur, der das Datenrecht geltend macht, und dem Akteur, dem gegenüber das Datenrecht geltend gemacht wird.

Diese Faktoren wirken im Wege eines beweglichen Systems zusammen, d.h., dass etwa ein besonders stark ausgeprägtes Allgemeininteresse am Datenzugang den besonders schwach ausgeprägten Beitrag zur Datengenerierung ausgleichen kann. Dabei sind die in Teil B dargelegten allgemeinen Grundsätze und Prinzipien stets zu berücksichtigen, so dass es nicht zu einer Aushöhlung zentraler Individualinteressen durch tatsächliche oder bloß vermeintliche Allgemeininteressen kommen kann. Die Faktoren bestimmen auch die **Konkretisierung und Ausgestaltung** z.B. von Formaten, Fristen, Schutzmaßnahmen oder finanzieller Entschädigung. Dazu gehört auch die Frage, ob nur auf Ansuchen desjenigen, der ein Datenrecht geltend macht (z.B. Datenzugangsanspruch), oder auch proaktiv (z.B. Datenveröffentlichungspflicht) gehandelt werden muss.

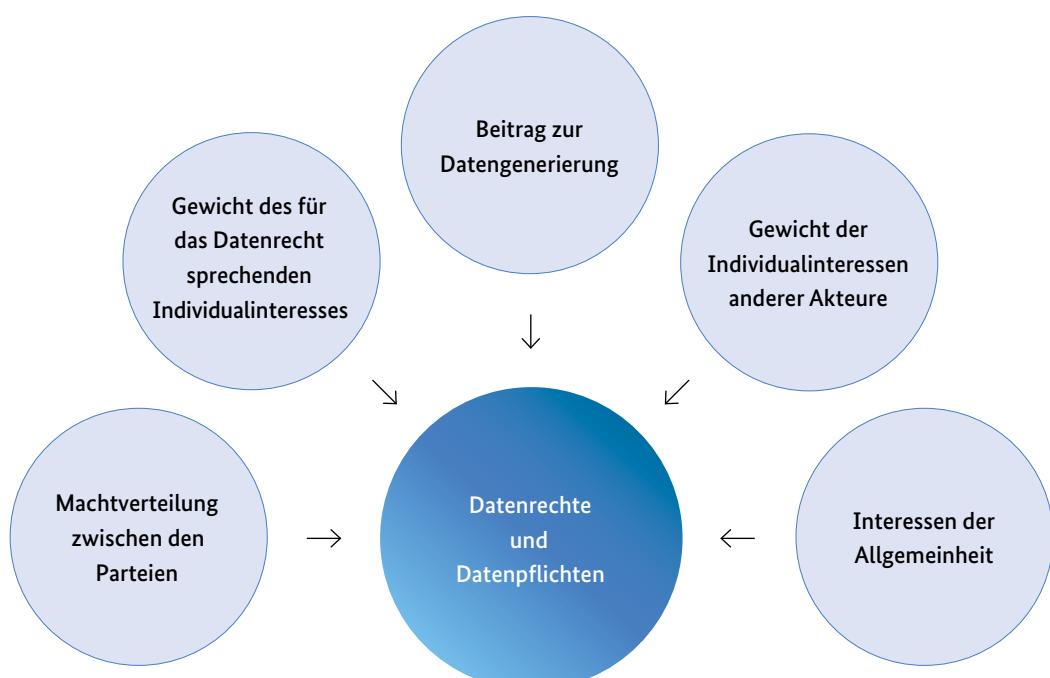


Abbildung 6: Allgemeine Faktoren zur Ausgestaltung von Datenrechten und korrespondierenden Datenpflichten

Die **Betroffenenrechte** der 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. Die hier formulierten Grundsätze können allerdings auch für nicht-personenbezogene Daten herangezogen werden, und sie gelten nicht nur für Individuen, sondern auch für juristische Personen und für Kollektive.

## 2.2 Konkretisierung der allgemeinen Grundsätze anhand typischer Szenarien

Von der **Zielrichtung** her können Datenrechte insbesondere auf eine Unterlassung der Datennutzung (bis hin zur Löschungspflicht), auf Zugang zu Daten (z.B. Offenlegung, Übertragung, volle Portabilität), auf eine Korrektur von Daten oder auf wirtschaftliche Teilhabe ausgerichtet sein.

### 2.2.1 Unterlassungs-Szenarien

Vielfach wird eine Situation gegeben sein, in welcher ein Akteur von einem anderen Akteur verlangt, eine bestimmte Datennutzung zu unterlassen. In Bezug auf personenbezogene Daten geht die DSGVO sogar vom Grundsatz der Unterlassungspflicht aus, sofern nicht eine Rechtsgrundlage gegeben ist und die übrigen Anforderungen eingehalten werden.<sup>2</sup> Auch jenseits des Anwendungsbereichs der DSGVO und ganz allgemein kann sich das Gewicht des Individualinteresses desjenigen Akteurs, der das Datenrecht geltend macht, aus ethischer Sicht zu einem **Unterlassungsanspruch** – bis hin zu einem Anspruch auf Löschung der Daten – verdichten, wenn die Datenverarbeitung

- a) diesem oder einem anderen Akteur Schaden zufügen könnte; und
- b) unvereinbar ist mit den Umständen, unter denen der Beitrag zur Datengenerierung geleistet wurde, insbesondere, weil
  - (i) dies zu einem anderen Zweck erfolgte und nicht zu erwarten ist, dass der Akteur den Beitrag freiwillig geleistet hätte, wenn er die jetzige Datenverarbeitung vorhergesehen hätte; oder
  - (ii) sein Einverständnis aus übergeordneten Gründen unwirksam wäre.

Bevor ein Unterlassungsanspruch bejaht werden kann, ist das so konkretisierte Individualinteresse jedoch noch mit den oben (→) genannten weiteren Faktoren in Abwägung zu bringen. Unterlassung kann daher etwa nicht begehrt werden, wenn die Datenverarbeitung ganz ausnahmsweise aus zwingenden Gründen (z.B. Verfolgung von Straftaten) dennoch gerechtfertigt ist.

2 Art. 6 Abs. 1, Art. 9 Abs. 1 DSGVO.



In Bezug auf **nicht-personenbezogene Daten** kann ein Unterlassungsanspruch beispielsweise in Wertschöpfungsketten und Kundenbeziehungen Bedeutung haben, in denen nicht-personenbezogene Daten von großer wirtschaftlicher Bedeutung sind, die Interessen der Beteiligten an einer Unterlassung aber durchaus gewichtig sein können (→ unten 5.3).

---

### Beispiel 1

*Von den Sensoren moderner Landmaschinen gesammelte nicht-personenbezogene Daten (Bodenqualität, Wetter usw.) werden von den Herstellern für die Erbringung zahlreicher Dienstleistungen (Precision Farming, Predictive Maintenance u.a.) genutzt. Würde der Hersteller die Daten auch an mögliche Investoren oder an Verpächter weiterleiten, erhielten diese damit Informationen, welche dem landwirtschaftlichen Betrieb bei künftigen Verhandlungen über seine Flächen schaden können. Es ist nicht davon auszugehen, dass ein landwirtschaftlicher Betrieb freiwillig zu diesem Zweck an der Generierung der Daten mitgewirkt hätte. Bei der ethischen Bewertung eines Unterlassungsanspruchs ist neben dem konkreten Machtverhältnis auch zu berücksichtigen, dass der Betrieb einen sehr gewichtigen Beitrag zur Generierung der Daten geleistet hat. An schutzwürdigen Interessen Dritter kämen nur das Erwerbsinteresse des Herstellers und ein Allgemeineresse an der korrekten Information für Investoren, Verpächter etc. in Betracht.*

---

Ein **Verzicht** auf einen eigentlich begründeten Unterlassungsanspruch ist aus ethischer Sicht nur begrenzt möglich. Er verbietet sich von selbst, wenn das Einverständnis zur Datennutzung im Sinne der Voraussetzung b. (ii) aus übergeordneten Gesichtspunkten heraus unwirksam wäre, etwa weil es gegen das Gesetz oder die guten Sitten verstößen würde, da nach unserer Rechts- und Werteordnung keine beliebige Selbst- oder Fremdschädigung akzeptiert werden kann. Soweit dies nicht der Fall ist, kann gegebenenfalls bei Erfüllung strenger Anforderungen an den Verzicht – etwa durch eine gesonderte Vereinbarung ohne Druck oder Koppelung mit anderen Leistungen – Freiwilligkeit gesichert werden, womit Voraussetzung b) (i) entfallen würde.

---

*In könnte der landwirtschaftliche Betrieb die Datenweitergabe an Dritte gestatten – beispielsweise aufgrund einer individuellen Vereinbarung mit entsprechender Vergütung und ohne, dass die Nutzung des Traktors davon abhängig gemacht würde.*

---

Für **personenbezogene Daten** folgen Unterlassungspflichten zwar regelmäßig bereits aus dem geltenden Datenschutzrecht, doch können die genannten Kriterien etwa herangezogen werden, um zu entscheiden, ob **die materiellen Grenzen der Einwilligung** überschritten werden (→ unten 3.2.1), oder um die Abwägung berechtigter Interessen zu konkretisieren.

---

### Beispiel 2

*Vom Nutzer eines sozialen Netzwerks wird mittels Daten über das Nutzungsverhalten ein umfassendes Persönlichkeitsprofil angelegt, das u.a. die Punkte „psychisch labil“ und „Esoterik“ beinhaltet. Er wird in der Folge fast täglich – oft in zeitlichem Zusammenhang mit Postings, die psychische Anspannung signalisieren – mit Angeboten über teure persönliche Horoskope, Leistungen von „Energetikern“ usw. konfrontiert, welche er vielfach annimmt. Bei Einrichtung seines Nutzerkontos hatte er ein Kästchen mit folgendem Text angeklickt: „Ich möchte, dass meine Daten im Hinblick auf persönliche Präferenzen und Eigenschaften ausgewertet werden, um Dienste, auch von Drittanbietern, besser personalisieren zu können (Profiling)“. Diese „Einwilligung“ macht die Verarbeitung aber nicht zulässig. Das kann auf verschiedene Weise begründet werden, u.a. damit, dass die Verarbeitung zu diesem Zweck dem Nutzer erheblichen Schaden zufügt und dies mit den Umständen, unter denen er die Daten generiert hat, unvereinbar ist (etwa weil er bei Kenntnis der Zusammenhänge mit diesem Zweck die Daten nicht generiert hätte, und weil die Rechtsordnung die Ausnutzung solcher psychischer Zustände missbilligt, vgl. § 138 BGB).*

---

Vielfach wird es Unterlassungspflichten geben, die durch keine Einwilligung oder Abwägung relativiert werden können, wobei oft von „roten Linien“ oder „**absoluten Grenzen**“ die Rede ist. Diese Grenzen müssen nicht datenspezifisch sein; und die meisten sind es auch nicht. Beispielsweise wäre eine dem Demokratieprinzip zuwiderlaufende Beeinflussung von Wahlen mit oder ohne Nutzung von Daten zu unterlassen. Eine datenspezifische absolute Grenze ist nach Auffassung der DEK etwa die Totalüberwachung von Menschen.

---

### Beispiel 3

*Eine Angestellte verpflichtet sich bei Abschluss des Arbeitsvertrags, die Standortfunktion von SmartWatch und Mobiltelefon sowie eine Reihe von Daten erhebenden Applikationen (u.a. zum Monitoring des Schlafverhaltens und von Emotionen) auch im Privatleben stets eingeschaltet zu lassen und die Geräte dem Arbeitgeber jederzeit auf Aufforderung zum Auslesen der Daten zur Verfügung zu stellen. Selbst wenn die Angestellte in jede dieser Maßnahmen eingewilligt haben sollte, und selbst wenn sie sich aus freien Stücken für diesen Arbeitgeber entschieden hat und ebenso gut das Angebot eines anderen Arbeitgebers hätte annehmen können, ergibt sich mindestens in der Gesamtschau eine vollständige oder annähernde Totalüberwachung, die mit der Menschewürde, der Selbstbestimmung und der Privatheit nicht vereinbar ist.*

---



Umgekehrt können die für Unterlassungs-Szenarien geltenden Kriterien auch indirekt relevant werden, wenn es um ethische oder gar rechtliche **Pflichten zur Datennutzung** geht. Eine solche kann insbesondere dann bestehen, wenn einen Akteur die Pflicht trifft, wichtige Rechtsgüter zu schützen und er über Daten verfügt, deren Nutzung geeignet ist, diesen Schutz zu gewährleisten oder zu verbessern. Die Pflicht zum Schutz wichtiger Rechtsgüter kann dann zu einer Pflicht zur Nutzung dieser Daten führen, jedenfalls sofern kein entgegenstehender begründeter Unterlassungsanspruch eines anderen Akteurs besteht.

#### **Beispiel 4**

*Ein Krankenhaus hat Probleme mit einem multiresistenten Keim. Um bessere Erkenntnisse zur Anfälligkeit bestimmter Patienten zu erhalten, so dass diese möglicherweise gezielt in ein anderes Haus verlegt werden können, wäre es erforderlich, die Gesundheitsdaten derjenigen Patienten zu analysieren, die in der letzten Zeit mit dem Keim angesteckt wurden. In einer solchen Situation hat das Krankenhaus generell die Pflicht, neue Patienten bestmöglich vor einer Infektion zu schützen und dazu alle verfügbaren und zumutbaren Vorsichtsmaßnahmen zu ergreifen. Dies umfasst auch die Nutzung der Gesundheitsdaten der Patienten, die sich bereits angesteckt hatten, sofern dies neue Patienten schützen kann und gegenüber den bereits angesteckten Patienten keine Unterlassungspflicht besteht.*

#### **2.2.2 Zugangs-Szenarien**

Bei der Frage des Zugangs zu Daten wird es zunächst sehr viele Situationen geben, in denen sich die Zugang suchende und die die Daten faktisch kontrollierende Partei „handelseinig“ werden. Sofern keine überwiegenden Interessen Dritter oder der Allgemeinheit dagegen sprechen, insbesondere keinem Akteur nach den oben genannten Kriterien ein Unterlassungsanspruch zusteht, sind solche **freiwilligen Arrangements** zu begrüßen. Angesichts des hohen Wertschöpfungspotenzials, das mit der Verfügbarkeit und Auswertung von Daten einhergehen kann, wird jedoch auch intensiv diskutiert, unter welchen Voraussetzungen und Bedingungen ein Zugang zu Daten aus ethischer Sicht gewährt werden soll oder gar muss.<sup>3</sup>

Dabei ist zunächst an Situationen zu denken, in denen die Erfüllung einer besonderen, vielfach sogar gesetzlich festgelegten, **Pflicht oder Aufgabe** (z.B. Strafverfolgung, Sorge für die öffentliche Gesundheit) den Zugang zu Daten erfordert. Ein etwaiges Recht, Zugang zu Daten zu erhalten, folgt dann den für diese Pflicht oder Aufgabe geltenden Regeln, wobei vor allem dem **Grundsatz der Verhältnismäßigkeit** überragende Bedeutung zukommt und stets etwaige Unterlassungsansprüche (→ oben ) betroffener Akteure zu prüfen sind.

Zudem kann es zu einer Geltendmachung von selbständigen Ansprüchen auf Zugang zu Daten kommen, etwa innerhalb **bestehender Wertschöpfungssysteme**, in denen meist viele Akteure in unterschiedlichen Rollen (z.B. als Zulieferunternehmen, Hersteller, Händler, Endnutzer) zur Generierung von Daten beitragen und dabei sowohl die eigenen Rollen als auch die Rollen anderer Akteure prinzipiell kennen und akzeptieren (→ näher unten 5.3). Das Individualinteresse eines Akteurs, welches für die Zugangsgewährung geltend gemacht wird, kann dann insbesondere darin bestehen, dass die Daten erforderlich sind für die

<sup>3</sup> Siehe anstelle vieler: Europäische Kommission: Aufbau einer europäischen Datenwirtschaft, COM(2017) 9 final, 10.1.2017, S. 11 ff (abrufbar unter: <https://ec.europa.eu/transparency/regdoc/rep/1/2017/DE/COM-2017-9-F1-DE-MAIN-PART-1.PDF>); Europäische Kommission: Aufbau eines gemeinsamen europäischen Datenraums, COM(2018) 232 final, 25.4.2018, S. 10 ff (abrufbar unter: <https://ec.europa.eu/transparency/regdoc/rep/1/2018/DE/COM-2018-232-F1-DE-MAIN-PART-1.PDF>).

- a) bestimmungsgemäße Nutzung eines im Rahmen des Wertschöpfungssystems genutzten Gutes (z.B. Reparatur einer vernetzten Maschine durch den Endnutzer);
- b) Qualitätskontrolle und -verbesserung einer im Rahmen des Wertschöpfungssystems erbrachten Leistung (z.B. seitens eines Zulieferunternehmens);
- c) Wahrheitsfindung bzw. Beweisführung (z.B. in einem Rechtsstreit mit Dritten);
- d) Vermeidung von wettbewerbswidrigen Effekten (z.B. Lock-in-Effekten); oder eine
- e) neue Wertschöpfung mit Hilfe der Daten (z.B. durch Entwicklung eines Smart Service).

Zugangsansprüche auf ähnlicher Basis werden auch diskutiert, wenn die Zugang suchende Partei und die Partei, die die Daten faktisch kontrolliert, zwar noch nicht Teil desselben Wertschöpfungssystems sind, ein **neues Wertschöpfungssystem** aber gerade geschaffen werden könnte. In solchen Situationen fällt die Bewertung anhand der allgemeinen Kriterien meist anders aus, schon weil die Zugang suchende Partei oft überhaupt keinen Beitrag zur Generierung der Daten geleistet hat und es eher **allgemeine Wohlfahrtserwägungen** oder spezielle Erwägungen, etwa zur Sicherung des **Wettbewerbs**, sind, welche für einen Datenzugang ins Feld geführt werden können (→ näher unten 5.5).

#### **Beispiel 5**

*Ein Zulieferunternehmen stellt die Motoren für die Landmaschinen her. Damit das Zulieferunternehmen die Qualität seiner Motoren überprüfen und stetig verbessern kann, wäre es für das Unternehmen sehr wichtig, Zugang zu bestimmten Traktordaten zu erhalten. Diese werden allerdings in der Cloud des Herstellers gespeichert, der dem Zulieferunternehmen keinen Zugang gewähren will. In dieser Situation wäre zu berücksichtigen, dass der Zulieferer einen signifikanten Beitrag zur Generierung der Motorendaten geleistet hat und die Daten dringend für die Qualitätsverbesserung einer Leistung im selben Wertschöpfungssystem benötigt, an dem auch der Hersteller beteiligt ist. Neben den konkreten Machtverhältnissen wäre auch zu berücksichtigen, dass alle Beteiligten, einschließlich der Allgemeinheit, ein Interesse an guter Motorenqualität haben. Auf der Seite des Herstellers könnten ökonomische Interessen, insbesondere Geheimhaltungsinteressen, zu berücksichtigen sein.*

#### **Beispiel 6**

*Angenommen in hätte der Hersteller – ein beherrschendes Unternehmen auf dem Traktorenmarkt – Boden- und Wetterdaten über Jahrzehnte gesammelt. Ein Start-up erkennt das Potenzial, mit den Daten eine Datenbank für Investoren aufzubauen und begeht nun Zugang zu den Daten. Hier wäre zu berücksichtigen, dass das Start-up selbst keinen Beitrag zur Generierung der Daten geleistet hat. Ob und welches Allgemeininteresse am Datenzugang besteht, hängt davon ab, ob der Hersteller seine Marktmacht missbraucht, sowie davon, welche Bedeutung die Brechung der Marktmacht weniger Unternehmen für die gedeihliche Entwicklung der europäischen Wirtschaft hat (falls das Start-up überhaupt in Europa arbeitet). In jedem Fall gilt es zu bedenken, dass Geschäftsgeheimnisse und andere Interessen Dritter – wie etwa des Herstellers und der landwirtschaftlichen Betriebe in Beispiel 1 – durch die Datenoffenlegung potenziell massiv beeinträchtigt werden.*



Zu den allgemein anerkannten Prinzipien von **Open Government Data**, also der Zurverfügungstellung von Daten der öffentlichen Hand an Private, gehören Prinzipien wie „standardmäßig offen“ und „verwendbar von allen zu jedem Zweck“.<sup>4</sup> Viele wollen diese Prinzipien im Sinne weitergehender Open-Data-Konzepte auch auf Daten ausweiten, die bei Privaten entstanden sind und von ihnen faktisch kontrolliert werden. Eine schwierige ethische Frage ist im Zusammenhang mit Open Data, inwieweit eine typisierte, d.h. den konkreten Einzelfall nicht mehr berücksichtigende Beurteilung von Interessen der Allgemeinheit erfolgen darf.

Die DEK betont in diesem Zusammenhang die Bedeutung der individuellen (denkbaren) Unterlassungsansprüche derjenigen Akteure, die zur Generierung der Daten beigetragen haben – insbesondere derjenigen, auf die sich die Daten beziehen. Das bedeutet, dass nicht nur unter Abwägung des Schädigungspotenzials und des zu erwartenden Gemeinwohlnutzens alle möglichen und zumutbaren Schutzmaßnahmen (einschließlich ständig neu zu verbessernder Anonymisierungstechniken) zu ergreifen sind, sondern dass sich eine pauschalierende Zugangsgewährung je nach Schädigungspotenzial auch ganz verbieten kann (→ näher unten ).

#### **Beispiel 7**

*Eine Stadt erhebt zur Erleichterung der Verkehrsplanung (u.a. Anpassung der Taktung öffentlicher Verkehrsmittel) in großem Umfang Mobilitätsdaten mithilfe von Smartphone-Signalen. Die Daten sind theoretisch „anonymisiert“, doch lässt sich bei Zusammenführen mit anderen Datensätzen und etwas Zusatzwissen ein bestimmter Smartphone-Besitzer mit 95%iger Wahrscheinlichkeit identifizieren. Für diese Daten interessieren sich u.a.: ein Forscher, der Erkenntnisse für die optimale Gestaltung von Erholungsflächen im Stadtgebiet gewinnen möchte; ein Start-up mit der Geschäftsidee einer Online-Detektei, bei der man gegen Entgelt Mobilitätsprofile seines Ehepartners, Konkurrenten usw. abfragen kann; ein Forschungsinstitut, das im Auftrag der Regierung eines ausländischen Staates Erkenntnisse über die politischen Aktivitäten ihrer Staatsbürger erlangen soll. Bei individueller Beurteilung wären die drei Zugangsverlangen sehr unterschiedlich zu bewerten. Es stellt sich daher die Frage, unter welchen Bedingungen die Stadt im Hinblick auf viele mögliche gemeinwohlfördernde Nutzungen die Daten offen bereitstellen darf oder gar muss.*

#### **2.2.3 Korrektur-Szenarien**

Daten können qualitativ schlecht sein. Insbesondere können der Kontext unpassend, die Kodierung **falsch** oder die Daten in einem Maße **unvollständig** sein, dass die mit ihrer Hilfe gewonnenen Ableitungen falsch werden. In derartigen Konstellationen kann sich ein ethisch begründeter Anspruch eines Akteurs, der an der Generierung von Daten beteiligt war, auf Korrektur der zu Grunde gelegten Daten oder der mit ihrer Hilfe gewonnenen Ableitungen ergeben. Da grundsätzlich weder ein schützenswertes Individualinteresse noch ein Allgemeininteresse an der Verarbeitung falscher oder unvollständiger Daten besteht, sind die Hürden für einen derartigen Anspruch gering. In der Regel ist es ausreichend, dass

- die Verarbeitung der falschen oder unvollständigen Daten diesem Akteur (insbesondere einem Akteur, auf den sich die Informationen beziehen) Schaden zufügen kann; und
- die Korrektur unter Berücksichtigung von Schwere und Wahrscheinlichkeit des Schadens einerseits und dem für die Korrektur erforderlichen Aufwand andererseits nicht unverhältnismäßig ist.

<sup>4</sup> Siehe Erwägungsgrund 16 der Richtlinie (EU) 2019/1024 über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors (PSI-Richtlinie); Principles 1 und 3 der auf dem G8-Gipfel am 18. Juni 2013 unterzeichneten G8 Open Data Charter; Principle 1 der im September 2015 auf dem Gipfel der Open Government Partnership unterzeichneten International Open Data Charter.

### Beispiel 8

*Die bei dem Hersteller in Beispiel 5 gespeicherten Daten betreffend die Motoren des Zulieferunternehmens stellen sich als grob fehlerhaft heraus. Dies ist für das Zulieferunternehmen nicht nur deswegen misslich, weil das Zulieferunternehmen mit diesen Daten seiner Aufgabe der Qualitätssicherung nur unvollkommen nachkommen kann, sondern auch deswegen, weil die Motorendaten mit den Motorendaten anderer Motorenhersteller gepoolt und ausgewertet werden und schlechte Leistungswerte der Motoren des betroffenen Zulieferunternehmens dessen Chancen, Aufträge anderer Hersteller zu erlangen, schmälern dürften. Hier kann die Verarbeitung falscher Daten dem Zulieferunternehmen Schaden zufügen, und Anhaltspunkte für eine Unverhältnismäßigkeit des Aufwands sind nicht gegeben.*

Wenn der Aufwand für die Korrektur zu groß, der mögliche Schaden aber schwerwiegender ist, ist regelmäßig ein Unterlassungsanspruch gegeben (→ oben ).

#### 2.2.4 Szenarien wirtschaftlicher Teilhabe

Situationen, in denen ein Akteur Daten nutzt, zu deren Generierung andere Akteure beigetragen haben, und in denen der Daten nutzende Akteur mit Hilfe der Daten Wertschöpfung betreibt, sind alltäglich und grundsätzlich auch erwünscht. Sofern nach den genannten Kriterien (→ oben ) kein Unterlassungsanspruch besteht, ist dies von den Akteuren, die zur Generierung der Daten beigetragen haben, hinzunehmen. Der **gemeinwohlbezogene Charakter der hier vertretenen Datenrechte und Datenpflichten** steht einem generellen Anspruch auf Vergütung solcher Akteure normalerweise entgegen. Vielmehr müssen sich solche Akteure mit kollektiven Teilhabemöglichkeiten – insbesondere über die Besteuerung von Wertschöpfung – zufrieden geben.

Soweit ein Vergütungsanspruch nicht aus einem wirksamen Vertrag folgt, kommt individuelle Vergütung allenfalls als Ausgleichsmaßnahme im Einzelfall in Betracht, etwa soweit die entschädigungslose Ausübung eines Datenrechts konkret unverhältnismäßig erschiene (→ vgl. oben 2.1, Faktor c). Nur ganz **ausnahmsweise** kann nach Auffassung der DEK einem Akteur, der zur Generierung von Daten beigetragen hat, auch ohne entsprechenden Vertrag aus ethischer Sicht eine **eigenständige Vergütung** für die Datennutzung durch andere zustehen. Dies sollte aber nur der Fall sein, wenn

- a) der Beitrag des Akteurs zur Datengenerierung einen besonderen **Aufwand** erfordert hat oder **besonders einzigartig** ist und aus wirtschaftlicher Perspektive nur schwer durch Beiträge anderer Akteure ersetzbar wäre; und
- b) mit Hilfe der Daten eine ganz außergewöhnlich **hohe Wertschöpfung** betrieben wird; und
- c) es dem Akteur aufgrund der Umstände, unter denen der Beitrag zur Datengenerierung geleistet wurde, **nicht möglich oder nicht zumutbar** war, über eine **Vergütung** zu verhandeln.

Die Höhe einer solchen, nur ganz ausnahmsweise geschuldeten Vergütung muss angemessen sein und darf insbesondere nicht den prinzipiellen Anreiz, mit Hilfe von Daten Wertschöpfung zu betreiben, gefährden. Sie muss auch berücksichtigen, dass der die Wertschöpfung betreibende Akteur in der Regel wirtschaftliche Risiken eingegangen ist.



## 2.3 Kollektive Aspekte von Datenrechten und Datenpflichten

Zu klären ist, ob und gegebenenfalls inwieweit die Überlegungen zu Unterlassung, Zugang, Korrektur und wirtschaftlicher Teilhabe auch auf **Kollektive** im Sinne definierter Gruppen von Personen (z.B. indigene Völker im Fall der Verwendung ihrer genetischen Daten) übertragbar sind, d.h. ob auch Kollektiven im Zusammenhang mit der Nutzung „ihrer“ Daten bestimmte Datenrechte zustehen können. So könnte beispielsweise erwogen werden, ob der Bevölkerung eines Staates oder der EU für die Nutzung von Daten, die von dieser Bevölkerung generiert wurden, aus ethischer Sicht ein Recht auf wirtschaftliche Teilhabe (etwa in der Form von Steuern oder Transferleistungen) zustehen kann. Nach Auffassung der DEK kann dies prinzipiell der Fall sein.

### Beispiel 9

*Ein Internetkonzern verdient Milliardensummen durch Nutzerdaten, die weltweit bei der Nutzung der Dienste des Konzerns anfallen. Obgleich jährlich auch ein Milliardengewinn mit Daten von Nutzern aus der EU erwirtschaftet wird, zahlt der Konzern in der EU so gut wie keine Steuern. Hier stellt sich die Frage, ob den Konzern aus ethischen Gründen eine Pflicht treffen sollte, die Allgemeinheit in der EU wirtschaftlich in der Form von Steuern an der Wertschöpfung teilhaben zu lassen. Dies berührt grundlegende Fragen der Verteilungs- und der Teilhabegerechtigkeit und damit einer gerechten Wirtschaftsordnung. Es können aber etwa auch Aspekte wie Marktmacht oder die besondere Einzigartigkeit von Beiträgen (z.B. Audiodaten in einer bestimmten Sprache zur Entwicklung neuer sprachgesteuerter Dienste) in die Beurteilung mit einfließen.*

Die Berücksichtigung von Gruppen und Kollektiven ist aufgrund des **relationalen Charakters vieler Daten** allgemein wichtig. Dieser relationale Charakter kommt beispielsweise zum Vorschein, wenn zahlreiche digitale Dienste von Nutzern verlangen, Daten ihrer Kontakte oder „Freunde“ preiszugeben. Dies wird bei den hier vertretenen Datenrechten und korrespondierenden Datenpflichten insofern

mitberücksichtigt, als den „Freunden“ sowohl eigene Rechte auf Unterlassung, Zugang usw. zustehen können als auch jedenfalls ihre Interessen bei der Abwägung über ein geltend gemachtes Datenrecht stets mit einzubeziehen sind (→ oben 2.1). Darüber hinaus können bestimmte Daten, zu deren Generierung ein Akteur beigetragen hat, aber auch indirekt **Aufschluss über andere Akteure** geben, welche als solche individuell nicht – auch nicht im weitesten Sinne – zur Generierung dieser Daten beigetragen haben. Dieser Punkt ist bei genetischen Daten besonders evident, betrifft aber auch andere Datenarten. Damit eng verwandt ist die Situation, dass individuelle Daten, selbst in aggregierter Form, Einflüsse mit möglicherweise negativen **Drittewirkungen** jenseits des datenliefernden Individuums entfalten können.

### Beispiel 10

*Eine Krankenversicherung setzt Anreize zum Gesundheitstracking durch das Angebot reduzierter Prämien: Die Vorteile derer, die Daten preisgeben, können sich in höheren Beiträgen für jene, die Daten nicht preisgeben wollen, niederschlagen, d.h. der Vorteil des einen ist dann der Nachteil des anderen.*

Auch Fragen der **Repräsentativität** von Trainingsdaten für algorithmische Systeme können als Relationalitätsproblem gefasst werden: Die mangelnde Bezüglichkeit zwischen jenen, die Trainingsdaten geliefert haben, und jenen, auf die die trainierten Systeme angewendet werden, kann zu systematischen Verzerrungen und einer möglichen Diskriminierung führen (→ näher Teil F, 2.6).

Um dieser Herausforderung gerecht zu werden, müssen individualistische Ansätze von Datenrechten in Ethik, Recht und Technikgestaltung um **relationale Konzeptionen von Datenrechten** erweitert werden (vgl. auch die Diskussion um Group Privacy). Das bedeutet, dass ein Beitrag zur Generierung von Daten, der durch einen Angehörigen einer relevanten Gruppe geleistet wurde, unter Umständen auch anderen Angehörigen dieser Gruppe zuzurechnen ist, so dass diesen trotz Fehlens eines individuellen Beitrags zumindest aus ethischer Sicht eigene Rechte auf Unterlassung, Zugang usw. zustehen können.

### 3. Anforderungen an die Nutzung personenbezogener Daten

#### 3.1 Personenbezogene Daten und Daten juristischer Personen

Personenbezogene Daten sind alle Informationen, die sich auf eine **identifizierte oder identifizierbare natürliche Person** beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann (Art. 2 Nr. 1 DSGVO).

Wenngleich im Folgenden nur personenbezogene Daten im rechtlichen Sinn betrachtet werden, möchte die DEK daran erinnern, dass der **Schutzbedarf von Unternehmen und juristischen Personen** nicht ganz in den Hintergrund treten darf. Durch die Vernetzung aller Maschinen, den Austausch von Daten zwischen den Fabrikkomponenten und die Speicherung aller Produktionsdaten in digitalen Zwillingen in Industrie-4.0-Anlagen ist auch die Gefährdungslage für juristische Personen nochmals erhöht: So kann zum Beispiel aus der Verknüpfung von Einzeldaten (z.B. aus dem Wirkbetrieb von Geräten) ein praktisch lückenloses Bild interner Betriebsabläufe entstehen, das durch fehlende Schutzmechanismen in die Hände von betriebsfremden Akteuren (Konkurrenten, Verhandlungspartnern, Behörden, Übernahmeinteressenten usw.) gelangen kann. Dies stellt nach Auffassung der DEK eine ethisch bedenkliche Gefährdung der digitalen Selbstbestimmung von Unternehmen und juristischen Personen sowie auch – da zu einem großen Teil Datenflüsse zu Drittstaaten stattfinden – für die **digitale Souveränität Deutschlands und Europas** dar, der entgegenzuwirken ist.

Ein wichtiger juristischer Ansatzpunkt für den datenbezogenen Schutz von Unternehmen ist der **Schutz von Geschäftsgeheimnissen**, insbesondere durch das Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG). Bei dessen Auslegung und Anwendung muss sichergestellt werden, dass der Schutz sensibler Unternehmensdaten angesichts seiner zentralen Bedeutung für eine faire und wettbewerbliche Wirtschaftsordnung und das darauf fußende wirtschaftliche und gesellschaftliche Wohlergehen volumnäßig gewahrt bleibt. Allerdings ist die dem GeschGehG zugrundeliegende Richtlinie 2016/943 in verschiedener Hinsicht nicht ausreichend auf die Realität von IoT und Industrie 4.0 zugeschnitten. Die DEK fordert die Bundesregierung daher auf, den **datenbezogenen Schutz deutscher und europäischer Unternehmen zu verbessern**.

Die von der DEK im Folgenden für personenbezogene Daten unterbreiteten Handlungsempfehlungen – etwa in Bezug auf die risikoadäquate Auslegung des geltenden Rechtsrahmens ([→ unten](#)) oder auf datenschutzfreundliches Design von Produkten und Dienstleistungen ([→ unten](#)) – gelten dabei in sachgerechter Abwandlung bzw. Abschwächung auch für den Schutz von Daten, die sich auf Unternehmen und juristische Personen beziehen.

#### 3.2 Digitale Selbstbestimmung als Aufgabe für die gesamte Rechtsordnung

##### 3.2.1 Kooperatives Verhältnis zwischen den geltenden Rechtsregimen

Die Nutzung personenbezogener Daten in den verschiedensten Kontexten ist einerseits eine unverzichtbare Grundlage unserer Wirtschaft und Gesellschaft. Sie steht aber andererseits stets in einem Spannungsverhältnis zu individuellen Grundrechten. Beim Grundrecht auf informationelle Selbstbestimmung als Teil des allgemeinen Persönlichkeitsrechts handelt es sich im Kern um den Schutz der Menschenwürde. Das **Datenschutzrecht**, insbesondere die DSGVO, konkretisiert diese Maßstäbe und bindet öffentliche und private Stellen.



Die DSGVO stellt eine der großen Errungenschaften europäischer Rechtsetzung dar, welche derzeit weiteren Ländern als Inspirationsquelle dient. Allerdings dürfen die Erwartungen an diesen Rechtsakt nicht überspannt werden. Die DSGVO ist auf Datenschutz fokussiert, nicht aber auf die umfassende Wohlfahrt des Einzelnen und der Allgemeinheit in der Datengesellschaft. Sie ist auch für sich betrachtet nicht geeignet, alle Schäden, welche der Einzelne durch Verarbeitung seiner personenbezogenen Daten erleiden könnte, abzuwenden und in diesem Sinne umfassenden Integritätsschutz zu gewährleisten. Insbesondere soweit es um den Schutz von Rechtsgütern und Interessen geht, die **vom Datenschutzrecht nicht speziell adressiert** werden (z. B. Vermögensinteressen, Leben und körperliche Unversehrtheit, psychische Integrität, Ehre), bleibt die gesamte Rechtsordnung berufen. Dies gilt auch dann, wenn personenbezogene Daten im Spiel sind.

Die **datenschutzrechtliche Einwilligung** stellt einen zentralen Mechanismus zur Gewährleistung informationeller Selbstbestimmung im digitalen und analogen Bereich dar. Allerdings ist der Rechtsordnung ein inhaltlich schrankenloses Selbstbestimmungsrecht – einschließlich der Freiheit zur beliebigen Selbst- oder Fremdschädigung – nicht bekannt und auch ethisch nicht vertretbar. Eine freiwillige und informierte Einwilligung des Einzelnen als Ausdruck seiner grundrechtlich geschützten Handlungsfreiheit sollte zwar nur in eng begrenzten Ausnahmefällen von der Rechtsordnung eingeschränkt oder gar verboten werden. Ebenso wie beim Abschluss von Verträgen oder bei der Einwilligung in Eingriffe in die körperliche Unversehrtheit sind aber auch bei der datenschutzrechtlichen Einwilligung materielle Schranken anzuerkennen.

Nach Auffassung der DEK hat sich gezeigt, dass der Einzelne durch Anzahl und Komplexität der ihm abverlangten Entscheidungen bezüglich einer datenschutzrechtlichen Einwilligung ebenso wie durch die Unabschätzbarkeit aller Auswirkungen einer Datenverarbeitung **systematisch überfordert** wird. Die DEK sieht in einem unsachgemäßen Umgang mit dem Rechtsinstitut

der Einwilligung seitens der Anbieter digitaler Dienste eine von mehreren Ursachen eines **Vertrauensverlusts** in der digitalen Gesellschaft. So kann der Einzelne derzeit vielfach nicht mehr darauf vertrauen, dass Staat und Rechtsordnung Rahmenbedingungen schaffen, in denen er sich sicher und relativ sorglos bewegen kann, ohne die Zufügung massiver Schäden durch Dritte befürchten zu müssen. Ebenso wie im Vertragsrecht zwischen Unternehmen und Verbrauchern die Inhaltskontrolle Allgemeiner Geschäftsbedingungen eine Art der „rationalen Gleichgültigkeit“ ermöglicht und Verbraucher selbst bei Bagatelltransaktionen umfassend schützt, gilt es, den gleichen Zustand durch **Inhaltskontrolle von Einwilligungserklärungen** zu erreichen<sup>5</sup>. Bei dieser Inhaltskontrolle sind prinzipiell die Wertungen der gesamten Rechtsordnung zu berücksichtigen.

### 3.2.2 Risikoadäquate Auslegung des geltenden Rechtsrahmens

Die DEK weist nachdrücklich darauf hin, dass der geltende Rechtsrahmen infolge der neuartigen Gefährdungslagen durch die umfassende Sammlung, Nutzung und Auswertung von personenbezogenen Daten in einer Weise ausgelegt und angewendet werden muss, dass diesen Gefährdungslagen bereits durch das geltende Recht soweit als möglich Rechnung getragen werden kann.

Unabhängig von der Erfüllung datenschutzrechtlicher Anforderungen existieren eine Reihe **absoluter Grenzen**, die eine Datenverarbeitung nicht überschreiten darf. Datennutzungen jenseits dieser Grenzen gilt es nach Möglichkeit bereits durch grundrechtskonforme Auslegung und Anwendung des geltenden Rechts<sup>6</sup> zu unterbinden. Dies betrifft nach Auffassung der DEK beispielsweise:

<sup>5</sup> Vgl. auch Erwägungsgrund 42 zur DSGVO.

<sup>6</sup> Infrage kommen insbesondere die Kontrolle von Allgemeinen Geschäftsbedingungen (§§ 307 ff BGB), die Grundsätze über Sittenwidrigkeit (§ 138 BGB) und sittenwidrige vorsätzliche Schädigung (§ 826 BGB) sowie vertragliche und vertragsähnliche Schutz- und Treuepflichten (§ 241 Abs. 2 BGB).

- Mit den Grundrechten unvereinbare **Eingriffe in den Kern der Privatsphäre und die Integrität der Persönlichkeit** durch Profiling und/oder Scoring (etwa bestimmte Formen der Ermittlung von Persönlichkeitszügen, Emotionen oder zu erwartenden Verhaltensweisen);
- Das Bewirken einer mit der Menschenwürde unvereinbaren **Totalüberwachung**, auch im Wege einer „Überwachungs-Gesamtrechnung“ oder der Erstellung eines „Super-Scores“;
- **Sittenwidrige Ausnutzungen** besonderer Notlagen oder eines pathologischen Gesundheitszustands;
- Dem Demokratieprinzip zuwiderlaufende **Beeinflussungen politischer Wahlen**.

Ethisch verwerfliche Irreführung oder Manipulation im geschäftlichen Verkehr – wozu auch Geschäftspraktiken gehören sollten, die auf die Hergabe von personenbezogenen Daten abzielen – sind bereits nach geltendem Recht und unabhängig von einem datenschutzrechtlichen Rechtsbruch als **irreführendes oder aggressives Verhalten** nach dem Gesetz gegen den unlauteren Wettbewerb (UWG) einzustufen und lösen entsprechende Rechtsfolgen aus (z. B. Anfechtung wegen Täuschung oder Drohung; Unterlassung und Schadensersatz). Dazu können nach Auffassung der DEK etwa auch gehören:

- Sog. **Addictive Designs**, d.h. technologische Gestaltungen, die geeignet sind, die Verhaltensfreiheit des Nutzers in Bezug auf die Nutzung (und das Beenden der Nutzung) durch unzulässige Beeinflussung wesentlich zu beeinträchtigen, vor allem durch Mechanismen, die ein Suchtverhalten verursachen;
- Sog. **Dark Patterns**, d.h. technologische Gestaltungen primär von Benutzungsschnittstellen, die geeignet sind, einen Nutzer über bestimmte Punkte zu täuschen und/oder ihn manipulativ zu veranlassen, eine bestimmte – möglicherweise auch wirtschaftlich relevante – Entscheidung zu treffen.

Absolute Grenzen der Datenverarbeitung sind auch zum Schutz vor **unangemessener vermögensmäßiger Benachteiligung** gezogen. Diesem Schutz dienen verschiedene Mechanismen des geltenden Rechts<sup>7</sup>. Beispiele für missbräuchliche Vertragsbedingungen bzw. Verletzung von Schutz- und Treuepflichten wären nach Auffassung der DEK etwa:

- Verwehrung oder unangemessene Erschwerung des Zugangs zu Gerätedaten, die für die übliche **Nutzung** eines Geräts einschließlich Reparatur durch eine unabhängige Werkstatt erforderlich sind (z. B. Gewährung nur nach Maßgabe von Art. 12 DSGVO, z. B. nur innerhalb eines Monats bzw. sogar von drei Monaten);
- Verwehrung oder unangemessene Erschwerung eines betriebsnotwendigen Datenzugangs für den **Zweiterwerber** einer vernetzten Sache (z. B. bei Verkauf einer mit Smart-Home-Technologie ausgestatteten Immobilie);
- Erschwerung des Anbieterwechsels durch sog. **Lock-in** veredelter Daten (z. B. Verweigerung der Herausgabe von Datenanalysen, für die der Nutzer wirtschaftlich betrachtet bereits bezahlt hat, und die nicht dem Schutz von Betriebs- und Geschäftsgeheimnissen des Unternehmers unterliegen);
- Verarbeitung von Nutzerdaten durch den Produzenten oder ein anderes Glied der Lieferkette zu einem Zweck, der den **wirtschaftlichen Interessen** des Nutzers signifikant zuwiderläuft (z. B. zum Zweck der Preisdifferenzierung, wenn damit die Abschöpfung der maximalen individuellen Zahlungsbereitschaft intendiert wird).

<sup>7</sup> Vgl. die in Fn. 6 genannten Instrumente.



## Social Media Monitoring

Social Media Monitoring ist die systematische **Beobachtung** der Inhalte sozialer Medien zu einem bestimmten Thema. Es hat sich zu einem Instrument der Datenverwertung entwickelt und macht sich dabei den Umstand zunutze, dass soziale Netzwerke die Kommunikationsmöglichkeiten der Nutzer erweitern und das digitale Verhalten zugleich einer konstanten Beobachtung aussetzen.

Unternehmen bedienen sich der nutzergenerierten Daten Sozialer Netzwerke häufig, z. B. zu Zwecken der Marktforschung und des Marketings. Öffentliche Stellen machen von Social Media Monitoring bislang seltener Gebrauch, aber auch sie nutzen es – beispielsweise durchsucht die Finanzverwaltung mittels eines Webcrawlers öffentlich verfügbare Inhalte im Internet, um gezielt nach gewerblichen Verkäufern zu suchen, die keine Umsatzsteuer abführen.

Mittels Social Media Monitoring zusammengetragene Informationen können über algorithmische Systeme einer weiteren, eingriffsintensiveren **Nutzung und Verwertung** (insb. der Erstellung von Persönlichkeitsprofilen zu kommerziellen Zwecken) zugeführt werden. Dies erfolgt dann rechtmäßig, wenn die Interessensabwägung nach Art. 6 Abs. 1 lit. f DSGVO positiv ausfällt oder ein sonstiger Rechtfertigungsgrund vorliegt. Die Tatsache, dass der Betroffene die Daten selbst öffentlich gemacht hat, rechtfertigt ausreichlich Erwägungsgrund 51 DSGVO für sich allein eine weitere Nutzung und Verwertung noch nicht.

Die Grenze der Rechtmäßigkeit der Beobachtung ist nach Ansicht der DEK jedenfalls da erreicht, wo das Monitoring auf öffentliche Informationen erstreckt

wird, deren Reichweite die betroffene Person bei Öffentlichmachung nicht einschätzen konnte (z.B. unbedachte Äußerungen von Kindern insgesamt) oder deren Sensibilität zu hoch ist (z. B. Äußerungen über Suizidabsichten). Auch sollten Daten von Bewerbern selbst dann, wenn der Betroffene sie selbst öffentlich gemacht hat, bei der Einstellung nicht verwendet werden, wenn sie zu tief in die persönliche Integrität eingreifen oder wenn sie sich nicht ihrem klaren Schwerpunkt nach auf die berufliche Vergangenheit beziehen (z. B. Äußerungen zur sexuellen Orientierung). Das Gleiche gilt für eine sonstige systematische Auswertung von Daten aus dem Privatleben (z. B. Tracking Daten).

Gerade für die weitergehende, eingriffsintensivere Nutzung und Verwertung können sich im Rahmen der Interessenabwägung Grenzen der Zulässigkeit ergeben (z. B. zielgerichtete gewerbliche Ansprache auf Basis der sexuellen Ausrichtung oder Ausnutzung emotional labiler Situationen). Insbesondere Anbieter Sozialer Netzwerke sind technisch in der Lage, Kommunikationsvorgänge, die über zentrale Plattformen laufen, im Detail auszuwerten; selbst wenn die Inhalte durch eine Ende-zu-Ende-Verschlüsselung einem allgemeinen Zugriff entzogen sein mögen, sind ihnen weitgehende Analysen auf Basis von Metadaten möglich. Das Auswerten von Kommunikation zwischen Individuen oder in geschlossenen Gruppen sollte rechtlich auch privaten Anbietern in Anlehnung an das Fernmeldegeheimnis untersagt sein. Insoweit empfiehlt die DEK der Bundesregierung, darauf hinzuwirken, dass diese Verbote im Rahmen der anstehenden Verabschiedung der e-Privacy-Verordnung kurzfristig umgesetzt werden.

### 3.2.3 Bedarf nach Konkretisierung und Verschärfung des geltenden Rechtsrahmens

Ein den Vorgaben der Verfassung genügender Rechtsgüterschutz wird in vielen Fragen der digitalen Gesellschaft zurzeit allenfalls mittels Auslegung und rechtsfortbildender Konkretisierung von unbestimmten Rechtsbegriffen und Generalklauseln durch Aufsichtsbehörden und Gerichte im Einzelfall bewirkt. Diese Situation ist nach Auffassung der DEK unangemessen. Zwar haben unbestimmte Rechtsbegriffe und Generalklauseln den Vorteil der Flexibilität und Zukunftsoffenheit. Dennoch dauert ihre Konkretisierung für neue und insbesondere digitale Zusammenhänge durch die behördliche und gerichtliche Praxis häufig Jahre bis Jahrzehnte, so dass in der Zwischenzeit sowohl ein **strukturelles Vollzugsdefizit** des geltenden Rechts als auch ein **Mangel an**

**Rechtssicherheit** zu verzeichnen ist. Auf Grund der besonderen Grundrechtssensibilität und der Ungewissheit, ob und in welchem Zeitraum sich eine den verfassungsrechtlichen Anforderungen genügende Rechtspraxis entwickeln wird, sieht die DEK es als zentrale Aufgabe des demokratisch legitimierten Gesetzgebers an, den Ordnungsrahmen zeitnah verbindlich festzuschreiben.

Angesichts der Risiken, die für den Einzelnen in kritischen Bereichen durch **persönlichkeitssensible Profilbildungen** (sog. **Profiling**, ggf. mit der Folge von **Scoring**) erwachsen, hält die DEK insbesondere in diesen Bereichen eine Verschärfung des geltenden Rechtsrahmens für dringend geboten, um den Gefahren der Manipulation und der Diskriminierung des Einzelnen wirkungsvoll begegnen zu können.

## Profilbildung

„Profiling“ ist in **Art. 4 Nr. 4 DSGVO** als jede Art der automatisierten Verarbeitung personenbezogener Daten definiert, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen.

Profilbildungen stellen letztlich **Ableitungen** (Schlussfolgerungen) auf der Grundlage bestimmter Ausgangsdaten dar, die sich v. a. bestimmter Methoden des statistischen Schließens bedienen (→ Teil C, 2.2.2). Diese Ableitungen können wirkliche oder vermeintliche „Eigenschaften“ eines Einzelnen betreffen (z. B. „psychische Stabilität“, „Vertrauenswürdigkeit“, „Sozialverträglichkeit“) und/oder prognostischer Natur sein, wenn sie das künftige Verhalten eines Einzelnen zum Gegenstand haben (z. B. ein bestimmtes Konsumverhalten).

Neben der Profilbildung wird auch häufig versucht, aus dem beobachteten Verhalten eines Benutzers in der Interaktion mit digitalen Systemen diesen mit der Hilfe sog. Matching-Algorithmen einem vordefinierten **Stereotyp-Schema** zuzuordnen (z.B. bei Reisebuchung: Sportfan, Kulturreisender, Familienmensch, Wandergast, Vertreter, Gourmet). Mit dem für einen individuellen Benutzer instanzierten Stereotyp sind typische Vorlieben, Ziele und Persönlichkeitsmerkmale gespeichert, die dann in die weitere algorithmische Verarbeitung eingehen.

Es werden nicht immer die Profile als solche gespeichert, sondern es werden **ad-hoc-Ableitungen** (insbesondere Verhaltensvorhersagen) dynamisch und in Echtzeit (z. B. „ist jetzt kaufbereit für Schuhe“) aus Rohdaten generiert.



Profilbildungen schlechthin zu verbieten, schösse angesichts des Umstandes, dass der durch Profile ermöglichte Grad an Personalisierung zahlreicher digitaler Angebote von vielen Nutzerinnen und Nutzern als komfortabel und hilfreich empfunden wird, über das Ziel hinaus. Die DEK empfiehlt der Bundesregierung jedoch, sich beispielsweise im Rahmen der anstehenden Evaluierung der DSGVO dafür einzusetzen, die **DSGVO um spezifische Regelungen zu Profiling-Verfahren zu ergänzen**, die über die bereits bestehende Regelung des Art. 22 DSGVO zur Zulässigkeit automatisierter Entscheidungen hinausgehen, oder sich sogar für einen eigenen europäischen Rechtsakt einzusetzen, der den Gefahren durch Profilbildungen für die Grundrechte Einzelner effektiv begegnet. Falls sich eine hinreichend wirkungsvolle europäische Lösung in absehbarer Zeit als nicht realistisch erweisen sollte, sollte im Rahmen des europarechtlich Zulässigen eine nationale gesetzliche Regelung für den Umgang mit grundrechtsgefährdenden Profilbildungen angedacht werden.

In Bezug auf Profilbildungen sollten aus Sicht der DEK insbesondere folgende Aspekte eine (horizontale und/oder sektorale) gesetzliche Regelung erfahren, sofern sie von der DSGVO bei zutreffender Auslegung nicht ohnehin bereits vorgegeben sind:

- a) Normierung **absoluter Grenzen** in der Form von gesetzlichen Verboten bestimmter **kritischer Einsatzzwecke** (z. B. Verwendung von Profilen, die aus Daten aus dem Privatleben gewonnen wurden, bei der Bewerberauswahl) und von Profilbildungen bei **besonders sensiblen personenbezogenen Daten**, etwa in Zusammenhang mit Emotionerkennungssoftware und biometrischen Daten, und bei Datenverarbeitungen mit **unvertretbarem Risikopotenzial** für die betroffenen Personen oder für die Gesellschaft;
- b) Normierung von **Zulässigkeitsvoraussetzungen** für kritische Profilbildungen, einschließlich Qualitätsanforderungen hinsichtlich Aussagekraft und Treffsicherheit der gebildeten Profile (→ näher hierzu Teil F, 4.2.1), und einem risikoadäquaten System von Einwilligungslösungen (sog. Opt-in) und Widerspruchslösungen (sog. Opt-out), wobei letztere nur bei sehr geringem Risiko infrage kommen;
- c) Konkretisierung des **Verhältnismäßigkeitsgrundsatzes** u.a. bezüglich der Anforderungen an die Art und den Umfang der zur Profilbildung herangezogenen Daten, der zulässigen Tiefe der zu Zwecken einer Profilbildung erfolgenden Schlussfolgerungen, und vor allem der Zwecke, für die Profilbildungen zulässigerweise eingesetzt werden dürfen;
- d) Spezifische Kennzeichnungs-, **Informations-** und **Auskunftspflichten** bezüglich der Profilbildungen als solcher – und zwar einschließlich bezüglich der Existenz und des Zweckes von algorithmischen Systemen, die für **ad-hoc-Ableitungen** geeignet sind, sowie der bereits erfolgten, kritischen Ableitungen –, nicht erst der im Anschluss erfolgenden automatisierten Entscheidung;
- e) Praktikable **Einwirkungsmöglichkeiten** einer betroffenen Person auf die über sie gebildeten Profile einschließlich der Möglichkeit zur Löschung/Korrektur/Überprüfung; dazu gehört auch das Recht auf einen „digitalen Neuanfang“ durch Löschung der gebildeten Profile, z. B. mit Erreichen der Volljährigkeit, wie es eine EU-Expertengruppe jüngst vorgeschlagen hat.<sup>8</sup>

<sup>8</sup> High-Level Expert Group on Artificial Intelligence: Policy and Investment Recommendations for Trustworthy AI, 26.06.2019, S. 14, 40 (abrufbar unter: [https://ec.europa.eu/newsroom/dae/document.cfm?doc\\_id=60343](https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60343)).

## Sprachassistenten

Sprachassistenten bieten große Chancen im Hinblick auf Komfort und – insbesondere für Menschen mit Einschränkungen – den erleichterten Zugang zu digitalen Techniken. Sie bergen aber auch Gefahren für die Selbstbestimmung der Betroffenen.

Sprachassistenten erheben, oftmals auch ohne explizite Aktivierung, ihre Umgebungsgeräusche. Die dabei erhobenen Sprachaufnahmen der Nutzer sowie Dritter sind **biometrische Daten** im Sinne der DSGVO. Neben der Echtzeitanalyse der Sprachaufnahmen zur Reaktion auf die eingesprochene Aufforderung findet regelmäßig eine automatische Protokollierung gewisser Daten in einer Log-Datei statt (sog. Logging). Die analysierte personenspezifische Stimmfärbung sowie das Sprachmuster lassen sich verwenden, um die jeweilige Person **eindeutig zu identifizieren** oder **Sprachemotionen** zu analysieren. Ein solches Profiling greift besonders tief und invasiv in den Kernbereich der Persönlichkeitsrechte ein und droht die strukturelle Ungleichheit zwischen Angebots- und Nachfrageseite im Markt weiter zu vergrößern. Die Möglichkeit, das gesprochene Wort neu zu kombinieren bzw. digital nachzuformen (sog. deep fakes), eröffnet weiteres hohes **Missbrauchspotenzial**.

Faktisch verschwimmt für den individuellen Nutzer neben der Kenntnis des „Wie“ das Wissen um das „Ob“ der Datenverarbeitung. Die Verwendung einer authentisch **menschlich klingenden Stimme** kann, insbesondere bei technisch unerfahrenen Menschen, zudem zu einer weitergehenden Preisgabe persönlichkeitssensibler Daten führen. Überdies zeichnen Sprachassistenten oftmals nicht nur lokal auf, sondern vernetzen sich über einen virtuellen Assistenten als Schaltzentrale und Herzstück moderner Wohnräume, vermehrt mit anderen Smart-Home-Produkten.

Die DEK sieht die umfassende Profilbildungsgefahr, die im Zusammenhang mit Sprachassistenten von der Zusammenführung verschiedenster Soft- und Hardwarekomponenten ausgeht, kritisch. Zudem können die Einfachheit, der Komfort sowie augenscheinliche Vorteile der Verknüpfung mit weiteren Geräten den Nutzer letztlich in eine „Plug & Play-Falle“ tappen lassen. Geeignete Maßnahmen zur Reduzierung der Risiken, die von Sprachassistenten ausgehen, wären neben den Verboten besonders kritischer Profilbildungen und Einsatzzwecke nach Auffassung der DEK etwa:

- a) Bindende technische Vorgaben zur Implementierung von Datenschutz „by design“ und „by default“ (→ siehe auch unten ), insbesondere grundsätzlich **rein lokale Verarbeitung von Sprachdateien** (und Löschbarkeit) und Beschränkung einer Datenweiterleitung an den Betreiber oder Dritte auf bereits in Maschinensprache übersetzte Befehle (z. B. eine Bestellung);
- b) Bindende technische Vorgaben zur **Abschaltbarkeit** von Mikrofon und Internetverbindung sowie **Sichtbarmachung**, ob das Mikrofon an- oder ausgeschaltet ist (→ siehe ebenfalls unten );
- c) Dem Medium angemessene Ausgestaltung von **Transparenzpflichten** (→ siehe Teil F, 4.1), indem die wichtigsten Offenlegungen in der jeweiligen Situation oder in regelmäßigen Abständen auch **akustisch** erfolgen.



Jenseits derartiger spezialgesetzlicher Schutzmaßnahmen sollte die Bundesregierung prüfen, inwieweit losgelöst von den Zielen des Datenschutzrechts – und damit außerhalb des Anwendungsbereichs der DSGVO – vorrangig auf europäischer, sonst auf nationaler Ebene auf weitere Regelungen hingewirkt werden sollte, um den notwendigen Ordnungsrahmen für einen angemessenen Umgang mit Daten zu schaffen bzw. abzurunden. Im Zuge dessen empfiehlt die DEK insbesondere (→ zu Beispielen jeweils oben):

- a) Ausdrückliche gesetzliche Normierung von datenspezifischen **Klauselverboten für die AGB-Kontrolle** (§§ 308, 309 BGB) und datenspezifischen **Schutz- und Treuepflichten** (§ 241 Abs. 2 BGB);
- b) Ausdrückliche gesetzliche Normierung datenspezifischer **Deliktstatbestände** in Konkretisierung des Tatbestands sittenwidriger vorsätzlicher Schädigung (etwa in Gestalt eines neuen § 826a BGB);
- c) Ausdrückliche gesetzliche Normierung datenspezifischer irreführender und aggressiver **Geschäftspraktiken**, wie z.B. Addictive Designs und Dark Patterns, durch Erweiterung der „Black List“ des UWG; wegen der vollharmonisierenden Wirkung der europäischen Richtlinie über unlautere Geschäftspraktiken müsste diese Änderung allerdings zunächst auf europäischer Ebene ansetzen.

Erfolgt die Profilbildung durch **staatliche Stellen**, sind mögliche Effekte im Sinne eines kumulativen Grundrechtseingriffs bzw. einer Überwachungsgesamtrechnung ebenso zu berücksichtigen wie mögliche Nebenfolgen oder „Kollateralschäden“. Besonderes Missbrauchspotenzial sieht die DEK in der Vernetzung einzelner Teilsysteme, wodurch Daten und Analyseerkenntnisse aus ganz unterschiedlichen Sach- und Lebensbereichen zusammengeführt werden. Dies führt zu einer erheblichen Verdichtung der Überwachung. Die Verknüpfung personenbezogener Informationen über verschiedene Überwachungssysteme hinweg und die Zusammenführung von Profilen wird dabei durch Techniken der intelligenten Mustererkennung (insbes. der Gesichtserkennung) erleichtert. Vor diesem Hintergrund empfiehlt die DEK zum einen, entsprechende Mustererkennung nur dort zu nutzen, wo dies für die Erfüllung staatlicher Aufgaben **unbedingt erforderlich** ist und zudem – über das nachrichtendienstliche Trennungsgebot hinaus – **klare gesetzliche Grenzen für den Austausch von Informationen** und Mustern zwischen den Behörden zu definieren. Dies kann auch die Neuregelung von Verwendungs- und Verwertungsverboten umfassen, insbesondere für den Austausch zwischen präventiv und repressiv tätigen staatlichen Stellen.

### 3.2.4 Bedarf nach einer Vereinheitlichung der Datenschutzaufsicht für den Markt

Die Datenschutzaufsicht über die Wirtschaft ist in Deutschland zwischen Bundes- und Landesbehörden verteilt. In Einzelfragen lassen sich Abweichungen in Aussagen zu datenschutzrechtlichen Anforderungen und eine divergierende Vollzugspraxis beobachten, die die betroffenen Akteure vor Herausforderungen stellt. Während im System der europäischen Mitgliedstaaten der Europäische Datenschutzausschuss (EDPB) als Institution für eine einheitliche Anwendung der DSGVO eingeführt wurde und im Einzelfall auch über Weisungsbefugnisse verfügt, erreicht das föderale Miteinander der Datenschutzbehörden der Bundesländer in Deutschland **bisher keine ähnliche Verbindlichkeit und Einheitlichkeit.**

Sofern sich die Abstimmung unter den deutschen Datenschutzaufsichtsbehörden nicht verstärken und formalisieren lässt und so die einheitliche und kohärente Anwendung des Datenschutzrechts gewährleistet werden kann, ist zu überlegen, die Datenschutzaufsicht im Markt durch **eine neue Behördenstruktur** zu vereinheitlichen. Eine solche Vereinheitlichung erlaubt den Aufbau spezialisierter Expertise, der für die Durchsetzung des Datenschutzrechts in einem technisch hochdynamischen Umfeld erforderlich ist. Dabei müsste gewährleistet sein, dass die einheitliche Behörde entweder selbst oder durch intensive Kooperation mit anderen Behörden auch die Durchsetzung **sonstiger datenrelevanter Rechtsmaterien**, die in engem funktionellem Zusammenhang mit dem Datenschutzrecht stehen (z.B. das Zivil- oder Lauterkeitsrecht), gewährleistet. Die Konzentration von Kompetenz für die Datenschutzaufsicht über den Markt in einer Stelle könnte ferner die Stimme Deutschlands im Europäischen Datenschutzausschuss – in dem alle Mitgliedstaaten bereits jetzt durch eine Datenschutzaufsichtsbehörde mit nationaler Zuständigkeit vertreten sind – weiter stärken. Schließlich sollte eine Zentralisierung der Behördenkompetenz mit der Konzentration der gerichtlichen Kontrolle der datenschutzaufsichtlichen Maßnahmen im Markt bei einem Gericht einhergehen, damit dieses gleichfalls eine entsprechende Expertise und eine kohärente Rechtsprechung entwickeln kann.

Organisationsrechtlich sind **verschiedene Modelle** denkbar. Im Zuge seiner Zuständigkeit zur Regelung des Rechts der Wirtschaft könnte der Bund die Kompetenz der Datenschutzaufsicht über die Wirtschaft (nicht-öffentlicher Bereich) auf den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit übertragen und diesen entsprechend ausstatten. Dieser könnte durch verschiedene Außenstellen eine Präsenz der Datenschutzaufsicht in der Fläche garantieren (ähnlich dem Bundesamt für Migration und Flüchtlinge oder der Bundesbank). Denkbar ist auch die Bildung einer gemeinsamen Einrichtung der Länder qua Staatsvertrag nach den Modellen etwa im Rundfunkbereich oder der gemeinsamen Zentralstellen der Länder für Sicherheitstechnik und Gesundheitsschutz. Hier müsste die Unabhängigkeit der Datenschutzaufsicht durch die gemeinsame Einrichtung im Staatsvertrag gesichert werden. In jedem Fall ist – um eine angemessene Schlagkraft zu gewährleisten – auf eine bessere **personelle und sachliche Ausstattung** der Behörden zu achten.

Die Zuständigkeit der **Landesdatenschutzbehörden für den öffentlichen Bereich** sollte schon aus verfassungsrechtlichen Gründen in jedem Fall unangetastet bleiben.



### 3.3 Personenbezogene Daten als Vermögensgut

#### 3.3.1 Ökonomisierung personenbezogener Daten

Personenbezogenen Daten kommt eine enorme wirtschaftliche Bedeutung zu. Der grundrechtliche Schutz der Persönlichkeit umfasst anerkanntermaßen auch die Entscheidung des Einzelnen, manche **Aspekte seiner Persönlichkeit gegen Entgelt zur Verfügung zu stellen** (z.B. Recht am eigenen Bild) und damit zu vermarkten.<sup>9</sup> Ebenso wie aber dem Einzelnen eine Vermarktung seiner Daten nicht vollkommen verwehrt ist, ist es auch nicht vollkommen ausgeschlossen, dass personenbezogene Daten auf Initiative Dritter hin wirtschaftlich verwertet werden. Der in diesem Zusammenhang teilweise bemühte Vergleich mit dem Handel menschlicher Organe hinkt in mehrfacher Hinsicht, u.a. weil Daten – anders als menschliche Organe – ein nicht-rivales Gut sind und die Tatsache, dass ein Anderer personenbezogene Daten verarbeitet, für sich betrachtet der betroffenen Person noch nicht unbedingt schadet; der Schaden wird erst durch einen bestimmten Kontext oder Zweck der Datenverarbeitung bewirkt.

Mit der Herleitung des informationellen Selbstbestimmungsrechts aus der Menschenwürde wird allerdings deutlich, dass der wirtschaftlichen Verwertung personenbezogener Daten dort **Grenzen** gezogen sind, wo auch ganz allgemein die Grenzen der Verarbeitung personenbezogener Daten verlaufen (→ oben 3.2.1 und ), einschließlich der materiellen Grenzen der Einwilligung. Die wirtschaftliche Verwertung personenbezogener Daten ist in diesem Zusammenhang weder generell strenger Regeln unterworfen noch generell privilegiert. Bei der Anwendung der allgemein geltenden Regeln müssen wirtschaftliche Aspekte allerdings in vielen Zusammenhängen berücksichtigt werden (z.B. hat wirtschaftlicher Druck Bedeutung für die Freiwilligkeit einer Einwilligung).

#### 3.3.2 Daten als Eigentum und die Frage eines finanziellen Ausgleichs

Die DEK sieht derzeit **keine hinreichenden Gründe**, zusätzliche eigentumsähnliche Verwertungsrechte einzuführen, welche eine wirtschaftliche Partizipation an mithilfe von Daten generierten Gewinnen ermöglichen würden (oft unter dem Stichwort „**Dateneigentum**“ oder „Datenerzeugerrecht“ diskutiert).<sup>10</sup> Dem Einzelnen stehen bereits jetzt aufgrund des Datenschutzrechts oder des allgemeinen Zivilrechts genügend Rechtspositionen mit Drittewirkung zu, deren Einschränkung er theoretisch nur gegen Zahlung eines entsprechenden Entgelts dulden müsste. Wenn ihm die Aushandlung eines solchen Entgelts nicht gelingt, liegt das an Umständen (z.B. fehlende Verhandlungsmacht und/oder schlecht funktionierender Wettbewerb), die nichts mit dem Fehlen eines weiteren eigentumsähnlichen Verwertungsrechts zu tun haben.

Die Asymmetrie der Verhandlungsposition ließe sich allerdings theoretisch durch die Einführung von **Verwertungsgesellschaften**, die eigentumsähnliche Verwertungsrechte an Daten kollektiv wahrnehmen, ändern. Eine eigentumsähnliche wirtschaftliche Komponente personenbezogener Daten stünde allerdings in einem potenziellen **Spannungsverhältnis zum Datenschutz**, insbesondere zur Freiwilligkeit und jederzeitigen Widerruflichkeit der Einwilligung und zum Löschungsanspruch. Zudem würden **zweifelhafte finanzielle Anreize** zur Produktion möglichst vieler personenbezogener Daten geschaffen und würden gerade besonders vulnerable Personen (z.B. Minderjährige, einkommensschwache Bevölkerungsgruppen) zur Preisgabe möglichst vieler Daten animiert. Eine eventuelle Einpreisung der Vergütungen durch die Industrie könnte zudem zu einer verhältnismäßigen **Mehrbelastung datenschutzbewusster Personen** führen.

9 Siehe z.B. § 22 Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie (KunstUrhG).

10 Siehe anstelle vieler: Europäische Kommission: Aufbau einer europäischen Datenwirtschaft, 10.01.2017, COM(2017) 9 final (abrufbar unter: <https://ec.europa.eu/transparency/regdoc/rep/1/2017/DE/COM-2017-9-F1-DE-MAIN-PART-1.PDF>);

Arbeitsgruppe „Digitaler Neustart“ der Konferenz der Justizministerinnen und Justizminister der Länder: Bericht vom 15. Mai 2017, S. 29 ff (abrufbar unter: [https://www.justiz.nrw.de/JM/schwerpunkte/digitaler\\_neustart/zt\\_bericht\\_arbeitsgruppe/bericht\\_ag\\_dig\\_neustart.pdf](https://www.justiz.nrw.de/JM/schwerpunkte/digitaler_neustart/zt_bericht_arbeitsgruppe/bericht_ag_dig_neustart.pdf)).

Die genannten Argumente verfangen zwar nicht in gleichem Maße in Bezug auf anonymisierte Daten. Angesichts der Vielzahl von Akteuren, die einen Beitrag zur Generierung und Veredelung von Daten leisten, würde ein faires Vergütungssystem allerdings ein Maß an **Komplexität** erreichen und ein Ausmaß an Allzeitüberwachung zwecks Messung von Datenflüssen erfordern, das außer Verhältnis zu jedem möglichen Gerechtigkeitsgewinn stünde. Hinzu kämen mögliche negative Konsequenzen für die **Datenqualität**, da Anreize geschaffen würden, z. B. durch Anlegen falscher Geräteprofile „künstlich“ Daten zu produzieren, die ein verzerrtes Bild der Realität liefern. Die DEK empfiehlt daher **auch bezüglich anonymisierter Daten keine Einführung von Verwertungsrechten**, die als Ausschließlichkeitsrechte ausgestaltet sind.

### 3.3.3 Daten als „Gegenleistung“

Eine Vielzahl digitaler Inhalte und Dienstleistungen (z.B. Suchmaschinen, soziale Netzwerke, Messenger-Dienste, Online-Spiele) werden Endnutzern ohne monetäre Gegenleistung angeboten. Die Finanzierung erfolgt auf andere Weise, insbesondere durch Leistungen Dritter für personalisierte Werbung und sonstige personalisierte Informationsangebote an die Nutzer sowie für deren Nutzerprofile und Nutzerscores. Dies hat zur plakativen Bezeichnung personenbezogener Daten als „Gegenleistung“ für den digitalen Inhalt oder die Dienstleistung geführt, so etwa im ursprünglichen – im Gesetzgebungsverfahren jedoch wieder geänderten – Entwurf von Art. 3 Nr. 1 der Richtlinie über digitale Inhalte.<sup>11</sup> Inwie weit das beschriebene wirtschaftliche Modell überhaupt mit dem **Koppelungsverbot** aus Art. 7 Abs. 4 DSGVO vereinbar ist,<sup>12</sup> wird letztlich durch den EuGH zu klären sein.

Wenngleich die plakative Bezeichnung zur allgemeinen Bewusstseinsbildung beigetragen hat, plädiert die DEK dafür, **von der Bezeichnung von Daten als „Gegenleistung“ abzusehen**. Zum einen sind personenbezogene Daten Teil der Persönlichkeit und genießen verfassungsrechtlichen Schutz. Zum anderen könnte die Einordnung als Gegenleistung nicht intendierte Implikationen nach sich ziehen. So könnte sie etwa als Argument dafür dienen, datenbezogene Allgemeine Geschäftsbedingungen nicht mehr in vollem Umfang der Inhaltskontrolle zu unterwerfen, oder dafür, dass ein Widerruf der Einwilligung, Löschungsverlangen usw. vertragliche Sanktionen gegen den Verbraucher auszulösen vermag.

In diesem Zusammenhang sollte der deutsche Gesetzgeber Freiräume bei der Umsetzung der Richtlinie (EU) 2019/770 über digitale Inhalte und digitale Dienstleistungen nicht in einer Weise nutzen, welche den Einzelnen von der Geltendmachung seiner datenschutzrechtlichen Rechtspositionen abhalten könnte. Insbesondere sollte der Anbieter im Fall des Widerrufs der Einwilligung zur Datenverwendung seine Leistung zwar mit sofortiger Wirkung einstellen dürfen, doch sollten **Zahlungsansprüche wegen einer bereits erbrachten Leistung ausgeschlossen** sein, ebenso wie ein nachträgliches **automatisches Zurückfallen in ein Bezahlmodell**.

Als Ausweg aus dem Koppelungsverbot werden verstärkt **Bezahlmodelle** diskutiert. Allerdings stellt jede noch so geringfügige finanzielle Belastung – insbesondere für vulnerable Bevölkerungsgruppen – einen Nachteil dar, der die Betroffenen abschrecken und zur übermäßigen Preissgabe ihrer personenbezogenen Daten bewegen kann. Auch ist eine überdurchschnittlich starke finanzielle Belastung besonders datenschutzbewusster Personen zu befürchten. Daher sollte vorrangig angestrebt werden, die **Finanzierung durch gewerbliche Nutzer**, die bislang unentgeltlich Gebrauch von bestimmten digitalen Inhalten oder Dienstleistungen machen, zu erreichen (z.B. die Seite eines Unternehmens bei einem sozialen Netzwerk).

<sup>11</sup> Europäische Kommission: Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte, 9.12.2015, COM(2015) 634 final (abrufbar unter: <https://ec.europa.eu/transparency/regdoc/rep/1/2015/DE/1-2015-634-DE-F1-1.PDF>).

<sup>12</sup> Europäischer Datenschutzbeauftragter: Stellungnahme 4/2017 zu dem Vorschlag für eine Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte, 14. März 2017, S. 19 (abrufbar unter: [https://edps.europa.eu/sites/edp/files/publication/17-03-14\\_opinion\\_digital\\_content\\_de.pdf](https://edps.europa.eu/sites/edp/files/publication/17-03-14_opinion_digital_content_de.pdf)).

Bezahlmodelle können allerdings auch das Bewusstsein von Verbrauchern für den monetären Wert der eigenen Daten stärken und Transparenz schaffen. Aus diesen Gründen kann nach Auffassung der DEK das **alternative Angebot eines Bezahlmodells** einen ethisch akzeptablen Ausgleich zur Herstellung der notwendigen Freiwilligkeit darstellen. Dabei ist jedoch zu beachten, dass der Preis nicht missbräuchlich und marktunüblich hoch sein darf, sondern eine auch aus Verbrauchersicht realistische Alternative zur Preisgabe personenbezogener Daten darstellen muss. Ferner ist aus ethischer Sicht sicherzustellen, dass es nicht zu einer Quersubventionierung durch datenschutzbewusste Nutzer kommt und dass die Bedürfnisse sozial schwacher Bevölkerungsgruppen etwa durch entsprechende staatliche Transferleistungen berücksichtigt werden.

### 3.3.4 Daten als Grundlage personalisierter Risikoeinschätzung

Bei der **personalisierten Risikoeinschätzung** (z. B. einmalig bei der Kreditvergabe oder laufend bei Versicherungen mit Telematiktarifen) geht es um höhere Granularität von preisrelevanten Vorhersagen durch Nutzung algorithmischer Systeme. Es handelt sich hierbei letztlich um einen sektorspezifischen Anwendungsfall einer bestimmten Form von Profilbildung und eines darauf aufbauenden Scoring (→ zu Profilbildungen allgemein bereits oben 3.2.3 und unten Teil F, 4.2.2). Die Verarbeitung zusätzlicher personenbezogener Daten bedarf bei der personalisierten Risikoeinschätzung regelmäßig der Einwilligung der betroffenen Personen. Diese werden zunächst jene Personen erteilen, welche sich dadurch ökonomische Vorteile erhoffen. Dabei kann die Einwilligung einer Person signifikante Auswirkungen auf andere Personen haben und ethisch unerwünschte Kettenreaktionen (sog. Unraveling-Effekte) auslösen. Dies kann dazu führen, dass der in die Datenverarbeitung Einwilligende unter unverhältnismäßigem Druck steht und die Freiwilligkeit der Einwilligung gefährdet wird.

#### Beispiel 11

*Besonders gesunde Versicherte willigen in die Datenverarbeitung durch eine Krankenversicherung ein. Um nicht in den Verdacht zu geraten, zu den Versicherten mit schlechterer Gesundheit zu gehören, geraten andere unter Druck, ebenfalls einzuwilligen.*

Sofern die Parameter durch das Verhalten des Einzelnen beeinflussbar sind, können derartige Modelle zudem erheblichen **Einfluss auf die private Lebensgestaltung** entfalten. Gerade im Versicherungssektor kommt aus ethischer Sicht noch der Aspekt hinzu, dass das Streben nach immer höherer Granularität der Risikoeinschätzung dem **Grundprinzip der kollektiven Risikoübernahme** durch die Gemeinschaft aller Versicherten zuwiderläuft. Im Extremfall „vollständigen“ Wissens auf der Seite des Versicherers und entsprechender Anpassung des Preises an das individuelle Risiko hat sich der Gedanke einer Versicherung ad absurdum geführt.

Nach Ansicht der DEK stellen sich daher aus ethischer Sicht insbesondere folgende Anforderungen an eine personalisierte Risikoeinschätzung:

- a) Die Datenverarbeitung darf **nicht den Kern privater Lebensführung** betreffen, sondern nur Bereiche, in denen der Einzelne ohnehin in Kontakt mit der Außenwelt tritt und damit rechnen muss, dass man Schlüsse aus seinem Verhalten zieht. Ethisch akzeptabel wäre danach bei einer Kfz-Versicherung etwa die Registrierung der gefahrenen Kilometer oder von Verstößen gegen die StVO, nicht dagegen des rein privaten, wenn auch möglicherweise risikorelevanten Verhaltens im Fahrzeug (z. B. Frequenz des Gähnens, Gespräche mit Beifahrern) oder gar des Gesundheitszustands (z. B. Herzschwäche) oder der sonstigen Lebensführung (z. B. Einkaufsverhalten betreffend Kaffee oder Alkohol);
- b) Zwischen den verarbeiteten Daten und dem zu bestimmenden Risiko muss ein **klarer ursächlicher Zusammenhang** bestehen, und die Verknüpfung darf keine **Diskriminierung** darstellen (→ siehe dazu unten Teil F, 2.6);

- c) Es darf sich nicht um Daten handeln, die unmittelbar Schlussfolgerungen mit **Wirkung für Angehörige oder sonstige Dritte** zulassen;
- d) Es muss umfassende **Transparenz** bezüglich der Auswirkungen, die bestimmte Parameter und deren Gewichtung auf die Gestaltung des Preises oder der sonstigen Konditionen haben, gegeben sein, und der Einzelne muss klare und verständliche Erläuterungen erhalten, wie er die Konditionen verbessern kann  
(→ siehe dazu Teil F, 2.7);
- e) Um unerwünschte Kettenreaktionen in Grenzen zu halten, darf die Differenz zwischen den „optimalen“ Konditionen und den bei Verweigerung der Einwilligung zu erreichenden Konditionen ein Höchstmaß nicht überschreiten (z.B. **maximale Preisdifferenz**).

### 3.3.5 Daten als Reputationskapital

Personenbezogene Daten, Profile und Scores erhalten im Zusammenhang mit **personalisierten wirtschaftlichen Konditionen** (personalisierte Preise, personalisiertes Ranking, personalisierte Produkte und Dienstleistungen) eine Funktion als Reputationskapital. Bei der personalisierten Verhaltensprämierung zu Zwecken der **Kundenbindung** (z.B. durch Rabatte in Abhängigkeit von der Einkaufsmenge des Vormonats) werden zwar Anreize zur Einwilligung in die Verarbeitung personenbezogener Daten geschaffen und besteht eine Tendenz, die private Lebensführung zu beeinflussen. Der DEK liegen jedoch keine Hinweise vor, dass in Zusammenhang mit Kundenbindungsprogrammen die soeben (→ oben) dargestellten ethischen Grenzen in der deutschen Wirtschaft derzeit überschritten werden. Die Entwicklung sollte jedoch weiter beobachtet werden.

Bei der **klassischen Preisdifferenzierung** und Maßnahmen ähnlicher Wirkung sieht die DEK den Schwerpunkt der Problematik im Bereich der Regulierung algorithmischer Systeme (→ dazu im Detail Teil F). Zu einem Problem der Datennutzung wird Preisdifferenzierung allerdings dann, wenn Verbrauchern suggeriert wird, die Preise generell durch Preisgabe möglichst vieler personenbezogener Daten oder durch bestimmte, an die relevanten Kriterien angepasste Verhaltensweisen (etwa Online-Einkauf über einen Computer einer bestimmten Marke) senken zu können bzw. wenn Verbraucher, die die Einwilligung in die zur personalisierten Preissetzung erforderliche Datenverarbeitung verweigern, im **Durchschnitt stets höhere Preise** zahlen. Letzteres wäre nach Ansicht der DEK nicht zuletzt ein ethisch bedenklicher Angriff auf die Freiwilligkeit der Einwilligung.

Darüber hinaus erlangen **echte Reputationsdaten**, die auch für außenstehende Dritte sichtbar sind (z.B. durch „Sterne“ indizierte Zuverlässigkeit als Vertragspartner im Rahmen einer Online-Plattform), immer größere wirtschaftliche und immaterielle Bedeutung. Derartige echte Reputationsdaten werden teilweise durch die neue **Verordnung (EU) 2019/1150 zur Fairness und Transparenz** für gewerbliche Nutzer von Online-Vermittlungsdiensten erfasst.<sup>13</sup> Dabei wurde ein behutsamer und weitgehend auf Transparenzanforderungen und Selbstregulierung aufbauender Regelungsansatz gewählt. Die DEK begrüßt im Grundsatz diesen behutsamen Ansatz. Sie weist jedoch darauf hin, dass insbesondere die Abhängigkeit einzelner Branchen von echten Reputationsdaten zu starken Lock-in-Effekten führen kann, die den Wettbewerb gefährden und problematisch sind, falls die Daten bei einem Wechsel des Online-Vermittlungsdienstes nicht mitgenommen werden können.

<sup>13</sup> Vgl. deren Art. 9 zum Datenzugang sowie viele allgemeine Bestimmungen, etwa zu Allgemeinen Geschäftsbedingungen und Ranking.



### Beispiel 12

*Ein Kleinstunternehmer, der über eine Online-Plattform Fahrdienstleistungen anbietet und sich ein gutes Bewertungsprofil erworben hat, möchte die Plattform wechseln und sein Bewertungsprofil übernommen haben.*

Die DEK sieht die Probleme, die mit einer allgemeinen gesetzlichen Verpflichtung zur Übernahme von Bewertungsprofilen verbunden wären. Sie empfiehlt der Bundesregierung jedoch, zu prüfen, unter welchen Bedingungen einem gewerblichen Nutzer doch ein Anspruch auf **Portabilität** seiner Bewertungsprofile zugesprochen werden kann, um auf europäischer Ebene auf eine weitergehende Regelung hinzuarbeiten.<sup>14</sup>

Die gesteigerte Bedeutung **sozialer Reputationsdaten** (Anzahl der „Likes“, „Followers“, „Freunde“) sind demgegenüber Teil einer größeren Entwicklung unserer Gesellschaft, die – mit der begrenzten Ausnahme von sog. Influencern – nicht mehr primär unter dem Aspekt der „Ökonomisierung“ personenbezogener Daten gesehen werden kann, sondern im Hinblick auf die systemischen gesellschaftlichen Auswirkungen zu diskutieren ist.

#### 3.3.6 Daten als Handelsware

Zahlreiche Unternehmen erzielen mittlerweile zum Teil beträchtliche Gewinne dadurch, dass sie gesammelte personenbezogene Daten, Profile und Scores oder aus aggregierten Rohdaten vorgenommene statistische Auswertungen über einzelne Personen an Dritte weiterverkaufen oder bereits vorhandene Profile mit Schätzdaten weiter anreichern und diese dann in den Handel bringen. Derartige Geschäftsmodelle werden im Folgenden als „**Datenhandel**“ bezeichnet.

Derzeit enthält die DSGVO keine spezifischen Regelungen zum Datenhandel. Sie qualifiziert derartige Geschäftsmodelle vielmehr schlicht als gewöhnliche Datenverarbeitungsprozesse, die den allgemeinen Regelungen der DSGVO unterliegen. Bei genauer Prüfung der geltenden Bestimmungen wird man oft zu dem Schluss gelangen müssen, dass Formen des Datenhandels gegen die Vorgaben der DSGVO verstößen und daher rechtswidrig betrieben werden. Insgesamt besteht im Bereich des Datenhandels jedoch ein **erhebliches Vollzugsdefizit**. Die DEK würde es deshalb begrüßen, wenn die Datenschutzaufsicht in Bezug auf diese Branche mit besonderer Dringlichkeit tätig werden würde und der Europäische Datenschutzausschuss (EDSA), hilfsweise die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK), unter Konkretisierung des risikobasierten Ansatzes der DSGVO klar abgrenzbare Fallgruppen für verschiedene Formen des rechtmäßigen Datenhandels entwickeln würde. Dabei wäre klarzustellen, in welchen Fällen des Datenhandels es einer Einwilligung der betroffenen Person für die Weitergabe von Daten bedarf, in welchen Fällen nur ein Widerspruchsrecht besteht, und in welchen Fällen zwingende schutzwürdige Gründe sogar das Widerspruchsrecht ausschließen.

Über den Vollzug des bereits geltenden Datenschutzrechts hinaus sollte die Weitergabe von Daten an Dritte im Lichte der allgemeinen Prinzipien der Datenverarbeitung (Art. 5 DSGVO) nur in engen Grenzen zulässig sein. Daher empfiehlt die DEK der Bundesregierung, auf europäischer Ebene u.a. bei der anstehenden Evaluierung der DSGVO darauf hinzuwirken, dass die **DSGVO um datenhandels-spezifische Regelungen ergänzt** wird. Für die Ausgestaltung einer solchen künftigen Regelung sollten die folgenden **ethischen Gesichtspunkte**, die zum Teil schon in der DSGVO niedergelegt sind, berücksichtigt werden:

<sup>14</sup> Vgl. etwa Artikel 6 und 7 des Entwurfs der „Model Rules on Online Intermediary Platforms“ des European Law Institute, die der DEK zur Verfügung gestellt wurden.

- a) Der Ausgangspunkt jeder Abwägung sollte in der informationellen Selbstbestimmung des Einzelnen liegen, sodass Datenhandel im Grundsatz der vorherigen **Einwilligung** der betroffenen Person unter Berücksichtigung der **materiellen Schranken** der Einwilligung (→ oben 3.2.1 und ) bedarf;
- b) Kann die Datenverarbeitung im Einzelfall auf eine andere Rechtsgrundlage als die Einwilligung gestützt werden, muss der Einzelne bereits vorab die Möglichkeit haben, ein **Widerspruchsrecht** auf einfache Weise auszuüben (z. B. Entfernen eines Häkchens unmittelbar vor Erhebung), und darf nicht erst auf gesonderte Kommunikationskanäle verwiesen werden;
- c) Datenhandelsmodelle ohne jedwede **Wahlmöglichkeiten** des Betroffenen sollten nur sehr selten in Betracht kommen, und zwar lediglich dann, wenn und soweit die Weitergabe der Daten aufgrund eindeutig überwiegender öffentlicher Interessen des Gemeinwohls erforderlich ist. Diese Kategorie sollte vollständig durch den Gesetzgeber konkretisiert werden;
- d) Die DSGVO enthält detaillierte Vorschriften zur Datenweitergabe an Auftragsverarbeiter und zur Datenweiterleitung in Drittstaaten. Zwar können im Lichte von Sinn und Zweck der DSGVO bei der Weitergabe an Dritte innerhalb des Gebiets der EU kaum niedrigere Anforderungen gelten und sollten diese Anforderungen etwa als „geeignete Garantien“ in die allgemeinen Regelungen hineingelesen werden. Dennoch wäre dringend zu empfehlen, die Pflichten bei der Weitergabe von Daten an Dritte (z. B. Kontrollpflichten) ebenso wie diesbezügliche Haftungstatbestände ausdrücklich gesetzlich zu konkretisieren;
- e) Verantwortliche sollten die konkrete Quelle, aus der ein Datum erhoben oder aus der es etwa durch automatisierte Schlussfolgerung generiert wurde, sowie die konkreten Einzelpfänger dokumentieren und offenlegen müssen, und zwar in einer standardisierten und maschinenlesbaren Form, welche die automatisierte Verwaltung etwa durch PMT/PIMS (→ dazu unten 4.3.) ermöglicht. Dadurch würde dem Umstand Rechnung getragen, dass Datenhändler in der **Wahrnehmung für Betroffene** bislang häufig im Verborgenen bleiben und dass eine bloße Benennung der Kategorien von Quellen oder Empfängern für den Betroffenen weitgehend nutzlos ist;
- f) Aufgrund der Vielzahl von Datenhändlern können Betroffenenrechte nur dann effektiv geltend gemacht werden, wenn zentrale Mechanismen die **Geltendmachung** erleichtern oder übernehmen (z. B. die Datenschutzaufsicht, → dazu oben , oder PMT/PIMS, dazu unten 4.3);
- g) Aufgrund des erhöhten Risikos und Kontrollverlusts in Folge von Streuungeffekten sollten Datenhändler einer **datenschutzrechtlichen Zertifizierungspflicht** unterworfen werden, die regelmäßige Auditierungen durch die Zertifizierungsstellen vorsieht. Die DEK empfiehlt, dass die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hierzu spezifische Zertifizierungskriterien aufstellen, die den von der DEK aufgezeigten Risiken und ihren Empfehlungen Rechnung tragen.



### 3.4 Daten und digitaler Nachlass

Moderne Kommunikationstechnologien und Kapazitäten der Datenverarbeitung ermöglichen eine nahezu lückenlose Aufzeichnung der privaten Aktivitäten eines Menschen über Jahrzehnte hinweg, ebenso wie deren automatisierte Auswertung. Gelangen die gesammelten Daten eines Menschen nach dessen Tod in die Hände der Erben oder eines sonstigen Dritten, bedeutet dies eine **neue Dimension von Gefährdung für die Privatheit**, und zwar sowohl für den Verstorbenen als auch vor allem für seine Kommunikationspartner zu deren Lebzeiten. Der oft angestellte Vergleich mit Tagebüchern und persönlichen Briefen hinkt, weil viele Kommunikationen (via Messenger, Chats, E-Mails usw.) funktional nicht an die Stelle von Briefen treten, sondern an die Stelle des flüchtig gesprochenen Wortes.

#### 3.4.1 Vorrang von Verfügungen zu Lebzeiten

Die DEK sieht die vorrangig anzustrebende Lösung in bewussten und informierten Dispositionen des Betroffenen noch zu Lebzeiten. Vielfach unterbleiben solche Dispositionen allein aus Unsicherheit oder Unkenntnis der rechtlichen und tatsächlichen Möglichkeiten. Vor diesem Hintergrund hält es die DEK für gerechtfertigt, die **Diensteanbieter zu verpflichten**, Nutzer auf Dispositionsmöglichkeiten für den Fall der dauernden Einwilligungsunfähigkeit (z.B. infolge von Demenz) oder des Todes hinzuweisen sowie die technischen Möglichkeiten bereitzustellen, möglichst barrierefrei – d.h. ohne oder mit nur minimalem Medienwechsel – Dispositionen zu treffen. Dazu könnte das **Telemediengesetz (TMG)** um eine entsprechende Vorschrift ergänzt werden.<sup>15</sup>

Nach Auffassung der DEK sollte die – nur besonders zugespitzte – Situation beim Tod einer Person auch zum Anlass genommen werden, ganz allgemein über die Gestaltung digitaler Kommunikationsformen nachzudenken. Die DEK empfiehlt der Bundesregierung daher, eine Verpflichtung für Messenger-Dienste zu prüfen, die **standardmäßige Löschung** von Nachrichten nach einer bestimmten Frist als Option anzubieten. Entscheidet sich der Nutzer für diese Option, würde dann eine Nachricht nach Ablauf der Frist – so sie vom Empfänger oder Sender nicht manuell archiviert wurde – automatisch gelöscht.

#### 3.4.2 Die Rolle von Intermediären

Die wachsende Sensibilität für das Thema hat auch neue Geschäftsmodelle hervorgebracht: Eine Vielzahl von Unternehmen bietet inzwischen Dienstleistungen rund um den digitalen Nachlass an (von der zentralen Verwahrung von Kontodaten und Passwörtern bis hin zur umfassenden Verwaltung des digitalen Nachlasses). Diese können sinnvolle Hilfestellungen sein. Sie sind aber zugleich auch mit Gefahren verbunden. Jene reichen von mangelnder Vorsorge für den Fall der Insolvenz oder sonstiger Auflösung des Unternehmens über Lücken in der Informationssicherheit bis hin zu echtem Betrug. Eine **Qualitätskontrolle** und vorsichtige **Regulierung** sowie die **Aufklärung** der Bevölkerung über mögliche Vorteile und Risiken erscheinen nach Auffassung der DEK zum Schutze der Bürger geboten.

15 Mario Martini: Juristenzeitung (JZ), 2012, S. 1145, 1154.

Die DEK empfiehlt darüber hinaus dem Staat, als Teil der Daseinsvorsorge für seine Bürger eine **zumindest staatlich beaufsichtigte Stelle** einzurichten, welche zu leistbaren Konditionen Basis-Dienstleistungen der digitalen Nachlasssicherung und Nachlassplanung auf dem aktuellen Stand der Informationssicherheitstechnik erbringt. Genau wie bei einem Testament eine Wahlmöglichkeit besteht, das Testament privat zu verwahren oder aber beim Notar oder Amtsgericht verwahren zu lassen, sollte eine vergleichbare Wahlmöglichkeit zwischen privater bzw. privatwirtschaftlicher Lösung und einer staatlichen Dienstleistung auch in Bezug auf den digitalen Nachlass bestehen.

### 3.4.3 Postmortaler Datenschutz

Die DEK empfiehlt keine prinzipielle Abkehr von den vom Bundesgerichtshof (BGH)<sup>16</sup> formulierten Grundsätzen eines **Übergangs auf die Erben**, da die unerwünschten und/oder überschießenden Wirkungen einer anderweitigen Default-Lösung (etwa eines gesetzlich angeordneten Treuhand-Modells oder einer Trennung vermögens- und persönlichkeitsbezogener Inhalte in Bezug auf ein und dasselbe Nutzerkonto) die möglichen Vorteile vielfach überwögen. Ist ein ganzes Nutzerkonto seiner Art nach ohne Vermögenswert, aber besonders persönlichkeits-sensitiv (etwa ein Online-Konto in einer Gruppe „Anonymer Alkoholiker“), dürfte es jedoch vorzuziehen sein, es aufgrund des höchstpersönlichen Charakters ganz vom Erbrecht auszunehmen. Soweit – auch zum Schutz der Kommunikationspartner des Verstorbenen – das **Tele-kommunikationsgeheimnis** Platz greift, ist der Gesetzgeber ohnehin nach wie vor aufgerufen, die Normkollision mit dem grundrechtlich verbürgten Erbrecht aufzulösen, etwa durch einen entsprechenden Hinweis im Erbrechts-teil des BGB.

Der vom BGH formulierte Grundsatz des Übergangs auf die Erben ist an das Bestehen eines Vertragsverhältnisses gekoppelt. Soweit kein Vertragsverhältnis besteht oder wegen Höchstpersönlichkeit nicht auf die Erben übergeht, können diese nicht einschreiten. Da der **Schutz durch die DSGVO mit dem Tod erlischt**, stehen sodann, nach derzeitiger Gesetzeslage, auch keine datenschutzrechtlichen Eingriffsmöglichkeiten zur Verfügung, die Angehörige geltend machen könnten. Dass damit die personenbezogenen Daten Verstorbener in die nahezu unbegrenzte Verfügungsgewalt der jeweiligen Verantwortlichen übergehen, erscheint ethisch bedenklich. Die DEK empfiehlt der Bundesregierung daher, nach dem Vorbild mehrerer europäischer Staaten von der in Erwägungsgrund 27 zur DSGVO erwähnten Möglichkeit Gebrauch zu machen, Regelungen zum **postmortalen Datenschutz** zu erlassen. Dabei sollten Angehörige fundamentale Betroffenenrechte – etwa auf Löschung von Daten oder Korrektur unrichtiger Daten – auch nach dem Tod des Betroffenen geltend machen können. Zugleich wäre in geeigneter Weise sicherzustellen, dass Verfügungen, die der Verstorbene zu Lebzeiten getroffen hat – und wenn auch nur konkret z.B. durch bewusste Öffentlich-Stellung seiner „Life Story“ – zu respektieren sind.

16 Urteil des Bundesgerichtshofs vom 12. Juli 2018, Aktenzeichen III ZR 183/17.



## 3.5 Besondere Gruppen von Betroffenen

### 3.5.1 Beschäftigte

Durch die teilweise weitreichende Erfassung der Bewegungs- und Leistungsdaten der Arbeitnehmer in modernen Arbeitsumgebungen und durch die für bestimmte Kollaborationsformen notwendige Erstellung biometrischer Profile entstehen erhebliche **Gefahren für die informationelle Selbstbestimmung und das allgemeine Persönlichkeitsrecht** der Arbeitnehmer. Zu den zu bedenkenden Fragen gehören neben den Rechtsgrundlagen der Datenverarbeitung und der Mitbestimmung der Interessenvertretungen etwa: Anforderungen an eine Information der Beschäftigten (vgl. etwa Herausforderungen durch Multi-Sensor-Fusion) und je nach Kontext Schaffung von Widerspruchsmöglichkeiten; Einzelheiten zur Speicherung, Speicherdauer und zulässigen Offenlegung von Beschäftigtendaten gegenüber Dritten; Recht auf Korrektur falscher oder überholter Daten (etwa bei persönlichen Profilen) und angemessene Löschregelungen; Rahmenbedingungen für eine begrenzte Kontrolle und Überwachung von Beschäftigten; Begrenzung der Lokalisierung von Mitarbeitern und Ausschluss von umfassenden Bewegungsprofilen; Begrenzung von Verpflichtungen zum Teilen von Social Media Accounts und zum Datenzugriff des Arbeitgebers im Kontext von „Bring your Own Device“-Modellen; Rahmenbedingungen für den Einsatz von biometrischen Systemen; oder Begrenzung von psychologischen Untersuchungsmethoden.

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. Kollektivverträge und Betriebsvereinbarungen sollen auch weiterhin im Bereich des Beschäftigtendatenschutzes eine wichtige Rolle spielen. Schon wegen der gesteigerten Grundrechtsrelevanz sollten die zentralen Grundsätze des Beschäftigtendatenschutzes aber nicht ausschließlich an Kollektivverträge und Betriebsvereinbarungen überwiesen werden, zumal diese nicht alle Beschäftigten erfassen. Die gegenwärtig bestehende Rechtsunsicherheit über das Ausmaß, in dem Vorschriften der DSGVO anwendbar bleiben, erschwert überdies sichere Investitionen.

Die DEK hält die klassische datenschutzrechtliche **Einwilligung**, verglichen mit anderen Rechtsgrundlagen der Verarbeitung von Beschäftigtendaten, nicht in allen Kontexten für geeignet, da die notwendigen Rahmenbedingungen für die Freiwilligkeit der Einwilligung im Beschäftigungskontext schwierig zu erfüllen sind und die jederzeitige Widerruflichkeit und Löschungsverpflichtung nicht in allen Konstellationen mit den Bedürfnissen des Arbeitgebers in einen angemessenen Ausgleich gebracht werden kann. Der Fokus eines Beschäftigtendatenschutzes sollte daher auf spezifisch auf den Beschäftigungskontext zugeschnittene, **gesetzliche Rechtfertigungsgründe** gelegt werden, die ein hohes Maß an Schutz und einen angemessenen Grundrechtsausgleich gewährleisten. Diese können einwilligungsähnliche Elemente aufweisen, welche die typischerweise gegebenen Machtverhältnisse im Beschäftigungskontext berücksichtigen.

Bei der Ausgestaltung der **Mitbestimmungsrechte der Interessenvertretungen**<sup>17</sup> über die Verarbeitung personenbezogener Daten im Betrieb muss der bestehenden **Wissensasymmetrie** zwischen Arbeitgeber- und Arbeitnehmerseite über die Wirkungsweise und Details der Verarbeitungsvorgänge angemessen Rechnung getragen werden. Es müssen daher Modelle gefunden werden, die den Interessenvertretungen über die geltenden Mechanismen hinaus den Rückgriff auf externen Sachverstand ermöglichen, wobei auf eine angemessene Einbindung des betrieblichen Datenschutzbeauftragten, aber auch auf den Schutz von Geschäftsgeheimnissen zu achten ist. Ange-sichts der ständigen Fortentwicklung datenverarbeitender Systeme im Betrieb (Software-Updates, selbstlernende Elemente usw.) sollte eine Fortentwicklung von punktueller Zustimmung hin zu **dauerhafter Begleitung von Prozessen** durch die Interessenvertretungen erfolgen.

Die Weiterentwicklung des Beschäftigtendatenschutzes sollte sich auch mit der Phase der **Bewerbung** um einen Arbeitsplatz und der **Begründung des Arbeits-verhältnisses** befassen. So ist beispielsweise darauf zu achten, dass das geltende Recht zu unzulässigen Fragen des Arbeitgebers im Bewerbungsverfahren und bei der Einstellung (z. B. nach dem Bestehen einer Schwangerschaft) weder durch den Einsatz sog. Human-Resources-Algorithmen noch durch die Aufforderung unterlaufen werden darf, dem Arbeitgeber Zugang zu Social-Media-Konten zu gewähren.

Bei einer Weiterentwicklung des Beschäftigtendatenschutzes ist darauf zu achten, dass auch diejenigen Personen erfasst werden, die in **unüblichen Beschäftigungsformen** arbeiten. Durch die Zunahme unüblicher Beschäftigungsformen in der Plattformökonomie verfügen die betreffenden Personen nicht über die klassischen Arbeitnehmer- und Mitspracherechte. Es kann zu einem enormen Machtungleichgewicht zwischen dem Auftraggeber bzw. dem Plattformbetreiber einerseits und dem Auftragnehmer bzw. den über die Plattform Arbeitenden andererseits kommen, das sich auch auf den Datenschutz und die informationelle Selbstbestimmung auswirken kann. Dem ist durch geeignete rechtliche Vorschriften – idealerweise auf EU-Ebene – und die Weiterentwicklung institutioneller Rahmenbedingungen, etwa durch eine Interessenvertretung, entgegenzuwirken.

### 3.5.2 Patienten

Mit Blick auf die Vorteile eines digitalisierten Gesundheitswesens spricht sich die DEK grundsätzlich für einen **raschen Ausbau digitaler Infrastrukturen sowie Prüfungs- und Bewertungsverfahren für digitale Versorgungsleistungen** innerhalb des Gesundheitssektors aus. Der qualitative und quantitative Ausbau digitalisierter Versorgungsmaßnahmen sollte die informationelle Selbstbestimmung des Patienten und seine Gesundheitskompetenz stärken.<sup>18</sup>

Bereits jetzt werden im Zusammenhang mit Versorgungsleistungen eine Vielzahl personenbezogener Daten verarbeitet. Bei ihnen handelt es sich im Regelfall um Gesundheitsdaten und genetische Daten, also um besondere Kategorien personenbezogener Daten i.S.d. Art. 9 DSGVO. Die **besondere Schutzbedürftigkeit dieser Daten bei gleichzeitiger Stärkung der Selbstbestimmung** von Patienten und Krankenversicherten, auch im Bereich der Forschung (→ unten), ist bei der Ausgestaltung einer zukünftig maßgeblich digitalen Gesundheitslandschaft umfassend zu berücksichtigen.

17 Derzeit etwa für den Betriebsrat § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz (BetrVG) und für den Personalrat § 75 Abs. 3 Nr. 17 Bundespersonalvertretungsgesetz (BPersVG).

18 Deutscher Ethikrat, Big Data und Gesundheit, Stellungnahme, 30.11.2017 (abrufbar unter: <https://www.ethikrat.org/fileadmin/Publikationen/Stellungnahmen/deutsch/stellungnahme-big-data-und-gesundheit.pdf>).



In diesem Zusammenhang betont die DEK die Dringlichkeit des Auf- und Ausbaus der **elektronischen Patientenakte** (ePA), um die Qualität, Transparenz und Wirtschaftlichkeit der medizinischen Versorgung zu verbessern.<sup>19</sup> Unter Berücksichtigung der zentralen Bedeutung der ePA für die Digitalisierung des Gesundheitswesens weist die DEK darauf hin, dass bei der Implementierung der ePA in erhöhtem Maße sowohl auf Aspekte der Informations- sicherheit als auch auf die Wahrung der Patientenhoheit zu achten ist; so sollte etwa das bestehende Kryptosicherheitskonzept der dezentralen Verwaltung von Schlüsseln bei den Versicherten (sog. PIN) erhalten bleiben. Zudem sollte die ePA auch im Falle der Einwilligungsunfähigkeit des Patienten auf der Grundlage der auch ansonsten anwendbaren Regelungen zur gesetzlichen Vertretung unabhängig von der Art der Krankenversicherung nutzbar sein.

Die Bedeutung digitaler Gesundheitsdienstleistungen und Produkte, die nicht kollektiv finanziert werden (sog. **zweiter Gesundheitsmarkt**), nimmt beständig zu – auch vor dem Hintergrund, dass die gesetzlichen Krankenversicherungen bislang lediglich vereinzelt digitale Versorgungsangebote bereitstellen. Neben Fitness-, Gesundheits- und Wellness-Angeboten ist der Möglichkeit des digitalen **Selbst-Monitoring** durch Apps sowie entsprechende Wearables eine signifikante Relevanz im Kontext des digitalisierten Gesundheitswesens beizumessen. Die Qualität dieser Apps und damit auch die Verwertbarkeit der dadurch erhobenen Daten ist jedoch vielfach nicht hoch und auch nicht umfassend geprüft. Dies birgt für die betroffenen Patienten und Nutzer ein zuweilen beträchtliches Gesundheitsrisiko. Zudem sollte es den Patienten nicht zugemutet werden, die Qualität der jeweiligen Produkte und Dienstleistungen, allem voran mit Blick auf den Datenschutz und die Informationssicherheit, eigenständig zu bewerten, noch sollte die digitale Gesundheitsversorgung eine Frage der individuellen finanziellen Leistungsfähigkeit sein. Mit Blick auf diesen Befund begrüßt die DEK die vorgesehene Etablierung eines Verfahrens zur Prüfung und Bewertung entsprechender Apps durch das Bundesinstitut für Arzneimittel und Medizinprodukte.

### 3.5.3 Minderjährige

Die DEK begrüßt die Bemühungen, sowohl auf gesetzgeberischer Ebene als auch auf der Ebene der Selbstregulierung, besondere **Schutzmechanismen** für die digitale Selbstbestimmung Minderjähriger zu entwickeln. Diese sollen erstens einem stärkeren Datenschutz, dem Schutz vor Profilbildung, Manipulation durch Dark Patterns und Addictive Designs usw. dienen und zweitens einem besseren Schutz vor nicht altersgerechten (gewaltverherrlichen usw.) Inhalten.

Allerdings erinnert die DEK auch daran, dass alle diese Schutzmechanismen ins Leere laufen, solange nicht ein zuverlässiges **Identitätsmanagement** gewährleistet ist und sichergestellt wird, dass Minderjährige auch als solche erkannt und behandelt werden. Eine vom Nutzer behauptete Altersangabe ist als Mittel der Überprüfung jedenfalls ungeeignet. Es wäre ethisch aber auch problematisch, zu fordern, dass Anbieter durch Erhebung – möglicherweise sogar besonders sensibler – personenbezogener Daten (etwa: Gesichtserkennung mit Datenübertragung in die Cloud des Anbieters) selbst eine Alterseinschätzung vorzunehmen haben oder aber die Last ganz den Erziehungsberechtigten aufzubürden, die damit leicht überfordert würden. Die DEK empfiehlt der Bundesregierung daher, die Entwicklung **familienadäquater Technologien** zu fördern, die eine selbstbestimmte Entwicklung der Minderjährigen ermöglichen und zugleich ihren Schutz zuverlässig gewährleisten.

<sup>19</sup> Siehe hierzu bereits die Empfehlung der DEK für eine partizipative Entwicklung der elektronischen Patientenakte (ePA) vom 28.11.2018 (abrufbar unter: [www.datenethikkommission.de](http://www.datenethikkommission.de)).

In diesem Zusammenhang empfiehlt die DEK der Bundesregierung, insbesondere bei mobilen Endgeräten auf europäischer Ebene darauf zu dringen, dass die in der DSGVO festgelegten Prinzipien von **Datenschutz „by design“ und „by default“** eingehalten werden, um den Schutz der informationellen Selbstbestimmung und der Privatheit Minderjähriger zu gewährleisten. Um die Hersteller der Betriebssysteme für mobile Endgeräte und die Anbieter digitaler Dienste dazu zu bringen, alle für die betreffenden Altersstufen geltenden rechtlichen Vorschriften einzuhalten und Dienste, die nicht altersgerecht sind, zu blockieren, müssten die deutschen und europäischen Datenschutzbehörden, die Kartellbehörden, die Medienaufsicht und die technischen Regulierungsbehörden in ihren jeweiligen Aufgaben- und Zuständigkeitsbereichen dazu beitragen, die Anforderungen durchzusetzen. Auch etwa die Akteure im Bereich der Schulen und Kindertagesstätten, in denen solche Systeme zum Einsatz kommen, sollten diese Anforderungen im Rahmen von Beschaffungen deutlich machen. Zur Notwendigkeit, Datenschutz „by design“ und „by default“ auch gegenüber Herstellern einzufordern (→ siehe näher unten ).

Zu erwägen ist in diesem Zusammenhang darüber hinaus insbesondere die Einführung einer EU-weiten Verpflichtung für die Hersteller mobiler Endgeräte, ein Endgerät bereits beim Kauf irreversibel (oder nur mithilfe eines Schlüssels reversibel) und erkennbar als „Kinder-Endgerät“ zu programmieren. Diese Programmierung hätte automatisch die Einhaltung aller für Kinder geltenden rechtlichen Vorschriften sicherzustellen und nicht altersgerechte Dienste zu blocken. Die Minderjährigen können den **bei Aktivierung eingestellten entsprechenden Status** ihres Geräts/Betriebssystems dabei nicht ohne Einverständnis der Eltern ändern. Eine solche Lösung hätte auch klare Vorteile gegenüber sog. Parental-Control-Apps, welche erstens vielfach ein eigenes Datenschutz- und Informationssicherheitsproblem darstellen und zweitens ethisch problematische Möglichkeiten der Totalüberwachung im privaten Bereich mit sich bringen.

### 3.5.4 Sonstige Pflege- und Schutzbedürftige

Die Verarbeitung von Daten vulnerabler Gruppen erfolgt vielfach zu deren eigenem Schutz, so etwa im Bereich der Pflege. Digitale Technologien ermöglichen beispielsweise älteren Menschen ein viel sichereres Verbleiben in der gewohnten Umgebung. Dies kann auch helfen, den negativen Auswirkungen des Fachkräftemangels in der Pflege entgegenzuwirken und eine bessere Versorgung sicherzustellen. Insbesondere **digitale Assistenzsysteme** können dabei, richtig eingesetzt, eine Brückentechnologie darstellen und sich adaptiv den unterschiedlichen Bedürfnissen verschiedener Menschen anpassen.

Sowohl das Recht auf Leben und auf körperliche Unverletztheit als auch das Recht auf informationelle Selbstbestimmung stellen Grundrechte dar, die im Wege praktischer Konkordanz miteinander in Einklang zu bringen sind. Dabei sind insbesondere die **Gefahren für Leben bzw. Gesundheit** auf der einen Seite und die Intensität des Eingriffs in die informationelle **Selbstbestimmung** auf der anderen Seite zu berücksichtigen.



Bei der Überwachung durch professionelle Akteure im Pflegebereich bedarf es nach Auffassung der DEK der Erarbeitung von **Standards und Leitlinien** durch die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK). Diese sollten insbesondere vorgeben, auf welche Rechtsgrundlagen sich diese Akteure in welcher Situation stützen können und in welchen Fällen – insbesondere im Falle der Ermangelung einer **Einwilligung** der betroffenen Person oder ihres Betreuers – eine Maßnahme gegebenenfalls auf Art. 6 Abs. 1 lit. f oder lit. d DSGVO gestützt werden kann oder ganz unterbleiben muss. Auch Vorgaben für die Informationsteilung sollten darin enthalten sein, wobei nach Auffassung der DEK bereits im Vorfeld der Aufnahme in einer Einrichtung (z.B. Pflegeheim, Kindergarten, Schule) differenzierte Informationen über die Möglichkeiten der digitalen Überwachung erteilt und ggf. – soweit keine gesetzliche Rechtsgrundlage für die Datenverarbeitung besteht – auch differenzierte Einwilligungen eingeholt werden müssten. Derartige Standards und Leitlinien wären zugleich geeignet, für die Träger von Einrichtungen und das Pflegepersonal mehr Rechtssicherheit zu schaffen und Haftungsrisiken zu verringern. Zur Klarstellung, dass auch eine antizipierte Einwilligung der betroffenen Person in einer **Patientenverfügung** möglich ist, sollte § 1901a BGB entsprechend angepasst werden.

Als besonders schutzbedürftig sind grundsätzlich auch Personen anzusehen, die sich im häuslichen Bereich und somit im sicher gewährten Zentrum ihrer räumlichen Privatsphäre bewegen. Auch hier entstehen im Zusammenhang mit neuen Technologien wachsende potenzielle **Überwachungsmöglichkeiten von Privatpersonen durch andere Privatpersonen** (z.B. die Überwachung von Partnern, Kindern oder Menschen mit Behinderung), bis hin zu einer ethisch äußerst bedenklichen Möglichkeit einer privaten Totalüberwachung. Da es vielfach an einer hinreichenden Sensibilität für das Thema fehlt, empfiehlt die DEK der Bundesregierung, aber auch den in vielen Punkten zuständigen Landesregierungen, diesbezüglich **bewusstseinsbildende Maßnahmen** zu ergreifen. Darüber hinaus empfiehlt die DEK der Bundesregierung, die Entwicklungen weiter zu beobachten, sieht jedoch derzeit noch keinen Bedarf für gesetzliche Maßnahmen (z.B. neue Straftatbestände).

## 3.6 Datenschutz durch Technikgestaltung

Diejenigen, die ethisch begründete Datenrechte wahrnehmen oder korrespondierende Datenpflichten befolgen müssen – seien es etwa Bürger, Unternehmen oder staatliche Stellen – müssen dazu auch in der Lage sein. Es bedarf dafür auch **technischer Voraussetzungen**, insbesondere befähigender Technologien. Durch solche Befähigungen darf allerdings nicht die Verantwortung für den Schutz grundlegender Rechte und Freiheiten auf individuelle Nutzer überwälzt werden. Hier ist vielmehr der Staat mit einer entsprechenden **Regulierung** gefordert, die den Schutz dieser grundlegenden Rechte und Freiheiten prinzipiell gewährleistet, ohne dass der Einzelne tätig werden müsste.

### 3.6.1 Datenschutzfreundliches Design von Produkten und Dienstleistungen

Mit Art. 25 DSGVO, der mit „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“ überschrieben ist, werden **Datenschutz „by design“ und „by default“** zur Pflicht für Verantwortliche. Dies bedeutet, dass Datenschutz im Sinne der Grundsätze aus Art. 5 DSGVO risikoadäquat bei der Technikgestaltung berücksichtigt werden muss. Die dafür notwendigen technischen und organisatorischen Maßnahmen müssen sowohl bereits vor der Verarbeitung, nämlich wenn der Verantwortliche die Mittel für die Verarbeitung festlegt, als auch während der eigentlichen Verarbeitung getroffen werden.

## Datenschutz „by design“ und „by default“

**Datenschutz „by design“** stellt die Wahl der technischen und organisatorischen Maßnahmen unter Bedingungen wie den Stand der Technik, die Implementierungskosten, die Verarbeitung und das Risiko für die Rechte und Freiheiten natürlicher Personen. **Datenschutz „by default“** ist nicht an solche Bedingungen geknüpft, muss also stets umgesetzt werden. In der Praxis werden allerdings oft überschießende personenbezogene Daten wie z. B. Identifikatoren verarbeitet, die Verarbeitung ist nicht ausreichend beschränkt, die Speicherfristen sind zu lang und es können mehr Personen auf die Daten zugreifen als nötig.

Aus diesem Grund wurden für das „**Privacy Engineering**“ die weiteren Schutzziele Nichtverkettbarkeit, Transparenz und Intervenierbarkeit entwickelt, die mittlerweile als sogenannte Gewährleistungsziele Teil des Standard-Datenschutzmodells (SDM) der deutschen Datenschutzaufsichtsbehörden geworden sind.<sup>1</sup> Das SDM definiert ähnlich den IT-Grundschutz-Katalogen des BSI Bausteine, die von Verantwortlichen und Technikgestaltern herangezogen werden können, um die für ihren jeweiligen Schutzbedarf angemessenen technischen und organisatorischen Maßnahmen zu treffen. Bislang sind erst einige Bausteine verfügbar, weitere werden folgen. Die Anlehnung an

die IT-Grundschutz-Kataloge und die Normenreihe ISO 2700x führt dazu, dass viele Entwickler mit dem grundsätzlichen Konzept vertraut sind und die rechtlichen Anforderungen besser bei der Konzeptionierung und Implementierung von technischen Systemen umsetzen können.

Auch die Frage, inwieweit eine **Zentralisierung oder eine Dezentralisierung** bei der Gestaltung von technischen Systemen zu bevorzugen ist, muss im Einzelfall geklärt werden. Zentralisierte Systeme erlauben in der Regel ein höheres Maß an Kontrolle und Einflussnahme durch die Betreiber. Dies kann gewollt sein, z. B. um Datenschutz- oder Informationssicherheitsfunktionalität durchzusetzen. Es kann aber auch kritisch werden, da die zentralisierte Datenhaltung und Steuerung der Verarbeitung ein höheres Missbrauchspotenzial aufweist – einerseits als Angriffsziel von Dritten, die an die Daten herankommen oder die Verarbeitung sabotieren wollen, andererseits durch den Betreiber selbst, beispielsweise durch eine Nutzung des großen Datenbestands zu anderen Zwecken als vorgesehen. Dezentralisierung kann in geeigneter Gestaltung dagegen gewährleisten, dass Daten nicht oder nicht einfach verknüpft werden können oder dass sich die Verfügbarkeit des Gesamtsystems schwerer stören lässt.

<sup>1</sup> Arbeitskreis Technik der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder: Das Standard-Datenschutzmodell – Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele V.1.1 – Erprobungsfassung, 2018 (abrufbar unter: <https://www.datenschutzzentrum.de/sdm/>).

Besondere Praxisrelevanz haben datenschutzrechtliche Designvorgaben in Bezug auf **Endgeräte**. Diese können am Körper (sog. Wearables, z. B. SmartWatch oder intelligente Textilien) oder zumindest in Körpernähe tragbar (z. B. Smartphone), anderweitig beweglich (z. B. vernetztes Auto) oder auch unbeweglich sein (z. B. Smart-Home-Einrichtungen). Dem Design der Software-systeme für solche Endgeräte kommt umso größere ethische Relevanz zu, je mehr sie in Körpernähe bzw. in sehr privaten und intimen Bereichen (z. B. Badezimmer,

Schlafzimmer) zum Einsatz kommen, je stärker besonders vulnerable Personen (z.B. Kinder und Jugendliche, Pflegebedürftige, Personen mit Behinderungen) betroffen sind und je tiefer sie in die Persönlichkeit einer Person eindringen. Eine besondere Herausforderung an selbstbestimmungsfreundliches Design stellt das hohe Maß an (Selbst-)Verantwortung dar, welches den Nutzern bei Zusammenstellung, Konfiguration und Betrieb der Geräte zugestanden bzw. abverlangt wird.



Die DEK empfiehlt der Bundesregierung, die Erforschung und Entwicklung **technischer Standards** für Endgeräte verstärkt zu fördern. Ferner empfiehlt die DEK nachdrücklich, auf europäischer Ebene auf die Einführung **technischer Vorgaben** zur Wahrung von Selbstbestimmung und digitaler Produktsicherheit im privaten Bereich zu dringen, insbesondere für den Bereich von **Endgeräten für Verbraucher**. Vorgaben an Endgeräte sollten nach Auffassung der DEK jedenfalls Folgendes umfassen:

- Produkte müssen auf dem Stand der Technik und dem Schutzbedarf angemessen vor **Cyberangriffen und zweckfremder Verwendung** von Daten geschützt werden, wobei insbesondere für sensible Daten (z.B. Gesundheitsdaten) geeignete Garantien vorliegen müssen. Die Wahrung eines hohen Grades an Cyberresilienz ist dabei eine Gemeinschaftsaufgabe von Staat, Wirtschaft und jedem Einzelnen;
- Es muss zu jedem Zeitpunkt klar ersichtlich sein, welche **Funktionen momentan aktiviert** sind, insbesondere ob GPS, Kamera, Mikrofon oder andere Sensoren eingeschaltet sind, ob eine Verbindung zum Internet besteht und ob Daten nach außerhalb des geschlossenen lokalen Bereichs übertragen werden;
- Die **Übertragung von Daten** nach außerhalb des lokalen Bereichs muss auf einfache Weise abzuschalten sein, und mittlerweile lokal gespeicherte Daten dürfen auch beim nächsten Einschalten nicht ohne den Willen des Nutzers übertragen werden (dies muss auch für einzelne Applikationen gelten, etwa auf Smartphones oder Smart-TV);
- Soweit **Basisfunktionen des Geräts auch ohne solche Datenübertragung** technisch möglich sind, müssen sie bei Abschalten der Übertragung erhalten bleiben (z.B. intelligenter Kühlschrank muss noch kühlen);
- Geräte sollten mit einem „**User Onboarding**“-Ansatz ausgeliefert werden, wobei das Onboarding bei erster Inbetriebnahme automatisch erfolgen und sich auch für Zweitnutzer nach Belieben wiederholen lassen sollte. Dabei sollte nicht nur die Funktionsweise erläutert werden, sondern ebenso die Erfassung und weitere Verarbeitung von Nutzerdaten;
- Endgeräte, die direkt mit dem Internet verbunden (z.B. Router) und mittels eines Passworts abgesichert sind, sollten nicht ohne eine vorherige Änderung des Initialpassworts in Betrieb genommen werden können. Systemseitig sollten nur **Passwörter**, die dem Stand der Technik entsprechen, zugelassen werden.

## Nachvollziehbarkeit und Transparenz

Datenschutz „by design“ umfasst ebenso die Nachvollziehbarkeit und Transparenz der Systeme, einschließlich der Anwendungen, Skripte, Quellen und Elemente zu jedem Entwicklungs- und Prozesszeitpunkt. Die DEK begrüßt die laufenden Bemühungen, Best-Practice-Modelle für gute Allgemeine Geschäftsbedingungen (AGB) und Verbraucherinformationen zu entwerfen („One Pager“). Dabei sollen Verbraucher im Rahmen eines Mehrebenen-Ansatzes in einem ersten Schritt einfache, konzentrierte Informationen über die wesentlichen Datenverarbeitungen erhalten und – wenn gewünscht – in einem weiteren Schritt zu den ausführlichen AGB und Datenschutzinformationen geleitet werden. Dies wird aber nicht ausreichen, das Problem der unzureichenden und/oder den Verbraucher überfordernden und damit ihr Ziel verfehlenden Information zu lösen.

Um dem Verbraucher eine informierte Kaufentscheidung zu ermöglichen, sollten auf europäischer Ebene unter maßgeblicher Einbeziehung der Wirtschaft und

Zivilgesellschaft einheitliche, maschinenlesbare und intuitiv verständliche Bildsymbole (**Piktogramme**) eingeführt werden, die wesentliche digitale Merkmale von Produkten, einschließlich digitalen Produkten (z.B. Apps), und Dienstleistungen vermitteln (z.B. für die Merkmale „Basisfunktionen nur mit Internetverbindung“, „Verfügt über Internetverbindung für Komfortfunktionen“, „Übermittelt Nutzerdaten“ und „Nutzer-Tracking“) und zusätzlich – insbesondere für graduell in unterschiedlichem Ausmaß gegebene Produktmerkmale – durch **Farbcodierungen** unterstützt sein können. Der Bundesregierung wird empfohlen, bei der Europäischen Kommission auf die Entwicklung solch standardisierter Bildsymbole gemäß Art. 12 Abs. 8 DSGVO hinzuwirken.

Die Förderung der Entwicklung zertifizierter **elektronischer Einkaufsassistenten**, die im Ladengeschäft oder Webshop ein Produkt identifizieren und Produktinformationen adressatengerecht aufarbeiten, kann zusätzliche Transparenz für Verbraucher schaffen.

Von der Gestaltung der Produkte, Dienste und Anwendungen hängt es ganz wesentlich ab, inwieweit die Verantwortlichen und Verarbeiter ihre Datenschutzhilfepflichten erfüllen können. Jedoch sind Hersteller, die nicht selbst personenbezogene Daten verarbeiten, keine Adressaten der DSGVO. Die Verantwortlichen, die nicht auf Eigenentwicklungen zurückgreifen können oder wollen, müssen also eingebauten Datenschutz einfordern.<sup>20</sup> Die DEK empfiehlt der Bundesregierung daher, Maßnahmen zu ergreifen bzw. Maßnahmen anderer Akteure zu fördern, die zu einer verstärkten **Verantwortlichkeit der Hersteller** führen. Dies kann etwa geschehen durch:

- Unmittelbare **Vorgaben für Produktdesign und Produktsicherheit** durch den Gesetzgeber;
- Schaffung **wirksamer Rechtsbehelfe** entlang der Vertriebskette, mit deren Hilfe die Verantwortlichkeit für unzureichenden Datenschutz „by design“ und „by default“ auf die Hersteller<sup>21</sup> abgewälzt werden kann (vgl. gewisse Fortschritte der Abwälzung vom Verbraucher auf den Händler und entlang der Vertriebskette durch die neue EU-Richtlinie 2019/771 über den Warenkauf);

20 Vgl. Erwägungsgrund 78 zur DSGVO.

21 Christiane Wendehorst: Verbraucherrelevante Problemstellungen zu Besitz- und Eigentumsverhältnissen beim Internet der Dinge, Teil 2: Wissenschaftliches Rechtsgutachten, Studien und Gutachten im Auftrag des Sachverständigenrats für Verbraucherfragen, Dezember 2016, S. 120 (abrufbar unter: <http://www.svr-verbraucherfragen.de/wp-content/uploads/Wendehorst-Gutachten.pdf>).

- Gestaltung von **Ausschreibungen** sowie der Richtlinien für **Beschaffungsmaßnahmen** der öffentlichen Hand in einer Weise, die den Nachweis absoluter DSGVO-Konformität einschließlich der Einhaltung von Datenschutz „by design“ und „by default“ einfordert;
- Schaffung von **Anreizen** für ein besonders hohes Maß an Datenschutz „by design“ und „by default“, etwa durch entsprechende Bedingungen in staatlichen Förderprogrammen.

### 3.6.2 Datenschutzfreundliche Produktentwicklung

Datenschutz durch Technikgestaltung ist auch bei der Produktentwicklung und Produktweiterentwicklung zu beachten. Dies gilt insbesondere für die **Entwicklung algorithmischer Systeme**, bei denen typischerweise große Mengen an Datensätzen – etwa als Trainingsdaten – erforderlich werden (→ zu Einzelheiten Teil C, 2.2).

#### Datenschutzfreundliches Trainieren algorithmischer Systeme

Um die Datenschutz-Grundsätze in Art. 5 DSGVO beim Trainieren algorithmischer Systeme zu erfüllen, bestehen verschiedene Möglichkeiten. So hat etwa die Norwegische Datenschutzaufsichtsbehörde Datatilsynet im Januar 2018 Mittel und Methoden für ein datenschutzfreundliches Trainieren algorithmischer Systeme<sup>1</sup> vorgeschlagen:

1. Einsatz **datenminimierender Verfahren** bezüglich der Trainingsdaten, z. B. durch das Verwenden synthetischer Daten (beispielsweise über sog. Generative Adversarial Networks), durch föderales Lernen oder durch den Einsatz von datensparsamen Varianten, wie sie für neuronale Netze vorgeschlagen werden;

2. Einsatz von **Verschlüsselungsverfahren** wie Differential Privacy, Homomorphic Encryption oder anderer Verfahren, die Informationsabfragen erlauben, ohne einen Vollzugriff auf die Datenbank zu gewähren;
3. Einsatz **transparenzfördernder Verfahren**, um eine höhere Verständlichkeit und Nachvollziehbarkeit zu erreichen.

Die DEK sieht in all diesen Bereichen allerdings noch **Forschungsbedarf**. Dies betrifft auch Möglichkeiten des datenschutzfreundlichen Testens der algorithmischen Systeme.

<sup>1</sup> Datatilsynet: Artificial intelligence and privacy, Report, Januar 2018, S. 27 f. (abrufbar unter: <https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf>).

# Zusammenfassung der wichtigsten 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.

**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.

**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.

**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 Risiko-einschätzung** (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 gelgenden 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.

**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.

**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.

**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**.

**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.

## 4. Verbesserung des kontrollierten Zugangs zu personenbezogenen Daten

Daten – auch personenbezogene Daten – sind eine **zentrale Ressource** der Datenwirtschaft und Schlüssel für viele wohlfahrtsfördernde Anwendungen. Die rasante Entwicklung digitaler Technologien – auch solcher, von denen jeder Einzelne enorm profitiert – wurde unter anderem durch die Auswertung der Daten von Milliarden von Nutzern weltweit ermöglicht. Auch wenn bei personenbezogenen Daten zunächst immer der Datenschutz im Mittelpunkt der Betrachtung steht, stellt sich doch verstärkt die Frage, inwieweit die generelle Verbesserung eines kontrollierten Zugangs zu personenbezogenen Daten – im Sinne des Prinzips der Wohlfahrt durch Nutzung und Teilen von Daten (→ oben 1.3.) und innerhalb des vom Datenschutzrecht vorgegebenen Rahmens – ethisch vertretbar oder sogar wünschenswert wäre.

### 4.1 Ermöglichung von Forschung mit personenbezogenen Daten

#### 4.1.1 Vorüberlegungen

Forschung stellt die Basis nahezu all unserer technischen Errungenschaften dar. Unter Bedingungen zunehmender Digitalisierung kommt datenbasierter Forschung dabei eine **herausragende Bedeutung** zu. Diese wird von der DSGVO bereits anerkannt und vom nationalen Recht, namentlich dem BDSG und den Landesdatenschutzgesetzen, punktuell gestärkt. Die DEK unterstreicht auch die signifikante Bedeutung der Verarbeitung genetischer, biometrischer und weiterer **Gesundheitsdaten** zu Forschungszwecken, zur Förderung der Prävention sowie zur Entwicklung neuer diagnostischer und therapeutischer Maßnahmen. Gerade der Einsatz Künstlicher Intelligenz verspricht in bestimmten Bereichen große Fortschritte, er ist aber je nach Fragestellung auf umfangreiche Datenbestände angewiesen. Die Freigabe von Gesundheitsdaten für Forschungszwecke wird auch immer wieder unter dem **Begriff der „Datenspende“** diskutiert. Dieser Begriff ist jedoch **irreführend**, weil Daten im Unterschied

zur Spende eines Organs oder einer Geldspende beliebig oft sowie gleichzeitig und auch vom Datengeber selbst weiterverwendet werden können.

Soweit die Forschungstätigkeit maßgeblich auf eine gemeinwohlorientierte Datennutzung ausgerichtet ist (etwa zur Gesundheitsvorsorge, zur Entwicklung nachhaltiger Mobilitätskonzepte oder allgemein zur Verbesserung von Lebensbedingungen), empfiehlt die DEK, vorhandene **datenschutzrechtliche Privilegierungstatbestände** auszuschöpfen und Forschung im Rahmen von Abwägungen als ein besonders wichtiges Interesse zu werten.<sup>22</sup> Ergänzend sollten die Bundesländer vorhandene Regelungsbefugnisse, beispielsweise im Kontext des Hochschulrechts oder aber auch im Rahmen des Datenschutzrechts, innovationsfreudlich sowie im Geiste des vorgenannten Forschungsprivilegs ausfüllen. Der Begriff der wissenschaftlichen Forschung ist dabei – auch unter Einbeziehung der Rechtsprechung des Bundesverfassungsgerichts – weit zu verstehen. Nicht entscheidend ist dabei, ob die jeweilige Forschungstätigkeit durch öffentliche oder durch private Stellen betrieben wird.

Die DEK gibt zu bedenken, dass innerhalb des Spannungsverhältnisses zwischen den Grundrechtspositionen der Forschenden sowie der informationellen Selbstbestimmung der Betroffenen stets ein **angemessener Ausgleich** zu suchen ist. Im Rahmen der gesetzlich erforderlichen Abwägungen ist der **Schutz sensibler Daten** und damit einhergehend die Rechte der Betroffenen, wie beispielsweise Patienten oder Versicherte, besonders zu gewichten. Dabei kann sich zum Beispiel die Verschwiegenheitspflicht, die an bestimmte Berufsgeheimnisträger, wie Ärzte (vgl. § 203 Strafgesetzbuch), adressiert ist, auf die Arbeit von Forschungsinstitutionen auswirken, soweit diese auf Daten angewiesen sind, die bei jenen Berufsgeheimnisträgern erhoben werden bzw. gespeichert sind. Dies erfordert die Berücksichtigung der zum Schutz informationeller Selbstbestimmung normierten Verfahrensvorkehrungen.

<sup>22</sup> Vgl. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder: Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, 2019, S. 14 (abrufbar unter: [https://www.datenschutzkonferenz-online.de/media/oh/20190405\\_oh\\_tmg.pdf](https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf)).

#### 4.1.2 Rechtsklarheit und Rechtssicherheit

Bereits das derzeit geltende Recht ermöglicht und fördert datenbasierte Forschung. Allerdings stellen sich im Detail **Auslegungsfragen**, die der weiteren Klärung durch Aufsichtsbehörden und Gerichte bedürfen. So ist beispielsweise noch nicht abschließend geklärt, ob die **Weiterverwendung** für Forschungszwecke von Daten, die zu einem anderen Zweck (z.B. Gesundheitsversorgung) einmal rechtmäßig erhoben wurden, wegen Art. 5 Abs. 1 lit. b DSGVO und im Lichte von Erwägungsgrund 50 bei „geeigneten Garantien“ i.S.v. Art. 89 DSGVO automatisch rechtmäßig ist, oder ob dafür ebenso eine eigene Rechtsgrundlage in Art. 6 Abs. 1-3 oder Art. 9 DSGVO gegeben sein muss wie für die erste Erhebung (bei Gesundheitsdaten wären dies z.B. gemäß § 27 BDSG eine ausdrückliche Einwilligung oder ein „erhebliches Überwiegen“ der Forschungsinteressen). Teilweise wird auch vertreten, dass sich nur derjenige auf das Weiterverarbeitungsprivileg berufen könne, der die Daten selbst erhoben hat. Ebenso besteht Unsicherheit in Bezug auf die Reichweite des Forschungsbegriffs im Zusammenhang mit der **Entwicklung und Weiterentwicklung von Produkten**.

Auch wenn der rechtliche Rahmen für datenbasierte Forschung in Deutschland – auch in Bezug auf Gesundheitsdaten und andere besondere Kategorien von Daten – durchaus vorhanden ist, fehlt es diesem Regelungsrahmen schon aufgrund der föderalen Struktur und den grundgesetzlich festgeschriebenen Gesetzgebungscompetenzen von Bund und Ländern in Details an Einheitlichkeit. Dies führt aus Sicht der Forschung zu **Rechtsunsicherheit**, die zusätzlich dadurch verstärkt wird, dass verlässliche Auslegungshilfen, insbesondere was die Anforderungen an eine wirksame Einwilligung und das „erheblich überwiegende Interesse“ des For-schenden i.S.d. § 27 BDSG betrifft, noch ausstehen. Diese Rechtsunsicherheit könnte die datenbasierte Forschung in Deutschland beeinträchtigen. Die DEK regt daher an, dass – etwa durch die Konferenz der unabhängigen

Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK), unter Einbeziehung relevanter Stakeholder aus Politik, Gesundheitswirtschaft und Zivilgesellschaft – **Handlungsempfehlungen sowie Auslegungskriterien** für einen praktikablen und rechtssicheren Umgang mit den betreffenden Normen ausgearbeitet werden (→ zu Standards der Pseudonymisierung und Anonymisierung unten 4.2).

Zur **weiteren Harmonisierung** der verschiedenen Regelungen im Bereich der Forschung (unterschiedliche mitgliedstaatliche Regelungen in der EU, Aufgabenteilung zwischen BDSG und Landesdatenschutzgesetzen, Spezialregelungen für besondere Bereiche) empfiehlt die DEK der Bundesregierung,

- a) auf eine **Synchronisierung** der forschungsspezifischen **Rechtsgrundlagen** im BDSG und in den Landesdatenschutzgesetzen sowie in bereichsspezifischen Gesetzen zu dringen;
- b) auf **europäischer Ebene** Vorhaben voranzutreiben, die auf eine stärkere Harmonisierung der mitgliedstaatlichen Regelungen zum Forschungsdatenschutz abzielen; sowie
- c) auf ein **Notifizierungserfordernis** für mitgliedstaatliche Regelungen in diesem Bereich und auf die Errichtung einer europäischen **Clearing-Stelle** für grenzüberschreitende Forschungsprojekte hinzuarbeiten.



#### 4.1.3 Einwilligungsprozesse bei sensiblen Daten

Ein zentrales Instrument des Schutzes von Teilnehmern an Forschungsvorhaben (sog. Probanden), insbesondere an klinischer Forschung und Forschung mit Gesundheitsdaten sowie anderen besonders sensiblen Datenkategorien, ist die freiwillige, informierte und ausdrückliche Einwilligung der betroffenen Personen. Sie dient dazu, die **informationelle Selbstbestimmung** des Probanden zur Geltung kommen zu lassen. Zusätzlich stellt sie durch die verständliche Information über das Forschungsvorhaben sicher, dass die Teilnahme an der Studie den **Werten und Präferenzen** des Probanden entspricht. Als rechtlich verankertes Schutzinstrument fördert sie Transparenz und damit auch das Vertrauen in die Forschung. Nicht zuletzt trägt sie zur Integrität von Forschung und Forschenden bei.

Die Einholung einer informierten Einwilligung stellt die verantwortlichen Forschenden allerdings insbesondere im Kontext sensibler Daten vor erhebliche Herausforderungen. Wenn etwa ein neues Forschungsprojekt an Gesundheitsdaten durchgeführt werden soll, die bereits in einer Datenbank liegen, muss die betreffende Person kontaktiert werden, um erneut eine Einwilligung einzuholen, falls sie nicht – wie es als sog. breite Einwilligung (**broad consent**) im Bereich der Ethik diskutiert wird – schon ursprünglich in die Weiterverwendung ihrer Daten eingewilligt hat. Sollen Gesundheitsdaten aus der alltäglichen medizinischen Versorgung für Forschungszwecke verwendet werden, ist der Zugang zu den Patienten, um eine informierte Einwilligung einzuholen, ebenfalls mit hohen praktischen Hürden versehen. Die DEK empfiehlt vor diesem Hintergrund die Ausgestaltung und Aufbereitung entsprechender **Musterverfahren zur Einholung von Einwilligungen**, um die forschungsbezogene Verarbeitung in diesem Bereich zusätzlich zu erleichtern.

Unter ausdrücklicher Berücksichtigung des Grundrechtsgehalts der Einwilligung spricht sich die DEK ergänzend für die Entwicklung **innovativer Einwilligungsmodelle** im Forschungskontext aus. So sind bereits dynamische und für den Einzelfall angepasste Einwilligungserklärungen (**dynamic consent**) in Erprobung. Dabei ist dafür zu sorgen, dass der Einwilligende auch nach Abgabe der Einwilligung die Möglichkeit behält, die Kontrolle über seine Daten auszuüben. Zu diesem Zweck empfiehlt die DEK die Entwicklung und Ausgestaltung von Privacy Management Tools (PMT) und Personal Information Management Systems (PIMS) (→ unten) für den Forschungsbereich, wie z. B. **digitale Einwilligungsassistenten** oder Datenagenten. Derartige Einwilligungsassistenten können maßgeblich dazu beitragen, dass der Betroffene auch nach Beginn des Verarbeitungsprozesses den Überblick über seine Erklärungen behält, bei geänderter Sachlage erneut zur Abgabe entsprechender Erklärungen aufgefordert wird sowie auf einfache Weise seine Einwilligung widerrufen kann.

Insbesondere im Zusammenhang mit der Forschung an Gesundheitsdaten wird verstärkt die Förderung einer weitgehenden, unabhängig von einem konkreten Behandlungs- oder sonstigen Anlassfall erfolgenden Freigabe von Daten für die Forschung im Sinne einer pauschalen Einwilligung (**blanket consent**) diskutiert. Selbst wenn hierfür aus Sicht der Forschung gewichtige Gründe ins Feld geführt werden können, stehen diesem Konzept eine Reihe von Bedenken und Hindernissen gegenüber, darunter insbesondere das Erfordernis der Zweckbestimmtheit und der Informiertheit der Einwilligung. Selbst bei weitreichenden rechtlichen Absicherungen des Einwilligenden gegen missbräuchliche Verwendung seiner Daten und zum Schutz seiner Privatheit können seine Präferenzen und Werte nicht differenziert berücksichtigt werden.

Vor diesem Hintergrund empfiehlt die DEK die Prüfung eines innovativen Einwilligungsmodells, das als „**Meta-Consent**“ in der Diskussion ist.<sup>23</sup> Unabhängig von einem konkreten Anlass entscheidet der Datengeber nach Beratung, für welche Art von Forschungsvorhaben er in welchem Forschungskontext welche Art von Einwilligung (spezifische oder breite Einwilligung) geben möchte. So kann er etwa bezüglich der folgenden Aspekte seine Festlegungen treffen:

- Forschungskontext (z.B. private oder öffentliche Forschung, kommerzielle oder nicht-kommerzielle Forschung, nationale, europäische oder internationale Forschung);
- Datenquellen (z.B. elektronische Patientenakte, Gewebe, Gesundheitsdaten, Lifestyle-Daten von Wearables);
- Art der Forschung (z.B. Präventionsforschung, Forschung zu Krebserkrankungen oder neurodegenerativen Erkrankungen, jede Art der Gesundheitsforschung).

Wenn die Daten anschließend für ein konkretes Forschungsvorhaben genutzt werden sollen, wird der Datengeber hierüber vorab **informiert** und erhält die Möglichkeit, dieser konkreten Datennutzung zu **widersprechen**.

Die konkrete Umsetzung des Modells im Einzelfall sollte auf jeden Fall unter der **Kontrolle** durch einen Treuhänder, eine Ethik-Kommission oder eine andere zuständige Stelle erfolgen, so dass die tatsächliche Umsetzung der Präferenzen des Einwilligenden gewährleistet ist. Die in einem Meta-Consent von dem Betroffenen niedergelegten Festlegungen zu seiner Einwilligung können von ihm jederzeit geändert werden. Auch hierfür sind die technischen und regulatorischen Voraussetzungen zu gewährleisten.

#### Beispiel 13

*Der Datengeber legt fest, dass die Daten aus seiner elektronischen Patientenakte für öffentliche und kommerzielle Forschung genutzt werden dürfen. Zudem legt er fest, dass Blut- und Gewebeproben zur öffentlichen und kommerziellen Forschung zu degenerativen Erkrankungen genutzt werden dürfen. Seine Einwilligung beschränkt er bezüglich der Daten aus der elektronischen Patientenakte auf den europäischen Raum. Ein Unternehmen aus Spanien möchte sowohl Daten aus der elektronischen Patientenakte als auch Daten der Gewebeproben zur Demenzforschung nutzen. Hierüber wird der Datengeber informiert und erhält vier Wochen Zeit, der Datennutzung zu widersprechen.*

23 Thomas Ploug / Søren Holm: Bioethics, 2016 (30:9), S. 721, 721 ff.



Bei der Prüfung und Ausgestaltung des Modells ist zu berücksichtigen, dass die **Forschungsfreiheit** und das Weiterverarbeitungsprivileg im Vergleich zur geltenden Rechtslage nicht eingeschränkt wird. Vielmehr soll durch das Modell eines Meta-Consent betont werden, dass die Datengeber ihre **Werte und Präferenzen** im Hinblick auf die Verwendung ihrer Gesundheitsdaten für Forschungszwecke zum Ausdruck bringen können. Das würde zudem das Vertrauen der Gesellschaft in den Umgang mit Gesundheitsdaten stärken.

Es ist darüber hinaus zu bedenken, dass nicht nur die Nutzung, sondern auch die Nichtnutzung von Daten in ethischer Hinsicht zu verantworten ist, da so möglicher Fortschritt in wichtigen Bereichen verhindert wird. Zudem können ganz bestimmte **Gruppen vom Fortschritt ausgeschlossen** und damit diskriminiert werden. So können etwa für hochaltrige Personen mit mehreren chronischen Erkrankungen, die mehrere Medikamente gleichzeitig einnehmen, aus methodischen Gründen nur sehr eingeschränkt klinische Studien aufgesetzt werden. Durch eine qualitativ hochwertige Auswertung ihrer Gesundheitsdaten können aber wichtige Erkenntnisse über Wechselwirkungen zwischen Medikamenten und ihre Wirkung unter Alltagsbedingungen gewonnen und für eine weitergehende Forschung sowie die weitere Behandlung dieser Patienten fruchtbar gemacht werden.

Vor diesem Hintergrund und im Hinblick auf den auch im europäischen Kontext sowohl medizinisch als auch wirtschaftlich bedeutsamen Gesundheitssektor empfiehlt die DEK eine aktive **Förderung eines „lernenden Gesundheitssystems“**. In einem solchen System werden die Daten aus der alltäglichen Gesundheitsversorgung systematisch und qualitätsgestützt im Sinne der evidenzbasierten Medizin forschend genutzt, um mit den Ergebnissen die Versorgung kontinuierlich zu verbessern. Ein lernendes Gesundheitssystem bringt hohe Anforderungen an ein Mehrebenen-Governance-System mit sich und stellt den Patienten bzw. Versicherten ins Zentrum einer sektorenübergreifenden Gesundheitsversorgung.

#### 4.1.4 Rechtlicher Diskriminierungsschutz

Die DEK weist allerdings auch darauf hin, dass bei der Ausgestaltung und Konzeption neuer, gesundheitsbezogener Forschungsvorhaben das erhebliche **Diskriminierungspotenzial** sensibler Daten (z.B. auf dem Arbeitsmarkt oder beim Abschluss von Versicherungen) zu berücksichtigen ist. Sowohl der technische Fortschritt in der Sequenzierung und Auswertung des menschlichen Genoms als auch die Auswertung von alltäglich erhobenen biologischen und Verhaltensdaten ermöglichen die Ermittlung von Risikoprofilen für zukünftige Erkrankungen, wobei es sich in aller Regel um die Angabe von Wahrscheinlichkeiten handelt. Im Falle genetischer Daten kann dies auch Auswirkungen auf Angehörige haben.

Vor diesem Hintergrund sollte die Bundesregierung die **Aufnahme eines korrespondierenden Tatbestandes innerhalb des Allgemeinen Gleichbehandlungsgesetzes** (AGG) sowie darüber hinaus spezifische **Verwertungsverbote** von Informationen über die Gesundheit einer Person – wie sie für genetische Informationen schon im Gendiagnostikgesetz festgelegt sind – prüfen.

## 4.2 Anonymisierung, Pseudonymisierung und synthetische Daten

Jeder Zugang zu personenbezogenen Daten hat sich in den Grenzen des geltenden Datenschutzrechts zu bewegen und muss sich an den dort statuierten Anforderungen an eine Datenverarbeitung – vom Zweckbindungsgrundsatz bis hin zu angemessenen Schutzmaßnahmen – messen lassen. Es ist daher für ein Unternehmen oder andere Anwender gegebenenfalls von ausschlaggebender

Bedeutung, sicher sein zu können, sich entweder außerhalb des Anwendungsbereichs des Datenschutzrechts zu bewegen oder jedenfalls datenschutzkonform zu arbeiten. Einen Bedarf nach mehr **Rechtsicherheit** sieht die DEK dabei beispielsweise zu Fragen der Anonymisierung und Pseudonymisierung von Daten, zum Erkennen und Berücksichtigen des Personenbezugs von (vermeintlich anonymen) Datenbeständen und zu sog. synthetischen Daten.

### Anonymisierte und pseudonymisierte Daten

Bei der **Anonymisierung** handelt es sich um eine Verarbeitung, die aus einem Bestand personenbezogener Daten den Personenbezug unwiederbringlich entfernt. Man unterscheidet zwei Anonymisierungsansätze, die sich einzeln oder kombiniert verwenden lassen: die **Randomisierung** und die Generalisierung. Unter Randomisierung versteht man eine Veränderung der Daten derart, dass eine Zuordnbarkeit zwischen anonymisierten Daten und der betroffenen Person nicht mehr gegeben ist. Dies kann beispielsweise dadurch erreicht werden, dass einzelne Datensätze verfälscht werden. Bei geeigneter Gestaltung der Randomisierung bleiben die statistischen Eigenschaften des ursprünglichen Datenbestands erhalten, z.B. wenn Werte nur vertauscht und nicht verändert werden. **Generalisierung** bezeichnet eine Vergrößerung von Daten, beispielsweise durch Aggregation von detaillierten Einzelangaben wie Altersgruppen statt Geburtsdaten, Regionenbezeichnungen statt Postleitzahlen, Zeiträume statt sekundengenauem Zeitstempel.

Um einen Personenbezug in einem Datenbestand aufzufinden, sind drei Strategien wesentlich:

- a) **Herausgreifen** („singling out“): Darunter versteht man die Möglichkeit, aus einem Datenbestand Datensätze zu einzelnen Personen zu isolieren, beispielsweise mit Hilfe singulärer Merkmale, mit denen einzelne Personen identifiziert werden können;
- b) **Verknüpfbarkeit** („linkability“): Hiermit ist die Möglichkeit gemeint, mindestens zwei Datensätze, die dieselbe Person oder Personengruppe betreffen, mit Hilfe übereinstimmender Werte wie z.B. Kennungen, räumliche Koordinaten oder Zeitangaben zu verknüpfen. Diese Verknüpfung ermöglicht die Anreicherung der Daten zu derjenigen Person, zu der bislang weniger Daten vorhanden waren, und kann auf diese Weise zu einer Identifizierung dieser Person führen;
- c) **Inferenz** („inference“): Darunter versteht man die Möglichkeit, den Wert eines Merkmals mit einer signifikanten Wahrscheinlichkeit von den Werten einer Reihe anderer Merkmale abzuleiten. Eine solche Ableitung ermöglicht ebenfalls eine Anreicherung der Daten zu einer Person und erhöht die Wahrscheinlichkeit eines Personenbezugs.



Ein anonymisierter Datenbestand ermöglicht – bezogen auf den Zeitpunkt der Beurteilung und die technologischen Möglichkeiten, die nach allgemeinem Ermessen wahrscheinlich genutzt werden (vgl. Erwägungsgrund 26 zur DSGVO) – keine (Wieder-)Herstellung eines Personenbezugs (sog. De-Anonymisierung) und bietet einem Angreifer, der auf die (Wieder-)Herstellung des Personenbezugs von einzelnen oder allen betroffenen Personen zielt, keinen ausreichenden Ansatzpunkt.

Sorgt man durch Veränderungen des Datenbestands, insbesondere durch das künstliche Hinzufügen von Unschärfen (je nach Kontext auch „noise“ oder „blurring“ genannt), dafür, dass Datensätze zu einer Person nicht herausgegriffen werden können, dass auf Verketzungsermöglichte Daten verzichtet wird und dass keine Inferenzen gezogen werden können, beschränkt diese Veränderung in der Regel die Nutzbarkeit (sog. utility) der Daten. Sofern man die später gewünschten Auswertungen eines Datenbestands kennt, kann die Anonymisierung dafür optimiert werden, beispielsweise um den nötigen Detaillierungsgrad der Daten in den betroffenen Merkmalen nach Möglichkeit zu erhalten. Dasselbe gilt für den Vergleich verschiedener Datenbestände im Sinne einer Interoperabilität. Ist dieses Ziel bekannt, kann die Anonymisierung durch geeignete gleiche Gruppierungen und durch die Berücksichtigung möglicher Zusatzrisiken durch Informationen aus den weiteren Datenbeständen entsprechend gestaltet werden.

Bei der **Pseudonymisierung** lässt sich der resultierende Datenbestand ohne zusätzliche Informationen nicht mehr einer spezifischen betroffenen Person zuordnen. Diese zusätzlichen Informationen sind beispielsweise Zuordnungstabellen oder kryptographische Hash-Verfahren. Im Gegensatz zur Anonymisierung bleibt ein Personenbezug im Rechtssinne bestehen. Der Verantwortliche muss dafür Sorge tragen, dass diese zusätzlichen Informationen bei der weiteren Verarbeitung des pseudonymisierten Datenbestands besonders gegen einen (unberechtigten) Zugriff gesichert werden, da sich dadurch der Personenbezug herstellen lässt. Die DSGVO sieht die Pseudonymisierung als eine technisch-organisa-

tische Maßnahme zur Reduzierung des Risikos für die Rechte und Freiheiten natürlicher Personen und erwähnt sie an zahlreichen Stellen.

Anonymisierung und Pseudonymisierung sind jeweils Verarbeitungen von vorhandenen Daten. Davon abzugrenzen ist die **Verwendung von Pseudonymen** durch den Nutzenden. Dies kann durch bewusst selbstgewählte Kennungen (z. B. User-Namen bei Online-Diensten oder E-Mail-Adressen) geschehen; es können aber auch technisch berechnete Kennungen zum Einsatz kommen, z. B. bei der Online-ID-Funktion des elektronischen Personalausweises oder bei der Nutzung von datenschutzfördernden attributbasierten Berechtigungszertifikaten. Bei der Verwendung von Pseudonymen ist sehr häufig kein großer Schutz gegen das Herstellen eines Personenbezugs gegeben, insbesondere bei einem kontext- und kommunikationspartnerübergreifenden Einsatz, was eine Verketzung und Anreicherung von Daten in einem nutzerbezogenen Profil ermöglicht. Im Gegensatz dazu bieten ständig wechselnde und auf den jeweiligen Kontext beschränkte Transaktionspseudonyme einen größeren Schutz gegen eine Identifizierung.

Die Verfahren, die auf eine **Verschleierung des Personenbezugs** im Internet zielen, leisten zumeist keine wirkliche Anonymisierung, aber können dennoch zum Schutz gegen Identifizierung und Beobachtung beitragen. Simple Web-Proxy-Verfahren erlauben eine Nutzung des Internets mit der Kennung (hier: der IP-Adresse) eines zwischengeschalteten Servers, so dass für die angesurften Webserver die Zugriffe mehrerer Nutzender gleich aussehen, sofern diese nicht durch Cookies o.ä. weitere Identifikatoren mitsenden. Der Proxy-Server selbst hat in diesem Fall jedoch Kenntnis von den Kennungen der Nutzenden. In Verfahren mit einem größeren Schutz vor einer Identifizierung können solche Zwischenrechner hintereinander geschaltet werden, beispielsweise in Mix-Netzen wie Tor oder in Mix-Kaskaden wie JonDo. Auch hier kann durch eine zusätzliche Verrauschung mit künstlich erzeugtem „Dummy Traffic“ eine Beobachtung der menschlichen Nutzenden erschwert werden.

#### 4.2.1 Verfahren, Standards und Vermutungsregeln

Eine **Anonymisierung**, also die vollständige und nicht rückführbare Befreiung der Daten von jeglichem Personenbezug, unter Beibehaltung der maximalen Aussagekraft (utility) der Daten, ist vielfach faktisch ausgeschlossen. Sie ist allerdings auch oft nicht notwendig, da einerseits viele Zwecke bei genauerer Prüfung auch mit einer leicht geringeren Aussagekraft verfolgt werden können, andererseits bei der Verarbeitung im öffentlichen Interesse, zum Beispiel zum Zweck der Forschung, die DSGVO schon Ausnahmen vorsieht, die eine Verarbeitung auch von personenbezogenen Daten ohne Einwilligung erlauben. Gleichwohl gilt es, die Bemühungen um wirksame **Anonymisierungstechnologien und -verfahren** zu intensivieren, die eine Datenverarbeitung ganz außerhalb des Anwendungsbereichs der DSGVO ermöglichen.

Rechtssicherheit lässt sich letztlich nur im Wege der Entwicklung **standardisierter Technologien und Verfahren** gewährleisten, die gleichwohl stets die sich mit hoher Geschwindigkeit vollziehende technologische Entwicklung berücksichtigen müssen. Die DEK empfiehlt daher der Bundesregierung, im Interesse sowohl der betroffenen Personen als auch der Anwender insbesondere auf EU-Ebene auf die Entwicklung handhabbarer **Standards für Anonymisierung** zu dringen. Gleches gilt für **Pseudonymisierungsmaßnahmen**, die der Risikolage für die Privatsphäre angemessen sind und wie sie im Rahmen des Digital-Gipfels der Bundesregierung derzeit bereits erarbeitet werden.

Anonymisierungsstandards sollten insbesondere klare Regeln für eine **gesetzliche** widerlegliche **Vermutung** einschließen, die dem Anwender Rechtssicherheit vermitteln, nicht dem Anwendungsbereich der DSGVO unterworfen zu sein. Hierbei ist zu berücksichtigen, dass in diesen Vermutungsregeln gegebenenfalls Einschränkungen zu definieren sind, beispielsweise in der zeitlichen Gültigkeit, wie dies auch im Bereich kryptographischer Verfahren der Fall ist.<sup>24</sup> oder in den zugelassenen Verarbeitungsformen, z.B. dass keine Veröffentlichung oder Zugänglichmachung gegenüber einer unbestimmten Zahl von Personen erfolgen darf. Solange keine rechtlichen Grundlagen für widerlegliche Vermutungsregeln bestehen, sollte die Entwicklung von technischen **Best-Practice-Verfahren** und die Erarbeitung von branchenspezifischen **Selbstverpflichtungen** (Codes of Conduct) unterstützt werden, um Erfahrungen zu gewinnen.

Eine Standardisierung der Verfahren zur Anonymisierung und Pseudonymisierung kann darüber hinaus in bestimmten Bereichen Regeln zur Entfernung des Personenbezugs vorgeben, die eine Vergleichbarkeit von verschiedenen Datenbeständen ermöglichen und damit die **Interoperabilität** verbessern. Die DEK empfiehlt, zumindest in den Bereichen, in denen bessere Interoperabilität gewünscht ist, kontextspezifische Regeln für die zu wählenden Gruppierungen (wie z.B. Wertebereiche von Altersgruppen, Postleitzahlen, IP-Adressen) zu spezifizieren. Von den Statistikämtern wird dies in Bezug auf ihre Datenbestände bereits jetzt so gehandhabt.

24 Bundesamt für Sicherheit in der Informationstechnik: Technische Richtlinie BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen, letzte Version von Februar 2019 (abrufbar unter: [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?\\_\\_blob=publicationFile](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile)).

Verfahren der Anonymisierung und der Pseudonymisierung beziehen sich auf Datenbestände, deren Personenbezug bekannt ist oder zumindest vermutet wird. Davon abzugrenzen sind Datenbestände, in denen kein Personenbezug vermutet wird, aber die bereits einzeln oder in Kombination zumindest dazu beitragen können, dass sich ein Personenbezug in vermeintlich anonymen Daten herstellen lässt. Die DEK empfiehlt, dass auch hierfür **standardisierte Prüfmethoden des Personenbezugs** entwickelt und vorgegeben werden, die es dem Anwender ermöglichen, eine Personenbeziehbarkeit festzustellen oder in ausreichendem Maße auszuschließen.

#### 4.2.2 Verbot der De-Anonymisierung

Vermutungsregeln sollten allerdings durch angemessene **strafbewehrte Verbote der De-Anonymisierung** flankiert werden. Dies gilt für den Fall, dass bei bisher anonymen Daten, etwa durch die Entwicklung der Technik, ein Personenbezug hergestellt werden kann. Diese müssten so gefasst werden, dass die Forschung zum Erkennen und Entfernen eines Personenbezugs in Datenbeständen nicht behindert wird, denn zur Entwicklung von geeigneten Anonymisierungsstandards und zum Überprüfen ihrer Wirksamkeit ist es nötig, etwa bestehende Möglichkeiten der De-Anonymisierung weiter zu untersuchen. Auch dürfte die Einführung von strafbewehrten Verboten der De-Anonymisierung nicht dazu verleiten, die für eine Anonymisierung geltenden Standards herabzusetzen oder den Begriff der personenbezogenen Daten im Sinne der DSGVO zu verwässern. Andernfalls würden auch Wettbewerbsnachteile für diejenigen Akteure entstehen, die sich mit technischen Mitteln um eine Anonymisierung bemühen und diese wichtige Technologie weiterentwickeln. Das Gleiche gilt für die Aufhebung von Pseudonymisierung, sofern diese Aufhebung nicht durch einen zu definierenden Katalog von Gründen gerechtfertigt ist.

#### 4.2.3 Synthetische Daten

Von echten Daten abgrenzen sind **synthetische Daten**, d.h. Daten, die künstlich generiert und nicht unmittelbar in der realen Welt erhoben wurden. Sie haben mehrere Vorteile gegenüber echten Daten.<sup>25</sup> Erstens lassen sich synthetische Daten in beliebiger Menge produzieren. Dies ist besonders wichtig für Simulationen, da echte Daten hier noch gar nicht angefallen sein können. Zweitens kann bei der Erzeugung synthetischer Daten dafür gesorgt werden, dass das gesamte Wertespektrum möglichst vollständig abgebildet wird, z.B. um das Verhalten eines technischen Systems bei ungewöhnlichen Datenkonstellationen zu testen. Drittens ist die Qualität von synthetischen Daten messbar. Je nach Bedarf im Einzelfall kann gewährleistet werden, dass die Eigenschaften eines Referenzdatenbestands aus der realen Welt erhalten bleiben, oder es lassen sich gezielt Verzerrungen, die in Echtbeständen vorkommen können, zur Vermeidung von Diskriminierungen herausnehmen. Solange der synthetische Datenbestand keinen Personenbezug aufweist, ist er anonym, und die DSGVO ist nicht anwendbar.

Die DEK empfiehlt der Bundesregierung, die **Forschung im Bereich synthetischer Daten zu fördern**. Dabei besteht u.a. Forschungsbedarf zu der Frage, inwieweit und in welchen Kontexten synthetische Daten die Verarbeitung echter Daten ersetzen können und wie eng die synthetischen Daten an die Eigenschaften von echten Daten angelehnt sein sollen. Die DEK empfiehlt, die Erzeugung und den Einsatz synthetischer Daten weiter zu untersuchen, beispielsweise im Hinblick auf ihre Datenqualität und auf die Vermeidung von Verzerrungen (Bias) und Diskriminierung.

25 Jörg Drechsler / Nicola Jentzsch: Synthetische Daten: Innovationspotenzial und gesellschaftliche Herausforderungen, Stiftung Neue Verantwortung, 2018 (abrufbar unter: [https://www.stiftung-nv.de/sites/default/files/synthetische\\_daten.pdf](https://www.stiftung-nv.de/sites/default/files/synthetische_daten.pdf)).

## 4.3 Kontrollierter Datenzugang durch Datenmanagement- und Datentreuhandsysteme

### 4.3.1 Privacy Management Tools (PMT) und Personal Information Management Systems (PIMS)

Defizite in der Befähigung zur Wahrnehmung von Datenrechten werden vor allem in Bezug auf die **Kontrolle Einzelner über ihre personenbezogenen Daten** in einer zunehmend komplexer werdenden Umgebung gesehen. In der Regel verfügen betroffene Personen etwa über keine Dokumentation erteilter Einwilligungen. Das Teilen von Daten durch den ursprünglich Verantwortlichen kann zudem zu einer Streuung führen, die für betroffene Personen die bestehenden Intransparenzen und damit verbundenen Datenschutzrisiken noch deutlich erhöht (→ siehe zum Problem des Datenhandels oben). Es fehlt derzeit an hinreichenden Standards und Softwarewerkzeugen, mithilfe derer betroffene Personen etwaige Datenzugangsbeteiligungen und Datenweitergaben fortlaufend nachverfolgen und steuern und damit ihre Datenrechte effektiv wahrnehmen können.

Zur Lösung des Problems werden verstärkt technische und institutionelle Maßnahmen vorgeschlagen. Dazu gehören diverse sog. **Privacy Management Tools (PMT)**, die von Applikationen zur Erleichterung der nutzerseitigen Einwilligungsverwaltung (Dashboards etc.) bis hin zu KI-Tools, die individuelle Nutzerpräferenzen automatisch umsetzen („Datenagenten“), rangieren. Stehen nicht die Herstellung und der Support technischer Applikationen im Vordergrund, sondern Dienstleistungen, wird eher von **Personal Information Management Systems (PIMS)** gesprochen. Sie können von Single-Sign-On-Diensten über lokale Datensafes und Online-Speichersysteme bis zu mehr oder weniger umfassender Fremdverwaltung von Daten der Nutzenden (sog. Datentreuhand-Modelle) reichen. In der zuletzt genannten Variante können PIMS

die digitale Selbstbestimmung unterstützen, indem sie die Ausübung von datenschutzrechtlichen Betroffenenrechten, wie das Erteilen und Widerrufen von Einwilligungen und die Wahrnehmung der Rechte auf Auskunft, Berichtigung, Löschung, Datenübertragbarkeit und Widerspruch teilweise für den Betroffenen übernehmen. Die DEK empfiehlt der Bundesregierung die **Förderung** von Innovationen und Standardisierungen für derartige Softwarewerkzeuge und Dienstleistungen.

### 4.3.2 Bedarf nach Regulierung von PMT/PIMS

Allerdings können von PMT/PIMS auch **Gefahren** ausgehen, wenn sie bestimmten, teilweise auch über die DSGVO hinausgehenden Anforderungen nicht genügen. So besteht bei fehlerhafter Ausgestaltung von PMT/PIMS die Gefahr, dass statt der Ermöglichung echter Selbstbestimmung betroffene Personen auf einen Weg der unbewussten oder sorglosen **Fremdbestimmung** geführt werden. Insbesondere würde es dem ethischen Wert der Selbstbestimmung letztlich widersprechen, wenn PMT/PIMS so ausgestaltet werden, dass Entscheidungen weitgehend (z.B. durch Blankomandate) von betroffenen Personen an die Betreiber von PMT/PIMS abgegeben oder Entscheidungen betroffener Personen durch diese interessengünstig beeinflusst werden. PMT/PIMS müssen den betroffenen Personen als Hilfsmittel dienen, dürfen deren selbstbestimmte Entscheidungshoheit jedoch nicht ersetzen oder diese gar durch sog. Dark Patterns o.ä. (→ oben 3.2.2.) manipulieren.



Aufgrund der erhöhten Grundrechtsrelevanz und der fehlenden Möglichkeiten einer Qualitätskontrolle durch den Betroffenen selbst empfiehlt die DEK der Bundesregierung die Erarbeitung von **Qualitätsstandards für PMT/PIMS und die Einführung eines Zertifizierungs- und Überwachungssystems**. Letzteres sollte insbesondere für Systeme gelten, die im Namen der betroffenen Personen bzw. an ihrer Stelle agieren oder durch ihre technische Gestaltung die Entscheidungen der betroffenen Personen wesentlich steuern und kanalisierten. Sofern Daten unmittelbar durch die Betreiber von PMT/PIMS gespeichert werden (im Gegensatz zur ebenso möglichen dezentralen Speicherung und bloßen Verwaltung), bedarf es auch Vorrangungen für den Fall der Insolvenz oder Auflösung.

PMT/PIMS können nur dann verlässlich arbeiten, wenn eine Kooperation mit allen betroffenen Verantwortlichen sichergestellt ist. Dabei ist eine hinreichende Breitenwirkung nur durch eine – unter sachgerechten Bedingungen stehende – **rechtliche Verpflichtung** für Verantwortliche im Sinne der DSGVO zu erreichen, die Kontrolle des Zugangs zu personenbezogenen Daten durch PMT/PIMS zu ermöglichen und beispielsweise sicherzustellen, dass jede datenschutzrelevante Information das PMT/PIMS erreicht und das PMT/PIMS in Bezug auf alle personenbezogenen Daten die Interessen der betroffenen Person wahrnehmen kann. Realistisch erscheint dabei zunächst ein **sektorspezifisches Vorgehen**, welches etwa für soziale Netzwerke zu erwägen ist.

Nach Ansicht der DEK kann der Betrieb derartiger Systeme entweder ohne Erwerbsabsicht, etwa durch **gemeinwohlorientierte Stiftungen** und ähnliche unabhängige Stellen und ohne jede Beteiligung von kommerziell motivierten Akteuren erfolgen, oder **privatwirtschaftlich** organisiert sein, wenn dabei der Betreiber an der Verwaltung, und nicht an der Nutzung der Daten verdient. In jedem Fall ist es notwendig, die besonderen Treuepflichten gegenüber der betroffenen Person gesetzlich präzise zu fassen, Akteure mit konfliktierenden Interessen auszuschließen und insgesamt entsprechende Kontrollmöglichkeiten – etwa auch zur Minimierung von Bias und Diskriminierung – einzubauen. Bei den privatwirtschaftlichen Modellen muss auch sichergestellt werden, dass eine Unterminierung der Funktion als Interessenwalter der betroffenen Person bei einer Erwerbsabsicht ausgeschlossen ist. Betreiber, die Zugriff auf personenbezogene Daten erhalten, müssen ihren Sitz in der Europäischen Union haben.

Die DEK empfiehlt der Bundesregierung, auf eine entsprechende **Ergänzung der DSGVO** hinzuwirken, die einen konkretisierenden und rechtssicheren Rahmen für PMT/PIMS vorgibt. Über rechtliche Fragen zu Mandaten usw. hinaus ist einer übermäßigen zentralen Speicherung personenbezogener Daten entgegenzuwirken, die z.B. im Fall von Cyberangriffen Risiken für die Betroffenen erhöhen würde. Für eine automatisierte Realisierung der Dienste sind maschineninterpretierbare Formate und Kommunikationsprotokolle zu standardisieren.

### 4.3.3 PMT/PIMS als mögliche Schnittstelle zur Datenwirtschaft

Bei entsprechender Regulierung könnten PMT/PIMS auch doppelfunktional tätig werden. So könnte einerseits der Einzelne mit Hilfe von PMT/PIMS sein Recht auf informationelle Selbstbestimmung wirksam ausüben und Zweckbegrenzungen zuverlässig überprüfen, andererseits könnten aber auch – insbesondere unter Nutzung des Portabilitätsrechts aus Art. 20 DSGVO – Daten aus „Datenilos“ geholt und für die europäische Datenwirtschaft freigesetzt werden. Der Grundgedanke von PMT/PIMS betrifft zwar zunächst nur die Verbesserung von Kontrolle des Einzelnen über seine personenbezogenen Daten. Dies beinhaltet an sich nicht, Datenzugang durch Dritte zu fördern. Eine mittelbare Datenzugangsfunktion wäre mit dem **Gedanken der treuhänderischen Verwaltung** aber dann zu vereinbaren, wenn sich der Datenzugang durch Dritte entweder als vom Betroffenen gewollte Datenfreigabe zur Förderung bestimmter Zwecke darstellt (→ etwa im Forschungskontext, oben ) oder aber der wirtschaftlichen Verwertung der Daten im Interesse des Betroffenen dient und mit seiner ausdrücklichen Zustimmung erfolgt (→ zur Problematik der Ökonomisierung personenbezogener Daten, oben ).

Sofern man eine zusätzliche Funktion von PMT/PIMS als Plattform für den rechtssicheren Datenzugang für Unternehmen anerkennen will, muss nach Auffassung der DEK sichergestellt werden, dass diese qualifizierten PMT/PIMS die Schutzfunktion der Betroffenenrechte nicht letztlich in ihr Gegenteil verkehren. Es bedarf der strengen Einhaltung der Grundsätze von Privacy und Ethics by Design. Insbesondere darf der Zweck nicht auf die möglichst weitgehende Datenverwertung und -streuung ausgerichtet sein. Die DEK betont, dass PMT/PIMS nicht ihre Funktion als eindeutige Interessenwälter der Betroffenen verlieren dürfen und ein **Interessenkonflikt ausgeschlossen** werden muss.



## 4.4 Datenzugang durch Datenportabilität

### 4.4.1 Förderung von Datenportabilität

Das Portabilitätsrecht in Art. 20 DSGVO (**Recht auf Datenübertragbarkeit**) stellt ein Instrument für den Betroffenen dar, in Bezug auf personenbezogene Daten, die der Betroffene einmal einem Unternehmen bereitgestellt hat, selbstbestimmt zu entscheiden, welche weiteren Unternehmen Zugang zu diesen Daten erhalten sollten. Es umfasst das Recht, die bereitgestellten Daten in einem „strukturierten, gängigen und maschinenlesbaren Format“ zu erhalten oder einem anderen Verantwortlichen direkt übermitteln zu lassen. Datenportabilität wirkt vor allem in zwei Richtungen:

- a) Bei einem Anbieterwechsel verhindert das Portabilitätsrecht unerwünschte Lock-in-Effekte und schützt damit sowohl den einzelnen Betroffenen in seiner wirtschaftlichen Dispositionsfreiheit als auch den freien Wettbewerb.
- b) Unabhängig von einem Anbieterwechsel erlaubt das Portabilitätsrecht dem Betroffenen, seine Daten von einem Verantwortlichen heraus zu verlangen und anderen Unternehmen zur Verfügung zu stellen. Diese anderen Unternehmen erlangen dadurch – sofern sie zugleich eine eigene datenschutzrechtliche Rechtsgrundlage (z.B. Einwilligung oder Vertrag) für die Verarbeitung haben<sup>26</sup> – einen Datenzugang, den sie auf anderem Wege möglicherweise nicht erlangt hätten.

Die Anforderungen an ein „strukturiertes, gängiges und maschinenlesbares Format“ werden in der Praxis bislang noch sehr unterschiedlich und uneinheitlich ausgelegt, obwohl sie Grundvoraussetzung für eine wirkungsvolle Ausübung des Portabilitätsrechts sind. Daher empfiehlt die DEK der Bundesregierung und den Datenschutzbehörden, in Anlehnung an Erwägungsgrund 68 zur DSGVO auf europäischer Ebene die Entwicklung **branchenbezogener Verhaltensregeln und Standards** zu unterstützen, damit Datenübertragbarkeit im Interesse aller Beteiligten einheitlich und praktisch wirkungsvoll umgesetzt werden kann.

Ohne Hinzutreten neuer Intermediäre (→ oben 4.3) dürfte die Anregung zur Ausübung des Portabilitätsrechts oft durch das Unternehmen, das einen neuen Kunden gewonnen hat, erfolgen. Dabei werden diejenigen Unternehmen besonders erfolgreich sein, die eine bequeme und automatisierte Ausübung des Portabilitätsrechts ermöglichen (z.B. Anbieter eines Kartendienstes ermöglicht per Klick das Portieren von Daten eines Mobilitätsdienstleisters). Aufgrund von Netzwerk- und Skaleneffekten besteht Grund zur Annahme, dass – zumindest mittelfristig – gerade daten- und marktmächtige Unternehmen die größten Profiteure des Portabilitätsrechts sein könnten. Der Bundesregierung wird daher empfohlen, die Entwicklungen **aufmerksam zu beobachten** und, soweit erforderlich, auf europäischer Ebene auf Maßnahmen zu dringen, die eine erleichterte Portabilität für die betroffenen Personen speziell von daten- und marktmächtigen Unternehmen zu anderen Marktteilnehmern, einschließlich Start-ups, fördern.

<sup>26</sup> Zum Erfordernis einer derartigen eigenen datenschutzrechtlichen Rechtsgrundlage siehe etwa Art. 29-Datenschutzgruppe: Leitlinien zum Recht auf Datenübertragbarkeit, WP 242, rev. 01, S. 7 f.

#### 4.4.2 Erweiterung des Portabilitätsrechts?

Derzeit wird eine Erweiterung des Portabilitätsrechts in verschiedener Hinsicht diskutiert, insbesondere was die Erweiterung auf andere als bereitgestellte (Roh-)Daten (z.B. auf bestimmte veredelte bzw. abgeleitete Daten) sowie ein Recht auf dynamische Echtzeit-Portabilität (d.h. Echtzeit-Streaming von Datenflüssen) betrifft. Die DEK legt der Bundesregierung im Sinne der soeben formulierten Empfehlung nahe, **derzeit auf keine rechtliche Änderung zur Erweiterung des bestehenden Portabilitätsrechts zu dringen**, da seine praktische Anwendung, die Aufsichtspraxis der Datenschutzbehörden und auch die Auslegung der DSGVO durch Gerichte so kurze Zeit nach Wirksamkeit des neuen Rechts zunächst abgewartet werden sollte.

#### 4.4.3 Von Portabilität zu Interoperabilität und Interkonnektivität

Aufgrund von Netzwerkeffekten (z.B. bei Messenger-Diensten) dürfte die Datenportabilität allein nicht ausreichen, entstandenen und drohenden Daten- und Service-Oligopolen entgegenzuwirken und die Markteintrittshürden für neue Wettbewerber soweit zu senken, dass dominante Anbieter ernsthaft herausgefordert werden. Die DEK empfiehlt der Bundesregierung daher, auf die Einführung **sektorspezifischer Pflichten zur Interoperabilität** hinzuwirken, wie dies z.B. auch früher bei Postdienstleistungen und im Mobilfunk realisiert wurde. Dabei muss eine datenschutzkonforme Gestaltung der Interoperabilität einschließlich datenschutzfreundlicher Voreinstellungen gewährleistet sein, beispielsweise durch die Möglichkeit der Verwendung unterschiedlicher und wechselnder Kennungen statt nur eines übergreifenden Identifikators, durch Reduktion der Datensammelmöglichkeiten an zentralen Komponenten oder durch sonstige geeignete Realisierung auf verschiedenen Schichten im interoperablen technischen Zusammenwirken.

Diese Interoperabilitätsverpflichtungen könnten **asymmetrisch zwischen marktmächtigen Unternehmen und neuen Marktteilnehmern ausgestaltet** werden (z.B. wäre dann ein marktmächtiger Anbieter von Messenger-Diensten verpflichtet, den Kunden kleinerer Anbieter das unmittelbare Versenden von Nachrichten an seine Kunden und umgekehrt das Empfangen von deren Nachrichten zu ermöglichen). Jedenfalls ist dafür Sorge zu tragen, dass nicht über die Interoperabilitätsanforderungen ein umso stärkerer Fluss personenbezogener Daten hin zu daten- und marktmächtigen Unternehmen entsteht. Sofern dies gewährleistet werden kann, wäre es sinnvoll, etwa eine **Interkonnektivitätsverpflichtung für Kurznachrichtendienste und soziale Netzwerke** vorzusehen, um so den Konzentrationseffekten der Netzwerke entgegen zu wirken und dem Ziel der Datenportabilität, nämlich Wettbewerb und Markteintritt in der datenintensiven Wirtschaft zu fördern, noch intensiver zu dienen. Dies wäre auch eine Voraussetzung dafür, im Sinne der digitalen Souveränität Deutschlands bzw. Europas bestimmte Basisdienstleistungen der Informationsgesellschaft in Europa neu aufzubauen bzw. zu stärken.



#### 4.5 Crowd Sensing zu gemeinwohlorientierten Zwecken

Auch das sog. Crowd Sensing will neue Datenressourcen für Datengesellschaft und Datenwirtschaft erschließen und verwendet dazu die technischen Geräte der Nutzenden als Sensoren. Diese erheben etwa in einem bestimmten Ortsbereich Daten und leiten sie an eine übergeordnete Instanz weiter, die die gesammelten Daten auswertet. Die DEK sieht die Potenziale, die diese Technologie mit sich bringen kann, insbesondere sofern ihr **Einsatz gemeinwohlorientierten Zwecken** dient. So kann Crowd Sensing beispielsweise in der Smart City für Echtzeit-Analysen der Verkehrslage, des Zustands der Infrastrukturen, der Luftqualität etc. genutzt werden. Zugleich sieht die DEK aber erhebliche Herausforderungen für eine ethisch angemessene Ausgestaltung. Denn die durch Crowd Sensing ermöglichten Analysen weisen typischerweise eine extrem hohe Granularität auf und können daher aus Sicht derjenigen, die die Daten besteuern, sowie gegebenenfalls auch für Personen in ihrer Umgebung überaus sensibel sein. Um eine unerwünschte Rückführbarkeit auf die Nutzenden sowie möglicherweise betroffene weitere Personen auszuschließen oder anderweitigen Missbrauch zu vermeiden, bedarf es daher auch hier verstärkter Bemühungen um **Standards der Anonymisierung und Pseudonymisierung** (→ oben 4.2). Hinzu kommt, dass die im Zuge von Crowd Sensing getätigten Datenübertragungen die Ressourcen der Geräte der Nutzenden beeinträchtigen können und Sicherheitsfragen auftreten (→ unten Teil F, 8.3).

Diese Gesichtspunkte sind auch zu beachten, wenn sich die Nutzenden freiwillig und bewusst an Crowd-Sensing-Programmen beteiligen (sog. Participatory Sensing). Insoweit ist an die **materiellen Schranken der Einwilligung** zu erinnern (→ oben 3.2). Insgesamt muss auch beim Einsatz zu gemeinwohlorientierten Zwecken stets sichergestellt sein, dass die rechtlichen Vorgaben, insbesondere des Datenschutz- und des Verbraucherschutzrechts, volumnäßig gewahrt bleiben. In diesem Fall ist ferner zu berücksichtigen, dass staatliche Entscheidungen und Maßnahmen regelmäßig nicht allein auf mittels Participatory Sensing gesammelte Daten gestützt werden dürfen, denn diese Daten sind durch die Freiwilligkeit der Teilnahme zwangsläufig **unvollständig und wahrscheinlich verzerrt**.

Sofern erörtert wird, ob personenbezogene Daten im Wege des Crowd Sensing ohne Kenntnis der Nutzenden erhoben, weitergeleitet und gesammelt werden dürfen (sog. Opportunistic Sensing), verstößt dies aus Sicht der DEK potenziell gegen elementare Grundsätze des Datenschutzes. Ob sich ein **gesetzlicher Zwang** zur Bereitstellung der eigenen technischen Geräte für die automatische Erhebung und Weiterleitung von Daten rechtfertigen lässt, wenn und soweit deren Analyse wichtigen Interessen des Gemeinwohls dienen kann, kann aus Sicht der DEK nur im konkreten Einzelfall entschieden werden.

# Zusammenfassung der wichtigsten Handlungsempfehlungen

## Verbesserung des kontrollierten Zugangs zu personenbezogenen Daten

**16**

Die DEK sieht in einer Datennutzung für gemeinwohl-orientierte 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 Einwilligungs-assistenten 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 wahrnehmende 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.

## 5. Datenzugangsdebatten jenseits des Personenbezugs

Der Datenwirtschaft kommt für die künftige Wettbewerbsfähigkeit deutscher und europäischer Unternehmen eine Schlüsselrolle zu. Die zunehmende Verbreitung des Internet of Things (IoT) und des Internet of Services (IoS) hat zu einer wachsenden industriellen Bedeutung von Daten geführt, die durch Sensorik automatisch erhoben werden und zur Entwicklung neuer Geschäftsmodelle und Innovationen beitragen können. **Deutschlands Stärke** in vielen IoT/IoS-relevanten Technologien (z.B. Sensortechnologie, Maschinenbau, eingebettete Systeme) und allgemein in der industriellen Produktion, nebst den verbundenen industrienahen digitalen Dienstleistungen, bedeutet hier eine günstige Startposition, die dazu genutzt werden muss, den Wohlstand in Zeiten zunehmenden weltweiten Wettbewerbs zu sichern. Deutschland verfügt mit seiner differenzierten und leistungsfähigen Forschungslandschaft, seiner breit aufgestellten Wirtschaftsstruktur und seiner Technologieführerschaft in wichtigen Industriefeldern, wie der Industrie 4.0, über eine ausgezeichnete Ausgangslage, um die mit der Datenwirtschaft verbundenen Potenziale für die Wertschöpfung der Zukunft zu nutzen.

### 5.1 Gesamtwirtschaftliche Bedeutung eines angemessenen Datenzugangs

Die DEK sieht einen wesentlichen Faktor zur Gewährleistung einer marktgerechten und gemeinwohlorientierten Datenwirtschaft und zur Stärkung der digitalen Souveränität Deutschlands und Europas in einem angemessenen Datenzugang deutscher und europäischer Unternehmen und in der Auflösung bestehender Abhängigkeiten von wenigen Datenoligarchen. Dabei bedeutet Datenzugang im engeren Sinne zunächst die Frage, inwieweit für ein bestimmtes Geschäftsmodell oder sonstiges Vorhaben erforderliche Daten **faktisch und rechtlich genutzt werden können**. Datenzugang im engeren Sinne nutzt nur Akteuren, die auch über entsprechendes **Bewusstsein über die Bedeutung von Daten** und 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 anderen Faktoren gemäß dem **ASISA-Prinzip** (Awareness – Skills – Infrastructures – Stocks – Access) zu berücksichtigen.

Der Schwerpunkt der Betrachtung liegt in diesem Abschnitt auf nicht-personenbezogenen Daten. Das Potenzial **genuin nicht-personenbezogener Daten** für Wissenschaft, Wirtschaft und Gesellschaft ist hoch und wird oft unterschätzt. Ein Großteil der Wissenschaftsdaten – angefangen bei den Daten der technischen Wissenschaften (z.B. Ingenieur- und Materialwissenschaften) und der Physik (z.B. die Daten der Teilchenbeschleuniger), über die Daten der Biologie (z.B. Pflanzen- und Tierreich), der Geologie und der Chemie, über Umweltdaten, Wetterdaten und Meeresdaten bis hin zu Wirtschaftsdaten (z.B. Daten der Finanzmärkte) – sind nicht-personenbezogen. Sie haben aber einen großen Wert für Wissenschaft, Wirtschaft und Gesellschaft, wenn sie u.a. mit Big Data-Methoden analysiert und zur Entwicklung von Künstlicher Intelligenz (KI) verwendet werden. Dies sollte gezielt gefördert und der Zugang zur Nutzung solcher Daten sollte systematisch erleichtert werden.

Aufgrund der Weite des Begriffs der personenbezogenen Daten unter der DSGVO ist allerdings auch davon auszugehen, dass ein nicht unerheblicher Teil der Datenbestände gemischter Natur ist und auch Daten beinhaltet, die personenbezogen sind oder werden können. Auch sind bestimmte, dem Einzelnen durchaus nützliche oder gemeinwohlorientierte Aktivitäten der Datenwirtschaft nicht ohne Verarbeitung personenbezogener Daten möglich. Daher erscheint es wenig sinnvoll, im Zusammenhang mit Datenzugang ausschließlich nicht-personenbezogene Daten zu betrachten. Ein sachgerechter Ansatz dürfte vielmehr in einem **allgemeinen Datenzugangsregime** liegen, das nur insoweit, als personenbezogene Daten betroffen sind, **vom Datenschutzrecht überlagert** wird, d.h. datenwirtschaftliche Aktivitäten müssen sich dann zwingend im Rahmen der DSGVO bewegen. Zu betonen ist jedoch, dass die DSGVO bereits heute in vielfacher Weise die wirtschaftliche Verwertung personenbezogener Daten erlaubt. So treten neben die Einwilligung (Art. 6 Abs. 1 lit. a DSGVO) fünf weitere Rechtfertigungstatbestände (Art. 6 Abs. 1 lit. b–f), die teils explizit auf wirtschaftliche Interessen und Bedürfnisse zugeschnitten sind.



## 5.2 Schaffung der erforderlichen Rahmenbedingungen

### 5.2.1 Bewusstseinsbildung und Datenkompetenz

Die werteorientierte Nutzung von Daten setzt zunächst bei den Akteuren – ob privat- oder gemeinwohlorientiert – ein hinreichendes Bewusstsein für die bestehenden Möglichkeiten und Risiken sowie hinreichende Datenkompetenz – u.a. in technischer, ökonomischer, ethischer und rechtlicher Hinsicht – voraus (→ oben, Teil D, 3.). Bei deutschen **Unternehmen** besteht bislang teilweise noch ungenutztes Potenzial, die eigenen Datenbestände und Datenströme produktiver und gegebenenfalls gemeinwohlorientierter einzusetzen. Die DEK begrüßt Maßnahmen zur Bewusstseinsbildung und zur Förderung digitaler Kompetenzen seitens diverser Akteure (z.B. der Industrie- und Handelskammern, Verbände oder auch berufsbildende Einrichtungen). Es bedarf einer Verbesserung der werteorientierten Datenkompetenz auf breiter Ebene, was etwa durch entsprechende **Bildungs- und Weiterbildungssangebote** erreicht werden kann. Diese müssen stets auch Sensibilität betreffend datenschutzwichtiger und ethischer Risiken für das Individuum und die Gesellschaft schaffen.

**Staatliche Stellen** erkennen erst langsam die Bedeutung und Implikationen der von ihnen bereits heute im großen Umfang, etwa zu Zwecken der Statistik, generierten Daten sowie die Vorteile und Risiken, die der Austausch von staatlichen Daten gegenüber Privaten (sog. Government-to-Business Data Sharing, G2B) oder von Betriebsdaten gegenüber staatlichen Stellen (sog. Business-to-Government Data Sharing, B2G), bieten. Angesichts der bisher eher zurückhaltend genutzten Möglichkeiten ist insoweit auf einen weiteren Wandel der Verwaltungskultur hinzuwirken, wie sie etwa bei eGovernment-Vorreitern wie z.B. den skandinavischen Ländern oder Estland zu finden sind. Die DEK empfiehlt der Bundesregierung zusätzlich, entsprechende Aktivitäten einschlägiger Forschungsinstitutionen zu stärken.

### 5.2.2 Förderung der Infrastrukturen für eine datenbasierte Ökonomie

Deutschland nimmt zwar nach wie vor eine Spitzenposition in der wissenschaftlichen Technologieforschung ein, jedoch sind es derzeit vor allem amerikanische und zunehmend auch chinesische Technologieunternehmen, die wichtige Daten- und Analyseinfrastrukturen für die neue digitale Wirtschaft bereitstellen. Daher liegen viele europäische Daten – sowohl Konsumentendaten als auch Unternehmens- und Forschungsdaten – außerhalb Europas und werden durch Software nichteuropäischer Unternehmen in Drittländern analysiert. Der Entwicklung **eigener Infrastrukturen** für eine datenbasierte Ökonomie kommt daher eine herausgehobene Rolle zu.

Die DEK empfiehlt der Bundesregierung, die folgenden, von der Europäischen Kommission angestoßenen **Maßnahmen auf europäischer Ebene** zu unterstützen:

- Einrichtung und weiterer Ausbau des Unterstützungszentrums für die gemeinsame Datennutzung;
- Erarbeitung von Modellverträgen für die Datenwirtschaft;
- Förderung von Foren und Konsortien zur Entwicklung von offenen Standards für einen rechtssicheren Datenaustausch, insbesondere von für den Datenaustausch geeigneter Formate und Programmierschnittstellen (APIs) und für die Rückverfolgbarkeit von Datenflüssen;
- Förderung von europäischen Plattformen für den rechtssicheren Datenaustausch und
- Einrichtung einer European Open Science Cloud (EOSC).

Als wichtige Voraussetzung für die digitale Souveränität Deutschlands ist die **Zugangskontrolle** für sensible Daten und die Möglichkeit einer ausreichenden **Überprüfung** kritischer Datenanalysesoftware, beispielsweise anhand der Offenlegung von Quellcode und Designkriterien, anzusehen. In geographischer Hinsicht sollte die Durchführung von ethisch sensiblen Analysen daher nach Möglichkeit in unserem Rechtsraum stattfinden.

Die DEK begrüßt ausdrücklich eine Reihe von Initiativen der Bundesregierung und anderer Akteure, die darauf gerichtet sind, von Deutschland aus sichere internationale Datenräume für verschiedene Anwendungsdomänen zu schaffen, und die Unternehmen und Organisationen verschiedener Branchen und aller Größen die souveräne Bewirtschaftung und den geregelten Austausch ihrer Datenbestände untereinander ermöglichen.

Zur Unterstützung bei der Aushandlung von Datenzugangsvereinbarungen in schwierigen Fällen und zur Vermittlung bei Streitigkeiten ist ferner die Einrichtung einer **Ombudsstelle** auf Bundesebene empfehlenswert. Soweit personenbezogene Daten betroffen sind, sollte diese die zuständigen Datenschutzbehörden beteiligen, wobei zur Vermeidung divergierender Entscheidungen die Entscheidungshoheit letztlich bei den Datenschutzbehörden liegen müsste.

## Aufbau von Dateninfrastrukturen

Zu den **Initiativen der Bundesregierung** betreffend den Aufbau von Dateninfrastrukturen gehören:

- a) Die Bemühungen der DFG zum Aufbau einer Nationalen Forschungsdateninfrastruktur (NFDI). In der NFDI sollen Datenbestände in einem aus der Wissenschaft getriebenen Prozess systematisch erschlossen, langfristig gesichert und über Disziplinen- und Ländergrenzen hinaus zugänglich gemacht werden;
- b) Das vom BMBF geförderte, offene Konsortium International Data Spaces (IDS, vormals Industrial Data Space). Es stellt für die teilnehmenden Unternehmen und Organisationen eine standardisierte Schnittstelle zu einer Datenaustauschplattform dar, die einem föderalen Architekturkonzept folgt;
- c) Die Initiative zum Aufbau eines großen Netzwerkes von Big Data- und KI-Zentren mit über ganz Deutschland verteilten Knoten im Sinne eines nationalen, allgemein zugänglichen Ökosystems. Dieses Netzwerk kann nicht nur eine große Vielzahl und Vielfalt an Daten kontinuierlich bereitstellen, sondern bietet gleichzeitig Werkzeuge der gesamten Datenwertschöpfungskette (Aufbereitung, Analyse, Visualisierung, Verwertung) einfach nutzbar an und entwickelt sie aufgrund der Erfahrung bei deren Nutzung stetig weiter.

Neben diesen technischen Plattformen sind auch die von der Bundesregierung gemeinsam mit Verbänden aufgesetzten Plattformen zur Förderung der koordinierten Forschung und Entwicklung sowie der Standardisierung und praktischen Umsetzung von datenintensiven Anwendungen in Form von gesellschaftlich und wirtschaftlich innovativen Zukunftsprojekten zu nennen, wie etwa die Plattformen Industrie 4.0, Smart Service Welt und Lernende Systeme.

Auf europäischer Ebene führt die **Europäische Kommission** vergleichbare Projekte durch (z. B. das Zukunftsprojekt FIWARE). Sie entwickelt derzeit einen kostenlos verfügbaren Baukasten von Open-Source-Softwarekomponenten, mit denen sich innovative Internetdienste rasch konfigurieren lassen. Die Big Data Value-Public-Private-Partnership (BDVA) hat auf europäischer Ebene ein interoperables und datengetriebenes Ökosystem für neue Geschäftsmodelle auf der Basis von Massendaten mit vielen Leuchtturmprojekten hervorgebracht. Auch im Rahmen des European Institute of Innovation and Technology (EIT Digital) ist europaweit ein technisch-wirtschaftliches Ökosystem mit 180 Unternehmen und Forschungseinrichtungen entstanden.



### 5.2.3 Nachhaltige und strategische Wirtschaftspolitik

Zu den größten Herausforderungen Europas im Bereich der Datenwirtschaft gehört die häufig mangelnde **Nachhaltigkeit** der Förderung von Forschungsprojekten und das Fehlen von hinreichend **Venture Capital**, um entwickelte Ideen zur Vermarktungsreife zu bringen und in einer Weise mit Kapital auszustatten, dass rechtzeitig der Sprung auf eine wettbewerbsfähige Größe gelingt. Der Erfolg der USA im Bereich digitaler Produkte und Dienstleistungen wurde durch die Bereitschaft vieler Kapitalgeber, Milliardenbeträge in hoch riskante Projekte zu investieren und zu einem nicht unerheblichen Teil auch zu verlieren, begünstigt. Zudem ist zu beobachten, dass innovative Unternehmen von ausländischen Firmen **aufgekauft** oder von internationalen Kapitalgebern zur Sitzverlegung in das außereuropäische Ausland gezwungen werden.

Die **Kapitalausstattung** ebenso wie **steuerliche Anreize** sind für deutsche Start-ups zu verbessern, damit Deutschland – über die von der DEK ausdrücklich befürwortete Strategie des „europäischen Weges“ hinaus (→ unten Teil G) – weiter hinreichende Anziehungskraft auf die innovativsten Köpfe und Ideen ausübt.

Bereiche wie Bildung, öffentliche Verwaltung und Medizin sind gekennzeichnet durch ein hohes öffentliches Interesse und eine Wertebindung, die sich in Recht und Berufsethik manifestiert. Gleichzeitig ist das Potenzial für Effizienzgewinne durch Digitalisierung und KI in diesen Bereichen hoch, ohne dass schon globale, dominante Plattformen im gleichen Ausmaß etabliert sind, wie wir sie bereits in anderen Themenbereichen vorfinden. Es empfiehlt sich vor diesem Hintergrund, gerade in diesen drei Bereichen mit öffentlichen Mitteln gezielt Anreize zur **Entwicklung von Plattformen** in Deutschland zu setzen, die unseren Werten entsprechen und zugleich international skalierbar sind.

### 5.2.4 Verbesserter Leistungsschutz

Die DEK spricht sich zwar auch unter dem Aspekt der Datenwirtschaft **gegen ein neues Ausschließlichkeitsrecht** an Daten aus (oft unter dem Schlagwort „Daten-eigentum“ oder „Datenerzeugerrecht“ diskutiert, → vgl. dazu schon oben 3.3.2). Ein solches Recht, das zu den bestehenden Regelungen wie Datenschutzrecht, Persönlichkeitsrecht, Recht des geistigen Eigentums, Geschäftsgeheimnisschutz, Eigentumsrechten am Speichermedium etc. hinzukäme und mit diesen in Einklang zu bringen wäre, würde die ohnehin bestehende Komplexität und Rechtsunsicherheit nur deutlich erhöhen, ohne dass ersichtlich wäre, dass ein solches Recht für die Verkehrsfähigkeit von Daten erforderlich oder auch nur in signifikanter Weise dienlich wäre.

Dennoch hält die DEK das Bedürfnis beispielsweise der Industrie oder auch öffentlicher Stellen für berechtigt, vertraglichen Absprachen (beispielsweise zur Einschränkung der Datenweitergabe oder der Zweckbindung von Datenverwendung) eine **begrenzte Drittirkung** zu verleihen. Nach derzeit geltender Rechtslage ist eine solche Drittirkung – sofern kein immaterialgüterrechtlicher Schutz eingreift, einschließlich des sog. sui generis-Schutzes von Datenbanken – allenfalls in Extremfällen gegeben. Hier wäre zu erwägen, in Anlehnung an Art. 4 Abs. 4 der Geschäftsgeheimnis-Richtlinie 2016/943 eine Drittirkung in weiterem Umfang anzuerkennen.<sup>27</sup> Danach gälte der Erwerb, die Nutzung oder die Weitergabe von Daten als rechtswidrig, wenn eine Person zum Zeitpunkt des Erwerbs, der Nutzung oder der Weitergabe wusste oder unter den gegebenen Umständen hätte wissen müssen, dass die Zwischenperson, von der sie die Daten unmittelbar oder mittelbar erhalten hatte, sie rechtswidrig genutzt oder weitergegeben hat. Dieses Konzept würde der Datenwirtschaft helfen und sich bruchlos in das bestehende, im Wesentlichen auf Verträge fokussierte Modell einpassen.

<sup>27</sup> Diese Lösung wird etwa von den Vorentwürfen Nr. 2 (Februar 2019) und Nr. 3 (Oktober 2019) der ALI-ELI Principles for a Data Economy (oben Fn. 1) verfolgt.

### 5.2.5 Datenpartnerschaften

Auch im Bereich des **Kartellrechts** hält die DEK es für sachgerecht, den geltenden Rechtsrahmen behutsam fortzuentwickeln. Die dynamische Entwicklung der Datenwirtschaft stellt das Kartellrecht vor neue Herausforderungen, und das Kartellrecht bringt umgekehrt ge- nauso neue Herausforderungen für digitale Unternehmen mit sich. Die DEK empfiehlt der Bundesregierung, insbesondere die Chancen und Risiken von **Datenpartnerschaften** zu prüfen. Zu erwägen wäre hierbei auch eine Pflicht zur vertraulichen Anzeige von Datenpartnerschaften an die Kartellbehörden, sowie – im Hinblick auf personenbezogene Daten – an die datenschutzrechtlichen Aufsichtsbehörden. Die DEK verweist im Übrigen auf die Vorschläge, die die Kommission Wettbewerbsrecht 4.0 zu diesen Themen unter den Begriffen „Datenaustausch“ und „Datenpooling“ vorgelegt hat.

### 5.3 Datenzugang in bestehenden Wertschöpfungssystemen

#### 5.3.1 Problemstellung

In modernen Wertschöpfungssystemen kommt dem Aspekt eines **fairen und effizienten Datenzugangs** erhebliche Bedeutung zu. Die faire und effiziente Regelung des Datenzugangs verschiedener Akteure im Wirtschaftsverkehr wird primär durch das **Vertragsrecht** gewährleistet. In ihm kommt die Autonomie privater Akteure, die sog. Privatautonomie, am deutlichsten zum Tragen. Zugleich besteht eine allgemeine Vermutung, dass durch frei ausgehandelte Vereinbarungen – jenseits von Fällen des Marktversagens – eine effiziente Ressourcenallokation erreicht und damit die allgemeine Wohlfahrt gesteigert wird.

Aufgrund von Machtungleichgewichten und Informationsasymmetrien kann es allerdings auch zu **unfairen und ineffizienten vertraglichen Regelungen** kommen. Dies trifft insbesondere auf Aspekte des Datenzugangs zu, welche typischerweise in der Verhandlungsphase unterschätzt und dementsprechend vergessen oder nicht hinreichend durchdacht werden. Angesichts des dynamischen Charakters datenbezogener Interessenslagen und der dementsprechend dynamischen Bewertung von Datenrechten und Datenpflichten (→ oben 2.1) ist es auch vielfach schwierig für die Parteien, für die gesamte Vertragsdauer vorauszusehen, wie ein faires und effizientes Datenzugangsregime genau zu gestalten ist. Dadurch kommt es in der Praxis nicht selten später zu nicht vorgesehenen Verschiebungen und Ungleichgewichten, die das ursprünglich vereinbarte Gefüge von Rechten und Pflichten empfindlich stören. Da typischerweise eine der Parteien von solchen Verschiebungen profitiert, kommt es aber vielfach nicht zu Neuverhandlungen und zu einer sachgerechten und effizienten Regelung.



Gerade in komplexen Wertschöpfungssystemen sind die Zugang begehrende Partei und die die Daten faktisch kontrollierende Partei oftmals auch gar **nicht unmittelbar vertraglich miteinander verbunden** (z. B. weil ein weiteres Glied in der Vertriebskette zwischengeschaltet ist), während sie aus Gründen der Fairness und Effizienz durch ein Datenzugangsregime miteinander verbunden sein sollten. Eingriffe in die vertragliche Abschlussfreiheit in Gestalt eines sog. Kontrahierungszwangs folgen derzeit im Verhältnis zwischen zwei Unternehmen (sog. Business-to-Business-Bereich, B2B) fast ausschließlich aus dem Kartellrecht, bei lebenswichtigen Gütern und monopolartigen Stellungen teilweise auch aus allgemeinen Vorschriften, und sind insgesamt auf wenige extreme Situationen beschränkt.

### 5.3.2 Situation bei Bestehen eines Vertragsverhältnisses

Nach Auffassung der DEK bedarf es zur Gewährleistung fairer und effizienter vertraglicher Regelungen des Datenzugangs zunächst Maßnahmen zur **Bewusstseinsbildung und zur Förderung digitaler Kompetenzen** (→ oben ) sowie praktische Unterstützung in Form der Bereitstellung von **Modellverträgen**, die eine gerechte Verteilung des Datenzugangs vorsehen, sowie von **Infrastrukturen und Intermediären**, die eine geteilte Datennutzung ermöglichen, ohne beispielsweise Geschäftsgeheimnisse offenbaren zu müssen (→ oben ).

Soweit ein vertragliches Rechtsverhältnis bereits besteht, kann den Prinzipien eines fairen Datenzugangs vor allem im Wege der (gegebenenfalls ergänzenden) **Vertragsauslegung** – etwa durch Annahme entsprechender vertraglicher Nebenpflichten – sowie im Wege der **Kontrolle Allgemeiner Geschäftsbedingungen (AGB)** nach § 307 BGB (sog. Inhaltskontrolle) Rechnung getragen werden. Ein Problem bei der Vornahme der Inhaltskontrolle stellt allerdings das weitgehende Fehlen dispositiver Regelungen dar, die als Maßstab der Inhaltskontrolle dienen könnten. Daher könnten einzelne Tatbestände als ausdrücklich verbotene Vertragsklauseln (sog. **Klauselverbote**) formuliert werden (→ zur entsprechenden Forderung bei Verträgen zwischen Unternehmen und Verbrauchern, sog. B2C-Verträge, siehe schon oben 3.2.3). Daneben kommt bei einer wesentlichen Änderung der Verhältnisse ein Rückgriff auf die Regelungen zur **Störung der Geschäftsgrundlage** nach § 313 BGB in Betracht.

Die DEK bekräftigt in diesem Zusammenhang die von der **Europäischen Kommission** in ihrer Mitteilung vom April 2018 zum „Aufbau eines gemeinsamen europäischen Datenraums“ entwickelten **allgemeinen Grundprinzipien für einen Datenaustausch zwischen Unternehmen (B2B-Bereich)**.<sup>28</sup> Diese Grundprinzipien sehen vor:

- a) Transparenz von Zugangsrechten und Zwecken der Datennutzung;
- b) Anerkennung von Beiträgen anderer Beteiligter zur Wertschöpfung;
- c) Gegenseitige Achtung der Geschäftsinteressen aller Beteiligten;
- d) Gewährleistung eines unverfälschten Wettbewerbs; und
- e) Minimierung der Datenabhängigkeit von einem Anbieter (Daten-Lock-in).

<sup>28</sup> Europäische Kommission: Aufbau eines gemeinsamen europäischen Datenraums, COM(2018) 232 final, 25.4.2018, S. 12 (abrufbar unter: <https://ec.europa.eu/transparency/regdoc/rep/1/2018/DE/COM-2018-232-F1-DE-MAIN-PART-1.PDF>).

Darüber hinaus kommen – insbesondere für potenziell gemischte Datenbestände mit personenbezogenen Daten – eine Ergänzung um das informationelle Selbstbestimmungsrecht der Betroffenen und das Nichtschadensprinzip in Betracht.

### 5.3.3 Situation bei Fehlen eines Vertragsverhältnisses

Soweit Teilnehmer eines Wertschöpfungssystems trotz aller unterstützenden Maßnahmen nicht unmittelbar vertraglich miteinander verbunden sind, greift mangels eines Vertrages weder die Vertragsauslegung noch die Inhaltskontrolle von AGB noch kann auf die Grundsätze von der Störung der Geschäftsgrundlage rekurriert werden. Nach Auffassung der DEK begründet allerdings bereits der bloße Umstand, dass eine Zugang begehrende Partei zu Generierung von Daten beigetragen hat – und zwar umso mehr, wenn dies innerhalb eines prinzipiell durch Verträge geprägten Wertschöpfungssystems erfolgt – eine rechtliche Sonderbeziehung zu der die Daten faktisch kontrollierenden Partei (→ oben). Aus dieser rechtlichen Sonderbeziehung können gewisse Schutz- und Treuepflichten einschließlich der **Pflicht zur Aufnahme von Vertragsverhandlungen über ein faires und effizientes Datenzugangsregime** erwachsen. Dies sollte von der Rechtsordnung künftig explizit anerkannt werden.

Die DEK empfiehlt daher eine **Ergänzung von § 311 BGB** um einen weiteren Absatz, welcher diese Sonderbeziehung bei Beteiligten eines Wertschöpfungssystems (z. B. als Zulieferbetrieb, Hersteller, Händler oder Endnutzer) zum Ausdruck bringt und entsprechende Pflichten nach sich zieht. Die Bedeutung von Daten für den allgemeinen Rechts- und Wirtschaftsverkehr rechtfertigt es, dies nicht länger unter die Generalklausel der „ähnlichen geschäftlichen Kontakte“ zu fassen, sondern mit einem eigenen Absatz im Gesetz zu bedenken. Dieser würde weder eine eigene Rechtsgrundlage für die Verarbeitung personenbezogener Daten darstellen noch könnte er datenschutzrechtliche Positionen beschränken.

Darüber hinausgehend könnte erwogen werden, ein an den oben (→ unter 2) genannten Prinzipien orientiertes **dispositives Datenschuldrecht** zur Lückenfüllung und als Maßstab für die Inhaltskontrolle von AGB zu schaffen.<sup>29</sup> Ein solches Datenschuldrecht könnte Bedingungen definieren, unter denen insbesondere Ansprüche auf Zugang zu Daten und/oder Ansprüche auf Unterlassung eines Datenzugangs oder einer Datennutzung und/oder Ansprüche auf Korrektur von Daten bestehen. Allerdings hat die DEK auch Bedenken, dass durch speziell normierte (wenngleich dispositivo) Ansprüche zusätzliche Streitigkeiten provoziert werden könnten.

### 5.3.4 Sektorspezifische Datenzugangsrechte

Was darüber hinausgehende Datenzugangsrechte in bestehenden Wertschöpfungssystemen anbelangt, wird zunächst an sektorspezifische Lösungen zu denken sein. Die DEK empfiehlt der Bundesregierung insofern, bei Erlass und/oder Überarbeitung sektorspezifischer Regelungen Fragen des Datenzugangs verstärkte Aufmerksamkeit zu widmen.

<sup>29</sup> Für personenbezogene Daten siehe Louisa Specht: Datenrechte – Eine Rechts- und Sozialwissenschaftliche Analyse im Vergleich Deutschland – USA, Teil 1: Rechtevergleichende Analyse des zivilrechtlichen Umgangs mit Daten in den Rechtsordnungen Deutschlands und der USA, ABIDA-Gutachten, 2017, S. 89 ff. (abrufbar unter: [http://www.abida.de/sites/default/files/ABIDA\\_Gutachten\\_Datenrechte.pdf](http://www.abida.de/sites/default/files/ABIDA_Gutachten_Datenrechte.pdf)); für nicht-personenbezogene Daten siehe ALI-ELI Principles for a Data Economy (oben Fn. 1).



## 5.4 Offene Daten des öffentlichen Sektors

### 5.4.1 Vorüberlegungen

Die Öffnung von Daten des öffentlichen Sektors durch sog. Open-Government-Data-Konzepte hat mit der jüngst überarbeiteten Richtlinie (EU) 2019/1024 über Offene Daten und Informationen des öffentlichen Sektors (PSI-Richtlinie) sowie auf nationaler Ebene mit dem Informationsweiterverwendungsgesetz (IWG), dem E-Government-Gesetz (EGovG) und weiteren Spezialgesetzen eine feste gesetzliche Grundlage. Open Government Data beruht auf der Überlegung, dass Bürger und Unternehmen für die Generierung dieser Daten bereits **mit Steuergeldern bezahlt** haben und daher an den Daten partizipieren und nicht etwa doppelt finanziell belastet werden sollten. Die Öffnung von Daten des öffentlichen Sektors zur Weiterverwendung durch die Privatwirtschaft kommt zudem der europäischen Datenwirtschaft zugute. Da den Daten des öffentlichen Sektors vielfach ein **großes Wertschöpfungspotenzial für privatwirtschaftliche Unternehmen** zukommt, können diese Unternehmen damit neue innovative Produkte und Dienstleistungen entwickeln und so auch zur allgemeinen Wohlfahrtssteigerung beitragen.

Über die Wirtschaft hinaus ist der Zugang zu staatlichen Daten auch wichtig für die **Demokratie und einen offenen Diskurs** in der Gesellschaft, denn er erhöht die Verwaltungstransparenz, erleichtert Partizipation und fördert eine auf Fakten gestützte öffentliche Diskussion und Kontrolle. Darüber hinaus können Daten des öffentlichen Sektors in vielfältiger Form für gesellschaftliche Initiativen und Innovationen genutzt werden, etwa zu sozialen oder ökologischen Zwecken.

Die DEK unterstützt daher grundsätzlich die auf dem G8-Gipfel 2013 beschlossene **Open-Data-Charta**. Diese definiert zentrale Prinzipien für den Umgang mit Verwaltungsdaten:

- Standardmäßig offene Daten (Förderung der Erwartung, dass Verwaltungsdaten bei Beibehaltung des Schutzes der Privatsphäre öffentlich gemacht werden);
- Qualität und Quantität (Freigabe qualitativ hochwertiger, aktueller und gut beschriebener offener Daten);
- Von allen verwendbar (Freigabe so vieler Daten wie möglich in so vielen offenen Formaten wie möglich);
- Freigabe von Daten für verbessertes verantwortungsbewusstes staatliches Handeln (Weitergabe von Expertise und Herstellung von Transparenz betreffend Datensammlung, Standards und Veröffentlichungsverfahren);
- Freigabe von Daten für Innovation (Nutzer-Konsultationen und Unterstützung künftiger Generationen von Ideengebern).

Geben öffentliche Stellen Daten unentgeltlich an kommerzielle Akteure weiter statt sie gewinnbringend zu veräußern oder sonst wirtschaftlich zu verwerten, sollte dies aus ethischer Sicht allerdings bei pauschalierender Betrachtung durch entsprechende gesamtgesellschaftliche **Wohlfahrtsgewinne** gerechtfertigt sein.

Ferner weist die DEK auf ein mögliches **Spannungsverhältnis** zwischen Forderungen nach Privacy-by-Default einerseits und Open-by-Default andererseits sowie ganz generell zwischen dem **Diskurs um Datenschutz und dem Diskurs um Open Government Data** hin. Soweit im Rahmen von Open-Data-Konzepten personenbezogene Daten in rechtlich zulässiger Weise öffentlich gemacht werden, ist nicht gesichert, dass die zur Wahrung des Schutzes der informationellen Selbststimmung getroffenen Sicherungsmechanismen in Form ausdrücklicher oder impliziter Weiterverwendungsbeschränkungen sowie in Form technischer und organisatorischer Schutzmaßnahmen gewahrt bleiben. Gleches gilt für die allgemeinen datenschutzrechtlichen Bestimmungen für die Weiterverwendung. Da Art. 30 DSGVO zudem nur die Dokumentierung der „Kategorien von Empfängern“ verlangt und staatliche Stellen die Einhaltung „geeigneter Garantien“ im Sinne des Art. 89 DSGVO so gut wie nicht überwachen können, geht von der Offenlegung von Daten, welche personenbezogen sind oder werden können, für die Betroffenen ein besonderes Gefährdungspotenzial aus.

Vor diesem Hintergrund ist im Zusammenhang mit Open-Government-Data-Konzepten stets eine besonders sorgfältige Abwägung des grundrechtlich verankerten Rechts auf informationelle Selbstbestimmung mit den durch Open Government Data verfolgten Gemeinwohlbelangen und dem – ebenfalls grundrechtlich verankerten – Recht auf Informationsfreiheit und mit der Berufsfreiheit der durch Open Government Data Begünstigten vorzunehmen. Nach Auffassung der DEK muss diese Abwägung **in Zweifelsfällen** für den staatlichen Schutzauftrag ausfallen. Dies gilt umso mehr, als der Einzelne teilweise nicht frei bestimmen kann, welche Daten er staatlichen Akteuren anvertraut bzw. er **in besonderem Maße darauf vertraut**, dass staatliche Akteure personenbezogene Daten nicht an Dritte weiterleiten.

#### 5.4.2 Rechtsrahmen und Infrastrukturen

Die DEK begrüßt den Nationalen Aktionsplan der Bundesregierung zur Umsetzung der G8 Open-Data-Charta und die Bemühungen der Bundes- und Landesregierungen um die Digitalisierung der Verwaltung unter Einschluss von Open-Government-Data-Konzepten. Sie empfiehlt der Bundesregierung, darauf hinzuwirken, dass die in § 12a Abs. 1 S. 1 EGovG bereits für die Behörden der unmittelbaren Bundesverwaltung normierte **Pflicht zur Veröffentlichung strukturierter, unbearbeiteter Daten (Open-by-Default)** und zur grundsätzlich unentgeltlichen Bereitstellung dieser Daten zur uneingeschränkten Nutzung umfassend implementiert wird. Im Lichte des oben beschriebenen möglichen Spannungsverhältnisses von Open Government Data und Datenschutz wird die von § 12a EGovG vorgesehene Bereitstellung zur entgeltfreien und uneingeschränkten Weiterverwendung der Daten durch jedermann allerdings nur für bestimmte Datenarten (insbesondere effektiv anonymisierte Daten) in Frage kommen.

Der von der DEK begrüßte Versuch des Gesetzgebers, einen Kulturwandel der Verwaltung im Umgang mit Daten zu initiieren, wird allerdings dadurch erschwert, dass die gegenwärtige **Rechtslage sehr zersplittet** ist. Sowohl für die Behörden wie auch für potenzielle Nutzer der Daten öffentlicher Stellen ist das Zusammenspiel der unterschiedlichen Rechtsregime aus allgemeinen und speziellen Informationszugangs-, Informationsweiterverwendungs- und E-Government-Regelungen je auf Bundes- und auf Landesebene nur schwer durchschaubar. Hinzu kommt das in der Praxis vielfach schwierige Zusammenspiel dieser Regelungen mit dem Datenschutzrecht und dem Schutz des geistigen Eigentums, insbesondere dem Urheberrecht. Die DEK empfiehlt diesbezüglich eine **Zusammenführung** und **Synchronisierung** der verschiedenen Rechtsgrundlagen in Deutschland sowie sachgerechte **Klarstellungen** zur Abgrenzung der Rechtsmaterien.

Der erforderliche Kulturwandel wird auch dadurch erschwert, dass sich derzeit kaum verbindlich überprüfen lässt, ob die Behörden ihren schon bestehenden Verpflichtungen zur Datenbereitstellung tatsächlich nachkommen. So sieht etwa § 12a Abs. 1 EGovG zwar eine Pflicht der Behörden der unmittelbaren Bundesverwaltung vor, Daten zum öffentlichen Abruf bereitzustellen, gewährt der Zugang suchenden Person aber ausdrücklich **keinen einklagbaren Anspruch auf Bereitstellung**. Damit fehlt es zugangssuchenden Unternehmen an wirksamen Mechanismen, um eine Durchsetzung der gesetzlichen Bereitstellungspflicht (Open-by-Default) zu erzwingen. Aus Sicht der DEK kann die Schaffung eines **subjektiven Rechts auf Bereitstellung** dazu beitragen, die Bereitschaft der Verwaltung zur proaktiven Bereitstellung offener Daten – im Rahmen der vom EGovG bzw. IWG für die Bereitstellungspflicht statuierten Grenzen – zu fördern.

Zudem stellt die geltende Rechtslage nicht hinreichend sicher, dass die von der öffentlichen Hand zur Verfügung gestellten Daten eine **ausreichende Datenqualität aufweisen**. Insbesondere beschränkt sich die Bereitstellungspflicht nach dem EGovG auf unbearbeitete Daten. Dabei ist eine problemlose Weiterverwendung von Daten, wie sie den Zielen von Open Government Data entspricht, nur möglich, wenn eine hohe Datenqualität gewährleistet ist.



Neben den rechtlichen sind zudem die **infrastrukturellen Grundlagen** (z. B. Open-Government-Data-Portale wie GovData) zu schaffen bzw. auszubauen, auch und gerade, was beispielsweise kommunale Plattformen betrifft. Dies gilt auch für die Investition in hinreichende Qualitätssicherungsmaßnahmen.

#### 5.4.3 Schutzauftrag des Staates

Im Hinblick auf den Schutzauftrag des Staates bezüglich aller ihm anvertrauten Daten muss durch **entsprechende Vorkehrungen** gewährleistet sein, dass der Schutz wichtiger Individualinteressen (z. B. bei personenbezogenen Daten, Betriebs- und Geschäftsgeheimnissen oder sonstigen schutzbedürftigen Daten, wie etwa vertraulichen Informationen im Rahmen von Vergabeverfahren der öffentlichen Hand) ebenso vollumfänglich garantiert ist wie der Schutz wichtiger Allgemeininteressen (wie etwa Sicherheitsinteressen oder Interessen der nationalen Souveränität). Die dem Open-Government-Data-Konzept zugrundeliegende ethische Überlegung, dass die Bürger und Unternehmen für die Daten bereits mit ihren Steuergeldern bezahlt haben, bedeutet auch gewisse **Einschränkungen der Weiterverwendung**. Insbesondere ist Sorge zu tragen, dass die Daten nicht zur privatwirtschaftlichen Entwicklung von Diensten und Produkten verwendet werden, welche die Freiheit der Bürger und Unternehmen letztlich einschränken und/oder ihnen schließlich zu ungerechten Konditionen angeboten werden.

Der Bundesregierung ist daher zu empfehlen, von der in Art. 8 der neugefassten PSI-Richtlinie eröffneten Möglichkeit Gebrauch zu machen, in Standardlizenzen **Modellkonditionen** einschließlich Zweckbindungsvereinbarungen und Bedingungen für die Weitergabe an Dritte zu entwickeln bzw. auf deren Entwicklung auf europäischer Ebene hinzuwirken. Die DEK empfiehlt, die Verwendung solcher Modellkonditionen – mindestens sektorspezifisch – sogar **bindend vorzuschreiben**. Dabei sollten sie sich u.a. an folgenden Eckpunkten orientieren:

- a) Gemäß Art. 8 Abs. 1 PSI-Richtlinie müssen die Bedingungen objektiv, verhältnismäßig, nichtdiskriminierend und durch ein im Allgemeininteresse liegendes Ziel gerechtfertigt sein; sie dürfen die Möglichkeiten der Weiterverwendung nicht unnötig einschränken und nicht der Behinderung des Wettbewerbs dienen;
- b) Unternehmen sollten sich Richtlinien unterwerfen, die klar definierte Garantien für die Rechte betroffener Dritter enthalten sowie Mechanismen für deren Überprüfbarkeit vorsehen;
- c) Mithilfe der Daten entwickeltes geistiges Eigentum darf nicht dazu genutzt werden, Aktivitäten, die öffentliche Stellen im Rahmen der Erfüllung ihrer öffentlichen Aufgaben verfolgen, zu untersagen bzw. nur noch gegen Zahlung einer Lizenzgebühr zuzulassen;
- d) Wird mithilfe der Daten ein Produkt oder eine Dienstleistung entwickelt, sollte dieses Produkt bzw. diese Dienstleistung öffentlichen Stellen unter Vorzugsbedingungen anzubieten sein;
- e) Marktstarke Unternehmen sollten eine Reziprozitätsverpflichtung in dem Sinne eingehen, dass sie ihrerseits unter gleichen Bedingungen Betriebsdaten zur Verfügung stellen; und
- f) Daten sollten nur für unternehmerische Aktivitäten in der EU verwendet werden, oder bei denen zumindest die Entwicklung des Produkts oder der Dienstleistung in der EU erfolgt.

Bei jedem Transfer von Daten, bei dem der Empfänger eine Kopie der Daten auf einer von ihm kontrollierten Infrastruktur erhält, lässt sich die Einhaltung vereinbarter Garantien und Zweckbeschränkungen im Prinzip nicht mehr zuverlässig kontrollieren. Im Bestreben, seinem Schutzauftrag bei Daten, die – gegebenenfalls auch nur im Fall einer De-Anonymisierung oder Verknüpfung mit anderen Datensätzen – zum Schaden Dritter oder der Allgemeinheit verwendet werden könnten, gerecht zu werden, werden staatliche Stellen insbesondere erwägen müssen, ausschließlich den überwachten Zugang und die **überwachte Verarbeitung** auf einer von der staatlichen Stelle kontrollierten Infrastruktur zuzulassen. Die dafür anfallenden Kosten wären auf die Zugang suchenden Unternehmen umzulegen.

## 5.5 Offene Daten des privaten Sektors

### 5.5.1 Plattformen und Datennutzung

In der deutschen Wirtschaft fallen im Geschäftsbetrieb des Unternehmens sog. Betriebsdaten an. Diese Daten haben einen großen Wert für Innovationen, insbesondere, wenn sie mit den Daten anderer Teilnehmer der Wertschöpfungskette verknüpft werden. Zum Zwecke einer derartigen Verknüpfung hat die deutsche Wirtschaft sektorspezifische Plattformen geschaffen.

---

*Beispiele für die verschiedenen Plattformtypen sind:  
(1) Zusammenschluss verschiedener Unternehmen in einer GmbH; (2) Eigenbetrieb eines Unternehmens mit Anbindung von Partnern; (3) Begründung einer unternehmenseigenen Plattform als Serviceplattform für Dritte.*

---

Neben den Plattformen verständigen sich die verschiedenen Branchen zunehmend auf gemeinsame Regelungskonzepte zur Nutzung der Daten.

Die DEK geht davon aus, dass die Wirtschaft weiterhin branchenspezifisch ihre Datennutzung innerhalb der Wertschöpfungssysteme selbst organisiert und dabei auch die für Innovation notwendige Offenheit für neue Marktteilnehmer und Start-ups zeigt. Es liegt nämlich im Interesse der Marktteilnehmer, in Zusammenarbeit mit innovativen Start-ups, digitale Sprunginnovationen zu entwickeln und in diesem Zusammenhang ihre Daten zu teilen. Die Selbstorganisation in unterschiedlichen Typen von Plattformen stärkt das in Europa bestehende industrielle Knowhow und gewährleistet eine höhere Qualität der Datennutzung (einschließlich Datenschutz und Informationssicherheit). Die DEK regt an, die positive **Entwicklung der privatwirtschaftlich organisierten Plattformen zu fördern**, um die erforderliche Marktgröße und Skaleneffekte zu erreichen und damit gemeinsam international wettbewerbsfähig zu sein.

### 5.5.2 Anreize zum weitergehenden freiwilligen Teilen

Bereits gegenwärtig existieren viele Geschäftsmodelle, die auf einer freiwilligen Gewährung eines Datenzugangs für die Allgemeinheit seitens privater Anbieter beruhen.

---

#### Beispiel 14

*Dies ist etwa beim sog. Geobusiness der Fall, bei dem (z.T. aus behördlichen Quellen stammende) Geobasisdaten mit weiteren Informationen angereichert werden, sodass für die verschiedensten Zwecke Geofachdaten bereitgestellt werden. Zu denken ist hier nicht nur an Kartendienste, wie Open Street Map oder Google Maps, die über die reinen topographischen und administrativen Informationen mit einer Vielzahl zusätzlicher Informationen versehen werden, sondern auch spezifische Angebote wie Vorhersagen hinsichtlich Wetter oder Verkehrsbedingungen.*

---



Die DEK empfiehlt eine Förderung solcher Offenlegung auf freiwilliger Basis. Hierfür sind neben den empfohlenen **Maßnahmen praktischer Unterstützung** (→ oben 5.2) auch **weitere Anreize** zum freiwilligen Teilen von Daten in Erwägung zu ziehen, etwa eine positive Berücksichtigung von Daten(frei)gaben und Open-Access-Strategien

- im Steuerrecht;
- im Rahmen des Vergaberechts;
- bei der Vergabe von Fördermitteln (auch außerhalb des Forschungsbereichs) oder
- bei der Durchführung von Genehmigungsverfahren.

Freiwilliges Teilen, Daten(frei)gaben und Open-Access-Strategien kommen in den vorgenannten Bereichen allerdings nur in Betracht, soweit damit keine Geheimhaltungserfordernisse aufgrund des Vergaberechts oder aufgrund von Betriebs- und Geschäftsgeheimnissen verletzt und keine Regelungen des Datenschutzrechts missachtet werden.

### 5.5.3 Gesetzliche Datenzugangsrechte

Im Gegensatz zum freiwilligen Teilen von Daten steht bei gesetzlichen Datenzugangsrechten der Gedanke im Mittelpunkt, dass bei großen Datenbeständen, soweit sie durch das Zusammenwirken vieler Mitglieder der Gesellschaft akkumuliert wurden – etwa durch soziale Netzwerke – der Gesellschaft auch etwas zurückzugeben ist. Dieser Gedanke könnte – in Verbindung mit dem grundlegenden Wert gesellschaftlicher Solidarität sowie mit im konkreten Fall einschlägigen Gemeinwohlinteressen – **weitergehende Zugangsgewährungs- und Offenlegungspflichten** Privater begründen.<sup>30</sup>

Zur Verbesserung des allgemeinen Zugangs zu privat gehaltenen Daten wird zunächst diskutiert, ein an Art. 20 DSGVO angelehntes, **allgemeines Portabilitätsrecht** für nicht-personenbezogene Daten zu schaffen. Das würde beispielsweise bedeuten, dass auch eine juristische Person, auf die sich bestimmte Daten beziehen oder auf die Daten bezogen werden können, gegenüber jedem Akteur, der solche Daten in seinem Besitz hat, verlangen kann, dass ihr diese Daten in einem gängigen und maschinenlesbaren Format übermittelt werden oder dass sie direkt auf einen dritten Akteur übertragen werden. Aus im Wesentlichen ähnlichen Gründen, wie sie bereits gegen eine Erweiterung von Art. 20 DSGVO angeführt wurden (→ oben ), empfiehlt die DEK der Bundesregierung, die Entwicklungen hinsichtlich **Nutzung und Auslegung des Art. 20 DSGVO zunächst abzuwarten**. Hinzu kommt als besondere Herausforderung, dass sich bei nicht-personenbezogenen Daten die Frage der Zuordnung, d.h. die Frage nach dem Inhaber des Portabilitätsrechts, ganz neu stellen würde.

Zur Verbesserung des allgemeinen Zugangs zu privat gehaltenen Daten werden auch eine Reihe weiterer Maßnahmen diskutiert, die im Ergebnis auf gesetzliche Datenzugangsrechte hinauslaufen. Dazu gehören als **denkbare Modi der Ausgestaltung** eine gesetzliche Pflicht zur Bereitstellung bestimmter intern erstellter Datenanalysen für die Öffentlichkeit, die Einräumung individueller Zugangsrechte (z.B. Pflicht zur Lizenzierung unter FRAND-Bedingungen<sup>31</sup> und/oder nach Anwendung des urheberrechtlichen Drei- bzw. Vier-Stufen-Tests<sup>32</sup>) oder auch die Offenlegung von Daten gegenüber der Allgemeinheit (Open Access), welche sowohl marktanteilsbezogen als auch allgemein ausgestaltet sein kann.

Bei all diesen Maßnahmen sind nach Auffassung der DEK zunächst mindestens die folgenden Faktoren zu berücksichtigen:

<sup>30</sup> Dazu u.a. Viktor Mayer-Schönberger / Thomas Ramge: Das Digital, 2017, S. 195 ff.

<sup>31</sup> FRAND = Fair, Reasonable and Non-Discriminatory.

<sup>32</sup> Der „Drei-Stufen-Test“ bezeichnet einen in mehreren internationalen Verträgen vorgesehenen dreistufigen Test, mit dem geprüft wird, ob eine Ausnahmeregelung (sog. Schrankenbestimmung) einen akzeptablen Eingriff in die Rechte des Urhebers darstellt. Solche Ausnahmen dürfen laut Test nur (i) in Sonderfällen zur Anwendung kommen, welche (ii) die normale, kommerzielle Verwertung nicht beeinträchtigen und auch (iii) die berechtigten Interessen des Rechteinhabers nicht ungebührlich verletzen. Es wird verstärkt gefordert, auch (iv) Drittinteressen sowie Allgemeininteressen zwingend in den Test einzubeziehen.

- a) Der Schutz der von der Zugangsgewährung oder Offenlegung betroffenen personenbezogenen Daten sowie von Betriebs- und Geschäftsgeheimnissen muss gewährleistet sein;
- b) Die Anforderungen an die Verhältnismäßigkeit des Eingriffs in die Grundrechte der von der Zugangsgewährungs- oder Offenlegungspflicht betroffenen Privaten müssen gewahrt sein; dies betrifft insbesondere die Berufsfreiheit;
- c) Negative Folgen für den Wettbewerb durch den Zugang oder die Offenlegung, etwa aufgrund strategischer Nutzung durch – gegebenenfalls selbst nicht offenlegungspflichtige – Mitbewerber sind zu vermeiden;
- d) Anreize, in Geschäftsmodelle der Datenwirtschaft zu investieren, dürfen nicht genommen werden; und
- e) Der Schutz strategischer Interessen deutscher bzw. europäischer Unternehmen gegenüber globalen Wettbewerbern ist zu berücksichtigen. Dies betrifft insbesondere Konsequenzen für die Stellung der deutschen bzw. europäischen Wirtschaft im globalen Wettbewerb, wenn gerade deutsche bzw. europäische Unternehmen zur Offenlegung ihrer Datenbestände gezwungen wären und diese Datenbestände in die Hände derjenigen Akteure gelangen würden, bei denen bereits jetzt die größte Datenkompetenz, die besten Dateninfrastrukturen und vor allem die größten Datenbestände liegen.

Vor diesem Hintergrund empfiehlt die DEK primär ein **sektorspezifisches Vorgehen**. Im Kontext raumbezogener Informationen stehen mit der INSPIRE-Richtlinie und deren Umsetzung in nationales Recht bereits sektorspezifische Zugangsregelungen zur Verfügung, die allerdings nur öffentliche Stellen zur Bereitstellung verpflichten. Einen ersten Anwendungsfall für ein sektorspezifisches

Datenzugangsrecht zu Daten im privaten Sektor gibt es im Bereich der Zahlungsdienstleistungen. Die DEK regt an, Bedarf und Implementierungsoptionen in einer Reihe weiterer ausgewählter Sektoren zu prüfen, wobei beispielsweise der **Nachrichten-, Mobilitäts- oder Energiesektor** infrage käme.

#### 5.5.4 Rolle des Wettbewerbsrechts

Wenngleich das geltende Wettbewerbsrecht kaum datenspezifische Regelungen enthält, sind doch die allgemeinen Regelungen auch auf die Datenwirtschaft anwendbar. Die **Essential Facility Doctrine** (EFD) kann – gegebenenfalls in leicht modifizierter Form – etwa eingreifen, wenn ein marktbeherrschendes Unternehmen exklusiv eine Ressource (z.B. Netz/Infrastruktur) kontrolliert, die für den Wettbewerb auf einem angrenzenden Markt unerlässlich ist. Die **Aftermarket-Doktrin** betrifft den Fall, dass der Nachfrager eines Primärprodukts infolge von Lock-in in der Ausübung seiner Wahlfreiheit auf einem Sekundärmarkt (z.B. Markt für Reparaturen/Ersatzteile) beschränkt wird bzw. ein Drittanbieter auf einem solchen Sekundärmarkt in wettbewerbswidriger Weise behindert wird.<sup>33</sup> Allerdings stellt die Missbrauchsaufsicht derzeit infolge der Unklarheit der Rechtslage, hoher Anforderungen sowie der Dauer und Kosten von Verfahren keine allgemeine Lösung etwaiger Probleme des Datenzugangs dar. Das geltende Wettbewerbsrecht oder einzelne seiner Elemente könnten jedoch zu einem zentralen Baustein eines neuen, **digitalen Wirtschaftsrechts** werden, das wesentlich auch Probleme des Datenzugangs adressiert. Diesbezüglich sind die Ergebnisse der Kommission Wettbewerbsrecht 4.0 zu berücksichtigen.<sup>34</sup>

<sup>33</sup> Jacques Crémér / Yves-Alexandre de Montjoye / Heike Schweitzer: Competition policy for the digital era, Special Advisers' Report for the European Commission, S. 87 ff (abrufbar unter: <https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf>).

<sup>34</sup> Ein neuer Wettbewerbsrahmen für die Digitalwirtschaft, Bericht der Kommission Wettbewerbsrecht 4.0, 2019 (abrufbar unter: [https://www.bmwi.de/Redaktion/DE/Publikationen/Wirtschaft/bericht-der-kommission-wettbewerbsrecht-4-0.pdf?\\_\\_blob=publicationFile&v=4](https://www.bmwi.de/Redaktion/DE/Publikationen/Wirtschaft/bericht-der-kommission-wettbewerbsrecht-4-0.pdf?__blob=publicationFile&v=4)).

## 5.6 Datenzugang zugunsten von öffentlichen Stellen (B2G) und gemeinwohlorientierten Zwecken

Zu erwägen ist, inwieweit eine Pflicht zur Zugangsgewährung definierter Teilmengen von Daten zugunsten bestimmter **öffentlicher Stellen** oder bestimmter **gemeinwohlorientierter Zwecke** in Betracht kommt. Eine besondere Bedeutung können Zugangsrechte zu den Daten Privater bzw. Offenlegungspflichten im Bereich der **Forschung** haben. Hier könnte ein erleichterter Zugang – im Falle einer angemessenen Ausgestaltung, die den Rechten der Betroffenen vollumfassend Rechnung trägt – zum allgemeinen Erkenntnisfortschritt beitragen. Entsprechende Zugangsrechte zu Daten des Privatsektors können zudem Nicht-Regierungs-Organisationen, Medien und ähnlichen Stellen die Erfüllung ihrer gesellschaftlichen Funktionen erleichtern und so zur Sicherung des **demokratischen Gemeinwesens** beitragen. Eine besonders herausgehobene Stellung muss auch stets dem Zweck der **Gefahrenabwehr** (z.B. Unwetterwarnung) zukommen.

Dabei empfiehlt sich aus Sicht der DEK erneut primär ein **sektorspezifisches Vorgehen**, das die Ausgestaltung von Datenzugangs- und Offenlegungspflichten an die konkret betroffenen verfassungsrechtlichen Vorgaben einerseits und die praktischen Gegebenheiten des Sachbereichs andererseits anpasst. Hohe Priorität besteht insbesondere im **Gesundheitssektor**, im **Mobilitätssektor** und im **Energie sektor**. Eine allgemeinere Pflicht zur Datenbereitstellung – etwa generell zu gemeinwohlorientierten Forschungszwecken – bedürfte dagegen nach Auffassung der DEK erst einer breiten gesellschaftlichen Debatte, zu welcher die DEK an dieser Stelle einladen möchte.

Die DEK bekräftigt die von der Europäischen Kommission in ihrer Mitteilung vom 25. April 2018 zum „Aufbau eines gemeinsamen europäischen Datenraums“ formulierten **Grundprinzipien für einen Datenaustausch zwischen privaten Unternehmen und dem öffentlichen Sektor (sog. Business-to-Government-Konstellation, B2G)**:<sup>35</sup>

- a) Verhältnismäßigkeit (d.h. Zweckdienlichkeit für ein klares und nachweisbares öffentliches Interesse und Angemessenheit im Hinblick auf Detailliertheit, Relevanz und Datenschutz);
- b) Zweckbindung (d.h. eindeutige Beschränkung auf einen oder mehrere Zwecke und Zusicherung der Nichtverwendung in Verwaltungs- oder Gerichtsverfahren);
- c) Schadensvermeidung (d.h. Schutz berechtigter Interessen wie dem informationellen Selbstbestimmungsrecht betroffener Personen, Geschäftsgeheimnissen, vertraulichen Geschäftsinformationen und Verwertungsinteressen);
- d) Berücksichtigung des öffentlichen Interesses bei den Vertragsbedingungen (Vorzugsbedingungen für öffentliche Stellen, Gleichbehandlung öffentlicher Stellen, Verringerung der Gesamtbelastung für Bürger und Unternehmen);
- e) Datenqualitätsmanagement (zumutbare Unterstützung bei der Qualitätsbewertung, aber normalerweise keine Pflicht zur Qualitätsverbesserung);
- f) Transparenz und Einbeziehung der Öffentlichkeit bezüglich Vertragsparteien, Zielen, erlangten Erkenntnissen und bewährten Verfahren.

Diese Grundprinzipien könnten einen **guten Ausgangspunkt** darstellen, und zwar nicht nur für die Bedingungen frei vereinbarter Verträge zum Datenaustausch, sondern auch als mögliche Bedingungen etwaiger weitergehender, sektorspezifischer gesetzlicher Maßnahmen zur Verbesserung eines Datenzugangs.

<sup>35</sup> Europäische Kommission, Aufbau eines gemeinsamen europäischen Datenraums, COM(2018) 232 final, 25.4.2018, S. 15 f (abrufbar unter: <https://ec.europa.eu/transparency/regdoc/rep/1/2018/DE/COM-2018-232-F1-DE-MAIN-PART-1.PDF>).

# Zusammenfassung der wichtigsten Handlungsempfehlungen

## 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.

**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.

**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.

**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.

**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**.

**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.

**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.



Teil F

# Algorithmische Systeme



# 1. Charakteristika algorithmischer Systeme

Zahlreiche Produkte und Anwendungen – von der Sprachassistenz über die automatisierte Kreditvergabe bis hin zum „autonomen“ Fahrzeug – basieren heute auf mehr oder weniger „intelligenten“ Algorithmen. Gerade aufgrund der Vielfalt der Erscheinungsformen derartiger Techniksysteme empfiehlt es sich aus Sicht der DEK, beim ethischen und rechtlichen Zugriff auf die Materie vom **allgemeinen Begriff des algorithmischen Systems** auszugehen (→ oben Teil C, 2.2.5). Die Leitfragen der Bundesregierung zu den Themenbereichen „Algorithmenbasierte Prognose- und Entscheidungsprozesse“ und zur „Künstlichen Intelligenz“ werden daher im Folgenden gemeinsam als Fragen des Umgangs mit algorithmischen Systemen diskutiert.

Bei der ethischen und rechtlichen **Bewertung einzelner algorithmischer Systeme** müssen allerdings insbesondere **folgende Differenzierungen** berücksichtigt werden:

- In **technischer Hinsicht** weisen algorithmische Systeme unterschiedliche Eigenschaften auf. Das Spektrum reicht von Systemen, die vollständig deterministisch operieren, bis hin zu Systemen, die im Wege maschinellen Lernens eigenständig Handlungspläne entwickeln, um das vom Betreiber des algorithmischen Systems vorgegebene Ziel zu erreichen.
- Im algorithmischen System als sozioinformatisches System können ethisch und rechtlich relevante Vorgänge auf **unterschiedlichen Systemebenen** angeordnet sein, d.h. auf der Ebene der Datenbasis, des Algorithmus im technischen Sinne bis hin zur Ebene der an der Entwicklung, Implementierung, Bewertung oder Korrektur des Systems beteiligten Menschen.
- **Zweck und Folgen** des Einsatzes algorithmischer Systeme differieren erheblich. Soweit algorithmische Systeme menschliche Entscheidungen und Prognosen unterstützen oder ersetzen, wirken sie oft unmittelbar auf die Rechte und Interessen von Individuen ein. Als Beispiele können die automatisierte Kreditvergabe und der automatisierte Verwaltungsakt dienen. Algorithmische Systeme finden aber auch dort Verwendung, wo sich ein derartiger Bezug zu menschlichen Entscheidungen allenfalls mittelbar herstellen lässt. Letzteres ist etwa bei verschiedenen für das „autonome“ Fahren konstitutiven Prozessen oder bei sog. Predictive Maintenance im Maschinenbau der Fall.
- Je nach Einsatzkontext berühren algorithmische Systeme unterschiedliche **ethische und rechtliche Prinzipien**. So wirft bei „autonom“ agierenden cyber-physischen Systemen üblicherweise das äußerlich sicht- und spürbare „Verhalten“ der Systeme Fragen auf. Dieser Aspekt steht etwa bei der Diskussion um den Einsatz von Robotik in der Pflege im Vordergrund. Für die Beurteilung dieser Systeme sind in erster Linie Prinzipien wie der Grundsatz menschenzentrierten Designs maßgeblich. Dort, wo algorithmische Systeme nicht in ähnlicher Form „verkörperlicht“ sind, ist es hingegen vielfach der äußerlich nicht sichtbare Weg zur „Entscheidung“ des Systems, dem die Aufmerksamkeit gilt. Diskutiert wird dabei etwa über die Transparenz der Systeme oder um den Grundsatz menschlicher Letztentscheidung gemäß Art. 22 DSGVO. Ein Beispielsfall hierfür ist die automatisierte Kreditwürdigkeitsprüfung. Die Unterscheidung von „verhaltens-“ und „entscheidungs-“orientierter Perspektive relativiert sich allerdings bei näherer Betrachtung. Denn jedem sichtbaren „Verhalten“ eines Systems ist zu irgendeinem Zeitpunkt eine menschliche „Entscheidung“ vorgelagert, etwa bei der Konstruktion des Systems, und jede „Entscheidung“ findet ihre Brisanz gerade darin, dass eine andere Systemkomponente (einschließlich eines menschlichen Akteurs) ihr „Verhalten“ daran ausrichtet.

Insbesondere dort, wo algorithmische Systeme eng in menschliche **Entscheidungsprozesse eingebunden** sind, bietet es sich aus Sicht der DEK an, **weitere Differenzierungen** vorzunehmen. Ein Algorithmus selbst kann keine Entscheidung im ethisch gehaltvollen Sinne treffen, da er aus sich heraus keine wertebasierten Präferenzen hat. Je nach der konkreten Aufgabenverteilung zwischen menschlichen Akteuren und Maschine lassen sich drei verschiedene Stufen des Einbezugs von algorithmischen Systemen in menschliche Entscheidungen unterscheiden:

- **Algorithmenbasierte** Entscheidungen sind menschliche Entscheidungen, die sich auf algorithmisch berechnete (Teil-)Informationen stützen. Beispiele sind klinische Entscheidungsunterstützungssysteme, die anhand von Patientendaten aus der elektronischen Patientenakte und auf der Grundlage einer Auswertung der wissenschaftlichen Literatur dem Arzt Behandlungsempfehlungen geben. Der Arzt trifft dann unter Berücksichtigung dieser Empfehlung mit dem Patienten gemeinsam die Entscheidung, welche Behandlung letztlich gewählt wird. Algorithmenbasierte Entscheidungen können gleichwohl auf subtile Weise menschliche Entscheidungen im Ergebnis signifikant beeinflussen, etwa wenn das algorithmische System Informationen über Menschen/Objekte/Verfahrensweisen zusammenstellt, die eine Wertung enthalten, die dem Anwender nicht bewusst sein muss.
- **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, insbesondere, weil sich die Entscheidung nur in algorithmisch ermittelten und vorgegebenen Bahnen bewegen kann. Als Beispiel kann eine Anwendung aus dem Bereich Industrie 4.0 dienen, bei denen in der Mensch-Maschine-Interaktion ein robotisches System dem am Fertigungsprozess beteiligten Menschen nur begrenzte Handlungsspielräume eröffnet.

- **Algorithmendeterminierte** und damit **vollständig automatisierte** Entscheidungen erfolgen *prima facie* unabhängig von einem menschlichen Akteur. Vielmehr führen die Ergebnisse eines algorithmischen Systems automatisiert zu Konsequenzen, so dass keine ausdrückliche menschliche Entscheidung mehr erfolgt. Anwendungsbeispiele reichen von Preisdifferenzierungen im Online-Handel über den voll-automatisierten Verwaltungsakt bis hin zu sog. autonomen Waffensystemen. Menschliche Entscheidungen sind gleichwohl involviert, da Menschen darüber entschieden haben, die algorithmischen Systeme zu diesen Zwecken und in dieser Weise einzusetzen.

---

#### Beispiel 1

Anhand eines *algorithmischen Systems* im Rahmen der Auswahl von Bewerbern für einen Arbeitsplatz können die Unterschiede veranschaulicht werden: Im Falle eines *algorithmischen Systems*, das dem ausählenden Arbeitgeber lediglich Informationen zu den einzelnen Bewerbern zusammenstellt, auf deren Grundlage dieser dann seine Entscheidungen trifft, handelt es sich um ein *algorithmenbasiertes Entscheidungsverfahren*. Das System führt zu algorithmengetriebenen Entscheidungen, sobald die dem Arbeitgeber übermittelten Informationen eine Bewertung der einzelnen Bewerber (etwa ein Ranking) enthalten, da dieses die Auswahlwahrscheinlichkeiten für einzelne Bewerber signifikant beeinflussen kann. Noch deutlicher wird die faktische Beschränkung der Entscheidungsmöglichkeiten des Arbeitgebers, wenn das System bereits eine Vorauswahl unter den Bewerbern trifft, so dass der Arbeitgeber einzelne Bewerbungen gar nicht mehr zur Kenntnis nimmt. Bei einem *algorithmendeterminierten Auswahlprozess* würde die Nachricht über die Annahme oder Ablehnung einer Bewerbung automatisiert durch das *algorithmische System* erfolgen, ohne dass ein Mensch die Auswahl noch einmal überprüft.

---



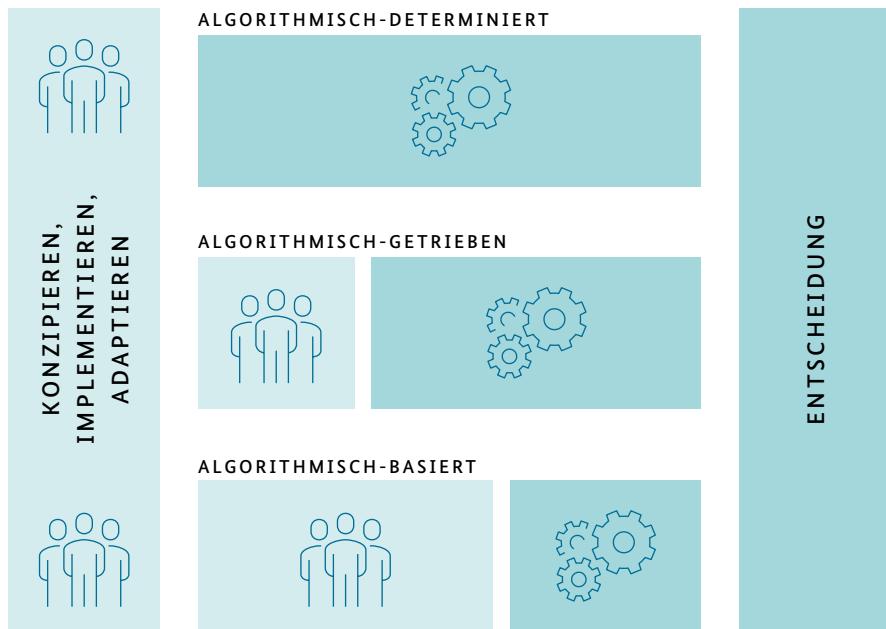


Abbildung 7:  
Charakteristika algorithmischer Systeme

Die Zuordnung eines algorithmischen Systems zu einer der drei Formen ist vielfach schwierig, und es sind **Mischformen** innerhalb einer komplexen Softwarearchitektur möglich. Auch kann je nach Wirkweise des Systems der Determinierungsgrad für menschliche Akteure im selben Punkt unterschiedlich hoch sein. So ist im obigen Beispiel ein Entscheidungsprozess, in dem ein algorithmisches System vorab einzelne Bewerber ausfiltert und diesen absagt, aus Sicht dieser aussortierten Bewerber algorithmendeterminiert, für alle verbleibenden Bewerber hingegen algorithmengetrieben.

Hinzu kommt, dass es aufgrund von sog. **Automation Bias- und Default-Effekten** in der praktischen Handhabung der Systeme zu **Überschneidungen** kommen kann. Selbst im Fall algorithmenbasierter Entscheidungen, bei denen der Mensch die volle Entscheidungshoheit hat, kann er dazu tendieren, ohne ausreichend kritische Prüfung der Empfehlung des algorithmischen Systems einfach zu folgen, da er sich ansonsten einem unbehaglichen Rechtfertigungzwang ausgesetzt fühlt und subjektiv den Eindruck hat, dass sich das Risiko der Verwerfbarkeit einer Fehlentscheidung erhöht. Gleichwohl ist die grundsätzliche Unterscheidung für die Zuordnung von Verantwortung für eine Risikobestimmung und damit auch für eine Regulierung relevant.

## 2. Allgemeine Anforderungen an algorithmische Systeme

Maßstab für die Gestaltung und den Einsatz algorithmischer Systeme sind die **allgemeinen ethischen und rechtlichen Grundsätze und Prinzipien**, zuvörderst die Würde des Menschen (→ oben Teil B, 3). Im Sinne des **Grundsatzes vorausschauender Verantwortung** sind bei der Bewertung konkreter algorithmischer Systeme die beabsichtigten und unbeabsichtigten Auswirkungen auf die Nutzer sowie auf die vom Einsatz eines algorithmischen Systems betroffenen Personen zu bedenken. Insbesondere mit Blick auf die Netzwerk-, Skalen- und Verbundeffekte sind, je nach Einsatzzweck und Anwendungskontext, auch gesellschaftliche Folgewirkungen zu reflektieren und vorausschauend zu berücksichtigen. Diese reichen von den positiven Effekten sozialer Innovationen bis hin zu (teilweise subtilen) negativen Effekten etwa auf Vielfalt und Kultur der gesellschaftlichen Debatte als wesentlicher Bedingung für eine funktionierende Demokratie. Hieraus lassen sich nach Auffassung der DEK die folgenden, für die Gestaltung und den Einsatz algorithmischer Systeme zentralen Anforderungen ableiten, die – im Sinne der hier eingenommenen **Governance-Perspektive** – im Zusammenspiel insbesondere von Entwicklern, Unternehmen, Nutzern und staatlichen Stellen umzusetzen sind.

### 2.1 Menschenzentriertes Design

Im Mittelpunkt steht das Gebot, ein **menschenzentriertes und werteorientiertes Design** algorithmischer Systeme anzustreben, das die grundlegenden Rechte und Freiheiten berücksichtigt. Die Zentrierung auf den Menschen hat nach Ansicht der DEK den gesamten Design-Prozess zu durchdringen. Sie ist durch eine breite Palette unterschiedlicher Maßnahmen sicherzustellen, zu denen auch und gerade die **inklusive und partizipative Entwicklung** von algorithmischen Systemen gehören kann.

Menschenzentriertes Design verlangt insbesondere Veränderungen der Selbstwahrnehmung und Selbstgestaltung infolge der Konfrontation des Einzelnen mit algorithmischen Systemen Rechnung zu tragen. Dabei sind etwa auch Kompetenzgewinne und -verluste im Umgang mit den Systemen, Auswirkungen auf die eigene Lebensweise und die Urteilsbildung sowie auf das körperliche Wohlbefinden schon bei der Entwicklung der Systeme zu berücksichtigen.

Augenmerk ist aber nicht zuletzt auch auf das **emotionale Wohlbefinden** betroffener Personen zu richten, die bei Einsatz menschlicher Akteure und herkömmlicher Technologie anders (niedriger oder auch höher) sein mag als bei Einsatz algorithmischer Systeme. Dies ist nicht nur für die von einer Entscheidung betroffene Person, sondern auch auf der Anwenderseite bedeutsam. Dabei ist u.a. zu berücksichtigen, dass unmittelbare zwischenmenschliche Interaktion eine Vielzahl von Funktionen erfüllt, die weit über das Fällen „guter Entscheidungen“ hinausgehen.

---

#### Beispiel 2

*Bei der Unterstützung medizinischer Diagnosen durch algorithmische Systeme ist zuvörderst die Treffsicherheit der Diagnose als Einsatzzweck zu identifizieren. Allerdings ist auch das vielfach ausgeprägte Bedürfnis nach menschlicher Zuwendung im Therapiegespräch (mit entsprechender Bedeutung für den Therapieerfolg) nicht außer Acht zu lassen und ebenso das Bedürfnis des Arztes, die eigene ärztliche Erfahrung einbringen zu können. Umgekehrt mag es in bestimmten Situationen – etwa bei schambesetzten Symptomen – für Patienten sogar angenehmer sein, sich nicht primär einem menschlichen Gegenüber anvertrauen zu müssen.*

---



Zu diesen Funktionen gehören etwa: die Befriedigung eines menschlichen Grundbedürfnisses nach **Kommunikation**; das Gefühl, das Gegenüber prinzipiell in seinen Denk- und Reaktionsweisen einschätzen zu können und vom Gegenüber verstanden zu werden, die Chance, das Gegenüber vom eigenen Standpunkt noch überzeugen zu können, sowie der gewisse Kontrolleffekt, der dadurch entsteht, dass das menschliche Gegenüber unmittelbar mit der Reaktion des von einer Entscheidung Betroffenen konfrontiert wird.

### Beispiel 3

*Emotionale Aspekte spielen auch beim Einsatz algorithmischer Systeme in der Mensch-Maschine-Interaktion eine wichtige Rolle. Beispielsweise kann ein an sich zur Unterstützung der Beschäftigten vorgesehenes System von diesen als invasiv oder bevormundend wahrgenommen werden, weil damit das Verhalten von Beschäftigten analysiert wird, ihnen bestimmte lieb gewonnene Tätigkeiten abgenommen werden oder ihnen suggeriert wird, dass die eigene Leistungsfähigkeit im Vergleich zum „Kollegen Roboter“ unterlegen ist.*

Das Wohlbefinden aller von einer Technologie Betroffenen, so etwa beim Einsatz von Robotik in der Pflege, ist ein zentraler Leitwert, der bei ethischer Technikgestaltung unbedingt berücksichtigt werden muss. Wichtig ist hierbei, dass Wohlbefinden höchst subjektiv und nicht statisch ist, sondern sich in Abhängigkeit des Kontexts und im Verlauf der Zeit verändern kann und daher einer **ständigen Neubewertung** bedarf.

## 2.2 Vereinbarkeit mit gesellschaftlichen Grundwerten

Je nach Einsatzgebiet können die Auswirkungen algorithmischer Systeme gesamtgesellschaftliche Relevanz haben, etwa auf die **demokratische Willensbildung**, die **Bürgernähe** staatlichen Handelns, auf den **Wettbewerb**, auf die **Zukunft der Arbeit** und auch auf die **digitale Souveränität** Deutschlands und Europas.

### Beispiel 4

*Bei der Entwicklung intelligenter Systeme haben diejenigen Anbieter eine privilegierte Startposition, die ihre Geschäftsmodelle auf großen Datenmengen aufbauen können, da viele Anwendungen algorithmischer Systeme auf eben solche Datenmengen angewiesen sind. Je mehr Daten durchforstet werden können, um so eher lassen sich Zusammenhänge und Erkenntnisse generieren. Zusammengenommen mit den für Plattformmärkte typischen Netzwerk-, Skalen- und Verbundeffekten beginnt sich ab einer gewissen Schwelle die Marktmacht von Unternehmen zu verfestigen, und es bilden sich Monopole. Dies versetzt Unternehmen schließlich in die Lage, den Marktzutritt neuer Akteure zu behindern und die marktregulierenden Kräfte des Wettbewerbs zu beeinträchtigen. Je nach Anwendungsbereich können Unternehmen dann gesellschaftliche Meinungsbildungsprozesse und Marktverhalten steuern. Um dem entgegenzuwirken und Rahmenbedingungen für einen fairen Wettbewerb zu schaffen, müssen die wettbewerbsrechtlichen Kontrollmechanismen neu justiert und gegebenenfalls nachgeschärft werden.*

Diese überindividuellen Folgewirkungen lassen sich nach Auffassung der DEK regelmäßig nicht allein durch staatliche Stellen und mit den Mitteln des Rechts in den Griff bekommen. Sie müssen vielmehr in allen Phasen der Gestaltung und des Einsatzes algorithmischer Systeme mitbedacht werden. **Entwickler, Unternehmen und Nutzer haben insoweit eine gesellschaftliche (Mit-)Verantwortung**. Insbesondere dort, wo entsprechende Folgewirkungen naheliegen, etwa im Falle algorithmischer Systeme, die die demokratirelevante Kommunikation zwischen Menschen berühren, bedarf es bereits im Gestaltungsprozess sorgfältiger Abschätzungen der Zwecke und der nicht-intendierten Nebenfolgen des Systems und die Prüfung der Frage, in wie weit die Funktion des Systems die Funktion der Demokratie, Grundrechte, das Sekundärrecht oder die Grundregeln des Rechtsstaats berühren kann. Soweit möglich, sollte sich bei der Technikgestaltung eine Kultur des „Einbaus“ der Grundprinzipien von Demokratie, Rechtsstaatlichkeit und Grundrechten in die Systemarchitektur etablieren.

Vieles im Zusammenspiel von Technik und Gesellschaft ist bisher freilich noch im Unklaren. Aus Sicht der DEK bedarf es daher vermehrter Forschungsanstrengungen, um die gesellschaftlichen Auswirkungen algorithmischer Systeme aufzuhellen und entsprechende Strategien zur Einhegung negativer Folgen zu entwickeln.

### 2.3 Nachhaltigkeit bei Gestaltung und Einsatz algorithmischer Systeme

Die Bewertung der individuellen und gesellschaftlichen Folgen algorithmischer Systeme muss auch eine zeitlich übergreifende und globale Perspektive einnehmen. Bei der Entscheidung über den Einsatz und die Gestaltung algorithmischer Systeme sind daher insbesondere auch Aspekte der **Nachhaltigkeit** und des **menschlichen Kompetenzerhalts** zu berücksichtigen. Diese sind wichtig für verbleibende menschliche Kontrollfunktionen (z.B. sog. Human-in-the-Loop-Prinzip), für den Ausfall algorithmischer Systeme in Ausnahmesituationen (z.B. im Katastrophenfall oder bei Cyberangriffen) und für die Innovationskraft künftiger Generationen (z.B. Entwicklung neuer digitaler Technologien). Es ist dabei in erster Linie eine Frage der Aus- und Fortbildung sowie der Bildung im Sinne eines lebenslangen Lernens, für entsprechende generelle Kompetenzen auch künftiger Generationen zu sorgen und schon die Ausbildung nicht auf die reine Anwenderperspektive zu beschränken.

Bildung und Förderung digitaler Kompetenzen fördern auch **soziale Nachhaltigkeit**. Gesellschaftliche Rahmenbedingungen etwa im Sinne von Institutionen und Verfahren sind so auszurichten, dass eine partizipative und inklusive Gestaltung algorithmischer Systeme und ihr dem Gemeinwohl dienender Einsatz gefördert werden.

Der Aspekt der nachhaltigen Entwicklung erfasst darüber hinaus die **ökologische Dimension**. Ungeachtet des positiven Beitrags, den algorithmische Systeme zum Umweltschutz leisten können, ist eine Minimierung des Bedarfs an elektrischer Energie und an bestimmten Ressourcen wie etwa „seltenen Erden“ sowie ihr effizienter Einsatz eine zentrale ethische Forderung.

**Ökonomische Nachhaltigkeit** erfordert eine Perspektive, die über ausschließlich kurzfristige wirtschaftliche Gewinne hinausweist und auch die langfristigen Auswirkungen berücksichtigt. So kann kurzfristiger kommerzieller Erfolg langfristig zu katastrophalen Auswirkungen führen, wie etwa die Weltfinanzkrise vor einigen Jahren gezeigt hat. Dies soll die Freiheit wirtschaftlicher Betätigung nicht einschränken, aber das Augenmerk auf die Verantwortung lenken, die im Rahmen einer sozialen Marktwirtschaft mit wirtschaftlichem Handeln verbunden ist.

Das Prinzip vorausschauender Verantwortung sowie Erwägungen der Gerechtigkeit und Solidarität sind im Hinblick auf Nachhaltigkeit bei der Gestaltung und dem Einsatz algorithmischer Systeme besonders zu berücksichtigen. Ebenso wie im Hinblick auf den Umgang mit Daten hat die **Risikofolgenabschätzung** für die ökologische, ökonomische und soziale Nachhaltigkeit bei der Gestaltung und dem Einsatz algorithmischer Systeme eine unverzichtbare Bedeutung.

### 2.4 Hohes Maß an Qualität und Leistungsfähigkeit

Algorithmische Systeme müssen gut und zuverlässig funktionieren, um die mit ihrer Hilfe verfolgten Zwecke zu erreichen. Dienen die Systeme dazu, ethisch wertvolle Zwecke zu befördern, kommt technischen und rechtlichen Vorgaben, die die **Hebung, Fortentwicklung und Sicherung des Stands der Technik** anstreben, eine ethische Qualität zu. Dort, wo die Systeme menschliche Aktivitäten unterstützen oder ersetzen, verbindet sich mit ihnen die Perspektive, auf diese Weise – unbeschadet des Eigenwerts menschlichen Handelns – ethische Grundsätze besser als bisher zu verwirklichen.



**Beispiel 5**

*Ein ethisch vertretbarer Einsatz algorithmischer Systeme im medizinischen Bereich setzt zunächst eine entsprechende medizinische Qualität der Technologien voraus, d.h. die Richtigkeit der Befunderhebung, die Treffsicherheit der Diagnose, die Erfolgswahrscheinlichkeit der empfohlenen Therapie oder die Erfolgsquote bei einem medizinischen Eingriff etc. müssen beim Einsatz des Systems grundsätzlich mindestens gleich gut und – angesichts des sensiblen Einsatzkontextes – idealerweise besser sein als beim Einsatz herkömmlicher Technologien und menschlicher Akteure.*

Die Steigerung von Qualität und Leistungsfähigkeit kann durch ganz unterschiedliche Maßnahmen erfolgen. Dazu gehören beispielsweise adäquate Risikomodelle, eine möglichst inklusive und partizipative Standardentwicklung, systemische Management- und Kontrollansätze sowie ein Prozessdesign, das auf stetige Verbesserung des Gesamtsystems hin ausgerichtet ist. Die Rolle jener menschlichen Akteure, die Teil des als sozioinformatisches Ensemble verstandenen algorithmischen Systems sind (→ oben 1), muss in diesem Kontext stets mitbedacht werden. Denn nach wie vor entfalten etliche algorithmische Systeme ihre Leistungsfähigkeit gerade im Zusammenspiel mit kritischen und fachkundigen Menschen. Teil einer an Qualität orientierten Systemgestaltung sind daher auch Mechanismen, die zur **Steigerung der menschlichen Fähigkeiten** beitragen und einem Abbau von Kompetenzen und kritischer Reflektionsfähigkeit und -bereitschaft, etwa im Zusammenhang mit einem Automation Bias, vorbeugen bzw. entgegenwirken. Beispiele für ein produktives und kompetenzerhaltendes Zusammenspiel von Mensch und Maschine finden sich etwa bei der algorithmengestützen bildgebenden Diagnostik im medizinischen Bereich.

**2.5 Gewährleistung von Robustheit und Sicherheit**

Algorithmische Systeme müssen robust und sicher sein, sonst lassen sich die mit ihnen verfolgten legitimen Zwecke nicht oder nur unter Inkaufnahme potenzieller Schäden an ethischen und rechtlichen Gütern und schutzwürdigen Interessen erreichen. Aus ethischer Sicht partizipiert das Postulat robuster und sicherer Systemgestaltung und eines entsprechenden Systemeinsatzes daher an der Wertigkeit der jeweiligen Systemzwecke sowie am Schutzbedarf der vom System verwendeten Daten. Aus diesem Grund sind allerdings auch die Anforderungen an die Robustheit und Sicherheit nicht für alle Systeme identisch. Die spezifischen Anforderungen können vielmehr je nach dem **konkreten Schutzbedarf und dem Einsatzkontext** verschieden ausgeprägt sein.

**Beispiel 6**

*Nicht belastbare oder unsichere Systeme, die in Steueranlagen eingesetzt werden, können unmittelbar Personen oder die Umwelt bedrohen, etwa wenn sie den Schadstoffausstoß von Industrieanlagen regeln, Roboter steuern oder autonome Fahrzeuge im Verkehr lenken. Ein Fehlversagen kann hier sogar zu Schäden für wichtige Rechtsgüter wie Leib und Leben führen. Um dies zu verhindern, gilt es, Prozesse zu initialisieren, die den gegenwärtigen Stand der Technik definieren, Rechtsnormen zu erlassen, die die Orientierung am Stand der Technik verbindlich machen, und Maßnahmen zu implementieren, die die effektive Durchsetzung des Standards garantieren.*

Robuste und sichere Systemgestaltung umfasst sowohl die **Sicherheit des Systems** gegen Einflüsse von außen (z.B. durch Verschlüsselung, Anonymisierung etc.) als auch den **Schutz der Menschen und der Umwelt vor negativen Einflüssen durch das System** (insbesondere durch einen systematischen Risikomanagementansatz, z.B. auf der Grundlage einer Risikofolgenabschätzung). Sie muss zudem alle Phasen der Datenverarbeitung und alle technischen und organisatorischen Komponenten einbeziehen. Risiken können sich dabei nicht nur aus der technischen Gestaltung, sondern auch aus Fehlern ergeben, die menschliche Entscheidungen im Umgang mit algorithmischen Systemen mit sich bringen. Da algorithmische Systeme und ihre Einbettung in die sonstige Informationstechnik einer Organisation nicht statisch sind, wird zudem ein **Managementsystem** benötigt, das die Wirksamkeit der Maßnahmen angesichts veränderter Bedingungen, beispielsweise neu bekannt gewordener Risiken, überprüft und sicherstellt.

## 2.6 Minimierung von Bias und Diskriminierung als Vorbedingung gerechter Entscheidungen

Ein wesentliches Ziel der Regulierung algorithmischer Systeme besteht darin, sicherzustellen, dass die den algorithmischen Systemen zu Grunde liegenden Entscheidungsmuster keine systematischen Verzerrungen (Biases) aufweisen, die zu diskriminierenden und ungerechten Entscheidungen führen. Dabei ist zunächst festzuhalten, dass verzerrte, diskriminierende oder ungerechte Entscheidungen auch bei Einsatz herkömmlicher Technologien und menschlicher Akteure zu beobachten sind. Im Gegensatz zu vorurteilsbehafteten Entscheidungen einzelner Menschen besteht bei algorithmischen Systemen aber die Gefahr, dass der einem System inhärente Effekt über eine skalenmäßig große Anwendung des Systems eine Breitenwirkung entfaltet, die einzelne menschliche Entscheider nie erreichen könnten. Vor diesem Hintergrund ist die Diskussion um Bias und Diskriminierung durch algorithmische Systeme nach Auffassung der DEK **auch als Chance zu begreifen**, in bestehenden Entscheidungskontexten bereits bestehende Probleme aufzudecken und ganz allgemein zu besseren Entscheidungsprozessen zu gelangen.

### Beispiel 7

*Ein zur Erkennung von Hautkrebs eingesetztes algorithmisches System wurde vorwiegend an Patienten weißer Hautfarbe trainiert und die Wahrscheinlichkeit einer korrekten Erkennung von Hautkrebs ist bei Patienten mit weißer Hautfarbe daher signifikant höher als bei Patienten mit anderer Hautfarbe. Als Medizinprodukt würde ein solches System nur für die Anwendung an weißhäutigen Patienten zugelassen werden. Der gleiche Effekt wäre freilich zu verzeichnen, wenn ein Dermatologe seine Ausbildung und klinische Praxis allein in einem bestimmten Kulturkreis erworben hat. Letztlich ist in beiden Fällen darauf zu achten, dass alle Patienten unabhängig von ihrer Hautfarbe medizinisch gut versorgt werden.*

Auch in Fällen, in denen bei der Entwicklung algorithmischer Systeme keine unmittelbare Diskriminierungsabsicht vorliegt, kann es zu diskriminierenden Entscheidungen kommen, also zu solchen, die bestimmte Gruppen ungerechtfertigterweise systematisch benachteiligen. Insbesondere bei Maschinellem Lernen röhrt das Problem vielmehr daher, dass die Systeme anhand vorhandener Daten Modelle erlernen. Die daraus resultierenden Prognosen und Empfehlungen **schreiben die Vergangenheit in die Zukunft fort**, wodurch bestehende gesellschaftliche Ungerechtigkeiten durch den Einbau inscheinbar neutrale Technologien verschleiert und potenziell verstärkt werden können.

### Beispiel 8

*Ein zur Bewertung von Bewerbungen um eine Führungsposition eingesetztes algorithmisches System wurde mit den Daten derjenigen Führungskräfte trainiert, die sich im betreffenden Unternehmen in den letzten Jahrzehnten bewährt haben. Da in den letzten Jahrzehnten vorwiegend männliche Führungskräfte eingestellt wurden, bewertet das System, das mit diesem Datensatz trainiert wurde, männliche Bewerber durchgehend besser als gleich qualifizierte Bewerberinnen.*



Unter dem englischen Stichwort **Bias** versammeln sich eine **Vielzahl systematischer Verzerrungen**, die unterschiedlicher Natur sind und unterschiedliche Ursachen haben. Bei menschlichen Akteuren geht es sowohl um kognitive Verzerrungen, als auch um gesellschaftliche Vorannahmen, Vorurteile oder Stereotypen, welche Entscheidungsfindungen negativ beeinflussen können. In Bezug auf algorithmische Systeme kann sich Bias auf die technische Abbildung eben jener gesellschaftlichen Vorannahmen, Vorurteile oder Stereotypen beziehen. Diese Abbildung kann v.a. im Kontext von Maschinellem Lernen an mehreren Stellen erfolgen. Häufig führt eine ungenügende Repräsentativität oder eine geringe Fallzahl einer gesellschaftlichen Gruppe in den Trainingsdaten zu Verzerrungen, indem die Spezifika dieser Gruppe im Rahmen der Entwicklung nicht ausreichend erkannt und damit berücksichtigt werden. Jenseits der verwendeten Trainingsdaten können auch andere technisch-methodische Entscheidungen, z.B. bzgl. der Zielvariablen oder Labels, zu diskriminierenden Modellen und dadurch ungerechten Entscheidungen führen. Zuletzt können sich auch erst im Einsatz von Systemen Probleme ergeben, z.B. wenn algorithmische Systeme unter veränderten gesellschaftlichen Rahmenbedingungen oder in nicht vorhergesehenen Einsatzkontexten genutzt werden.

Besonders kritisch sind unter dem Gesichtspunkt der Diskriminierung algorithmische Systeme, die rechtlich als besonders **sensibel anerkannte Kategorien von Daten** wie Geschlecht oder Herkunft **direkt** verwenden. Eine direkte Verwendung sensibler Informationen kann, je nach Anwendungsgebiet, wichtig für eine korrekte Datenverarbeitung sein und ist – im Rahmen der rechtlichen Grenzen – vielfach auch zulässig.

### Beispiel 9

*Viele Systeme zur Krankheitsdiagnose kennen und berücksichtigen das Geschlecht oder das Alter eines Patienten. Auch für die Umsetzung von Geschäftsstrategien, etwa dem Ausbau des Geschäfts in einer Altersgruppe, Berufsgruppe oder einer Region, können sensible Merkmale im Rahmen einer Geschäftsentcheidung Verwendung finden, wenn sie beispielsweise ein Kundensegment definieren, für das vereinfachte Annahmekriterien gelten.*

Ebenfalls kritisch kann aber auch die Verwendung von Informationen sein, die sensible Kategorien **indirekt** kodieren.

### Beispiel 10

*Im Rahmen der Schätzung der Kreditwürdigkeit wird das Haushaltseinkommen als Information verwendet. Dieses fällt in Deutschland für die Geschlechter im Mittel unterschiedlich aus. In der Folge kann ein algorithmisches System, welches das Haushaltseinkommen verwendet, zu unterschiedlichen Verteilungen der Schätzungen für die Kreditwürdigkeit von Männern und Frauen gelangen.*

Diskriminierung vollständig zu verhindern, ist selbst hinsichtlich rechtlich anerkannter Kategorien wie Geschlecht oder Herkunft im Kontext von algorithmischen Systemen schwierig. Darüber hinaus kann der Einsatz algorithmischer Systeme dazu führen, dass **ganz neue nach mehr oder weniger zufälligen Merkmalen zusammengewürfelte Gruppen** mit einer gewissen Systematik und ohne rechtfertigenden Grund von gesellschaftlichen Gütern ausgeschlossen werden oder mit sonstigen negativen Folgen konfrontiert werden. Vor diesem Hintergrund ist eine Sensibilisierung für komplexe bedingte diskriminierende Effekte für alle an der Entwicklung und dem Einsatz eines solchen Systems Beteiligten erforderlich, damit sie solche so weit wie möglich vermeiden oder ihnen gegensteuern können (→ siehe unten ).

Allerdings haben technische Maßnahmen zur Minimierung von Diskriminierung selbst bei der Anwendung ständiger Verbesserungsprozesse Grenzen, u.a. weil sich unterschiedliche technische Fairnessziele nicht gleichzeitig erfüllen lassen. Welche Kriterien für Nicht-Diskriminierung und Gerechtigkeit in welchem Kontext angemessen sind, ist keine technische, sondern eine gesellschaftliche und politische Frage. Daher dürfen diese Entscheidungen auch nicht allein den Technik-Entwicklern überlassen werden. Stattdessen muss sie Bestandteil einer künftigen Regulierung algorithmischer Systeme werden und sich in den Betreiberpflichten der Verantwortlichen manifestieren. Bedingung dafür ist, dass die **Kriterien kontextspezifisch und demokratisch ausgehandelt** werden.

Die genaue Analyse algorithmischer Systeme ist schwierig. Um Diskriminierungen erkennen und vermeiden zu können, müssen Verantwortliche und Kontrollstellen die Möglichkeiten haben, sich ein Bild des algorithmischen Systems sowohl im Rahmen seiner Entwicklung als auch im Zuge seines produktiven Einsatzes über eventuell auftretende ungewollte Diskriminierungseffekte zu machen. Durch Verfahren wie **Risikofolgenabschätzung und Output-Analysen** können solchen Effekte identifiziert werden.

Es besteht ein Spannungsverhältnis zwischen den Vorgaben zur Einschränkung in der Erhebung und Speicherung diskriminierender Merkmale und dem Anliegen, dass es möglich bleibt, etwaige diskriminierende Effekte festzustellen oder eine Nicht-Diskriminierung belegen zu können. Diese verschiedenen Anforderungen müssen im Einzelfall in einen Ausgleich gebracht werden, was auch Einfluss auf Tests in verschiedenen Phasen des Lebenszyklus der Systementwicklung haben kann; ein standardmäßiges Mitsammeln von allen potenziell diskriminierenden und damit sensiblen Informationen nur zum Zwecke eines Nachweises, dass aufgrunddessen keine Diskriminierung stattfindet, wäre nicht gerechtfertigt. Hier bedarf es verstärkter Anstrengungen, eine **praktische Konkordanz von Anti-Diskriminierungsrecht und Datenschutzrecht** herzustellen.

## 2.7 Transparenz, Erklärbarkeit und Nachvollziehbarkeit

Für eine belastbare ethische und rechtliche Bewertung algorithmischer Systeme ist es essenziell, dass ausreichend Informationen über dessen Reichweite, Funktionsweise, Datengrundlage und Datenauswertung zur Verfügung stehen. **Nur ein im Ansatz transparentes System lässt sich darauf überprüfen, ob es einen legitimen Einsatzzweck verfolgt.** Je nach Art und Adressat möglicher Transparenzverpflichtungen kommen dem Transparenzgrundsatz weitere zentrale Funktionen zu. In Bezug auf die Öffentlichkeit muss hinreichend Transparenz hergestellt werden, um eine ausreichende Informationsgrundlage für einen gesellschaftspolitischen Diskurs über algorithmische Systeme führen zu können. Aufsichtsbehörden oder sonstige Kontrollstellen müssen in der Lage sein, entscheiden zu können, ob die rechtlichen und technischen Vorgaben beim Einsatz algorithmischer Systeme eingehalten werden bzw. wurden. Einzelne Bürger müssen informierte und souveräne Entscheidungen bezüglich der Verwendung algorithmischer Systeme treffen können und im Falle von negativen Auswirkungen auf ihre Freiheiten und Rechte beurteilen können, ob und inwiefern Sie von ihren Rechten Gebrauch machen wollen. Auch das ist eine Konsequenz des ethischen Prinzips der digitalen Selbstbestimmung.

Angesichts immer komplexerer Systeme ist die Forderung nach Transparenz in der Praxis allerdings damit konfrontiert, dass es selbst für Fachleute oft kaum mehr möglich ist, alle Einzelkomponenten eines Systems und ihr Zusammenspiel vollständig zu durchdringen und in angemessener Zeit **nachzuvoilziehen**. Insbesondere bei einzelnen Methoden des Maschinellen Lernens ist es beim heutigen Stand von Wissenschaft und Technik schwierig, anzugeben, welche Eingabe zu einer spezifischen Ausgabe des Systems geführt hat. Hinzu kommt, dass selbst technisch einfache algorithmische Systeme oftmals in komplexe sozioinformatische Ökosysteme eingebunden sind, d.h. informations- und arbeitsteilige Prozesse, in denen eine Vielzahl von Herstellern und Betreibern mitwirkt.



### Beispiel 11

Die Anzeige einer individualisierten Online-Werbung ist das Ergebnis komplexer Prozesse, in denen die Auslieferung und Bezahlung der Werbung auf der Basis von verhaltensbasierter Analyse und Segmentierung erfolgt. Hierzu werden insbesondere sog. Analytics-Dienste genutzt, die webseitenübergreifend durch Einbinden des entsprechenden Programmcodes (wie beispielsweise JavaScript-Code zum Tracking) von den Seitenanbietern eingesetzt werden. Die Komponenten solcher Systeme sind auch nicht statisch, sondern können sich verändern, z.B. wenn Hersteller neue Versionen bereitstellen oder wenn es sich um adaptierende bzw. selbstlernende Systeme handelt.

Die allgegenwärtige Komplexität kann jedoch das Ziel, algorithmische Systeme transparent zu gestalten, nicht widerlegen oder Intransparenz rechtfertigen. Ebenso wie die erwähnten Rechtsgründe sind sie gleichwohl bei der Ausgestaltung etwaiger Informationsrechte und Transparenzpflichten zu berücksichtigen, die sich am rechtlich und tatsächlich Möglichen orientieren müssen. **Transparenz als Prinzip** verlangt dabei auch, die Technik so fortzuentwickeln, dass eine Offenlegung von Informationen einfacher wird – etwa durch Verwendung von Open-Source-Software und Open-Hardware – und Ansätze zu entwickeln, die Komplexität reduzieren. Hier ist auch die Forschung gefordert. Unter dem Stichwort „Explainable AI“ arbeiten Forscherinnen und Forscher mit wachsendem Erfolg daran, aussagekräftige Erkenntnisse über die internen Prozesse algorithmischer Systeme zu generieren.

Auch rechtliche Gesichtspunkte können bestimmten Formen der Offenlegung von Informationen über algorithmische Systeme **Grenzen** ziehen. Quellcodes und Hardware-Designs sind oftmals als Geschäftsgeheimnisse geschützt. Betreiber haben zudem vielfach ein legitimes Interesse daran, Manipulationen an ihren Systemen zu verhindern. Sofern algorithmische Systeme personenbezogene Daten verarbeiten, kann auch das Datenschutzrecht dem Informationsinteresse der Öffentlichkeit oder betroffener Bürger Grenzen ziehen. Sofern es allerdings bei der Transparenzanforderung an die Systeme um die Offenlegung des Quellcodes geht, der als solcher keine personenbezogenen Daten enthält, steht das Datenschutzrecht der Offenlegung nicht entgegen.

Die Forderung nach Transparenz muss stets die **unterschiedlichen Kompetenzniveaus** der potenziell an Transparenz Interessierten berücksichtigen. So kann die Offenlegung des Computercodes Aufsichtsbehörden, die entsprechende Kontrollen vornehmen, ein Verständnis des Systems entscheidend erleichtern. Laien haben hingegen vielfach eher ein Bedürfnis nach klar verständlich aufbereiteten Informationen über grundlegende Eigenschaften des Systems, die es ihnen ermöglichen, eine alltagstaugliche Risikoeinschätzung durchzuführen. Zugleich beschränkt sich ihr Interesse selten auf das System „an sich“. Schon um in Zukunft etwaige negative Entscheidungen zu vermeiden, wird zusätzlich eine **Erklärung** verlangt, wie die sie konkret betreffende Entscheidung zustande gekommen ist und welche Faktoren dabei welches Gewicht entfaltet haben. Die spezifische Ausgestaltung der Vorgaben für Transparenz und Erklärbarkeit sollte sich dabei am Verständnishorizont der Betroffenen orientieren und für diese stets **nachvollziehbar** sein. In diesem Sinne sichern Vorgaben zu Transparenz und Erklärbarkeit die Handlungsfähigkeit und Selbstbestimmung der Bürger.

## 2.8 Klare Rechenschaftsstrukturen

Ebenso wie die Herrschaft über Daten die Pflicht begründet, für diese Macht Rechenschaft abzulegen, muss auch die Möglichkeit, über algorithmische Systeme zu verfügen, mit der Bereitschaft einhergehen, **für das eigene Handeln Rede und Antwort zu stehen**, d.h. gegebenenfalls auch zu **haftan**.

Erneut ist es die Komplexität algorithmischer Systeme, die in der Praxis Verantwortungszuschreibungen erschweren kann. Hersteller der Hard- oder der Software, Datenzulieferer, Algorithmenentwickler, Betreiber einzelner Komponenten, Auftraggeber, Anwender – jeweils als Organisation oder als darin konkret Beschäftigte – leisten ihren Beitrag zum System. Vielfach werden Komponenten verwendet, die sich ohne Kenntnis oder Kontrolle des Einsetzenden verändern können, etwa durch wichtige Updates für die Informationssicherheit. Oftmals sind die Beteiligten zudem an verschiedenen Orten auf der ganzen Welt ansässig. Es bedarf Anstrengungen auf allen Ebenen, um einer Diffusion der Verantwortung entgegenzuwirken und **Rechenschaftsstrukturen zu etablieren**, beginnend bei der technischen Gestaltung der Systeme bis hin zu rechtlichen Vorgaben, etwa in Form des aus dem Datenschutzrecht bekannten Instituts der „gemeinsamen Verantwortlichkeit“ (Artikel 26 DSGVO).

## 2.9 Ergebnis: Verantwortung geleitete Abwägung

Die Bewertung algorithmischer Systeme in ethischer Hinsicht ist **in der Praxis überaus komplex**. Dies ist bedingt durch die Vielzahl der zu berücksichtigenden Faktoren sowie durch die Tatsache, dass in einem konkreten Anwendungsbereich unterschiedliche Individuen jeweils „besser“ und „schlechter“ gestellt werden können. Entsprechendes gilt für gesellschaftliche Folgewirkungen und Nachhaltigkeitsaspekte, die sich selten eindeutig als „positiv“ oder „negativ“ klassifizieren lassen werden. Das bedeutet jedoch nicht, dass der Mensch seine Urteilskraft aufgeben darf. Dort, wo Abwägungen schwierig werden, sind vielmehr alle bei ihren Wertungen und Entscheidungen zur besonderen Sorgfalt angehalten. Dort, wo algorithmische Anwendungen (perspektivisch) eine so überragend große Leistungsfähigkeit und Reichweite entwickeln, dass Fragen über die Zukunft der Menschheit entstehen, geraten Abwägungen der Chancen und Risiken zunehmend an Grenzen und erfordern grundsätzlichere anthropologische und ethische Auseinandesetzungen. Gerade hier ist das Prinzip der vorausschauenden Verantwortung von grundlegender Bedeutung.

Bei alldem stellt der **demokratische Prozess** Mittel und Wege bereit, um einander widersprechende Überzeugungen zum Ausgleich zu bringen – idealerweise unterstützt durch besondere **deliberative Prozesse und Institutionen**, in denen sich die Gesellschaft in einer möglichst inklusiv und partizipativ ausgestalteten Form über den Umgang mit den Herausforderungen durch algorithmische Systeme vergewissern kann.



Nur selten dürfte die Situation gegeben sein, dass eine Abwägung zwischen menschlichem Handeln und dem Einsatz eines algorithmischen Systems verzichtbar ist, weil dieses in allen ethisch relevanten Belangen ein „besseres“ Ergebnis erzielt als menschliche Akteure, die herkömmliche Technologien nutzen. Dort, wo dies der Fall ist, gilt nach Auffassung der DEK allerdings, dass der Einsatz algorithmischer Systeme **ethisch geboten ist**, denn ein genereller ethischer Vorzug menschlichen Handelns vor dem Einsatz von Maschinen zulasten des Schutzes wichtiger Rechtsgüter ist nach Auffassung der DEK nicht gerechtfertigt. Regelmäßig werden bei der Frage, ob menschliches oder maschinelles Handeln zu bevorzugen ist (→ s. dazu auch Teil B, 1), jedoch weitere Faktoren wie etwa emotionales Wohlbefinden von Menschen, menschlicher Kompetenzerhalt und nachhaltige Entwicklung zu berücksichtigen sein, die letztlich doch wieder eine Abwägung erforderlich machen. Diese Abwägung kann zulasten, aber auch zugunsten des algorithmischen Systems ausgehen.

Sofern hingegen nach Berücksichtigung aller Umstände durch den Einsatz eines algorithmischen Systems zu lasten wichtiger Rechtsgüter ein schlechteres Ergebnis erzielt wird als bei dem Einsatz herkömmlicher Technologien und menschlicher Akteure – etwa, weil mehr Fehlentscheidungen getroffen werden – und bloß ein Gewinn an Effizienz oder Bequemlichkeit entsteht, ist der Einsatz algorithmischer Systeme im Grundsatz **ethisch abzulehnen**. Ethisch vertretbare Ausnahmen können in diesem Fall aus ökonomischen Erwägungen heraus allerdings ausnahmsweise hinzunehmen sein, wenn einer nur minimalen Beeinträchtigung ein außergewöhnlich hohes Einsparungspotenzial gegenübersteht, das dem Wohle der Allgemeinheit zugute kommt.

---

### Beispiel 12

*Führt der Einsatz eines diagnostischen algorithmischen Systems in einem bestimmten klinischen Bereich dazu, dass nur 2 % der Patienten versterben, während infolge menschlicher Fehldiagnosen 10 % aller Patienten versterben würden, wäre der Einsatz des Systems – je nach den Umständen des Einzelfalls – ethisch geboten, auch wenn dadurch leichte, aber verschmerzbare Einbußen beim emotionalen Wohlbefinden der Patienten einträten und zusätzliche Maßnahmen zum menschlichen Kompetenzerhalt ergriffen werden müssten.*

---

### 3. Empfehlung eines risikoadaptierten Regulierungsansatzes

Aus regulatorischer Sicht legt die Tatsache, dass algorithmische Systeme je nach Einsatzzweck, Leistungsfähigkeit, Robustheit und Sicherheit sowie mit Blick auf ihre Wirkungen ethisch sehr unterschiedlich zu bewerten sind, einen **risikoadaptierten Regulierungsansatz<sup>1</sup>** nahe. Dieser folgt dem Prinzip, dass ein **steigendes Schädigungspotenzial** algorithmischer Systeme mit **wachsenden Eingriffstiefen** der regulatorischen Instrumente einhergeht. Das Risiko-Spektrum algorithmischer Systeme reicht dabei von solchen, deren Anwendung allenfalls ein geringes Risiko birgt, bis hin zu Systemen, die zu irreversiblen Schäden für Individuen und Gesellschaft führen können. Ursache für die Risiken können etwa nicht adäquate Modelle, eine ungeeignete Datengrundlage insbesondere bei selbstlernenden Systemen oder unpassende Grundannahmen und Gewichtungen sein (→ oben 2.3 und 2.6).

Mögliche **Schäden** durch algorithmische Systeme können unterschiedlicher Natur sein, etwa finanziell, immateriell oder physisch. So können einzelne Anwendungen potenziell schwerwiegende finanzielle Schäden verursachen (etwa Kredit- oder Versicherungskonditionen), Chancen der Teilhabe beeinflussen (etwa Diskriminierung bei Stellenvergaben) sowie Grundrechtsverletzungen und Risiken für Leben und Gesundheit von Verbrauchern nach sich ziehen (beispielsweise bei Pflegerobotern oder Mobilitätsanwendungen).

Übergreifendes Ziel rechtlicher Regulierung des Einsatzes algorithmischer Systeme ist es, schädliche Effekte auf individueller und überindividueller Ebene zu vermeiden. Insbesondere dort, wo algorithmische Systeme grundrechtssensible Sachverhalte berühren, bedarf es dazu auch gesetzlicher Vorgaben für die Gestaltung der Systeme. Anzustreben ist dabei eine Regulierung, die so viel wie nötig und zugleich so wenig wie möglich vorschreibt, um Innovation und Kreativität nicht zu behindern, gleichzeitig aber den Schutz grundlegender Rechte, Freiheiten und Werte sichert. Eine **effiziente und sachgerechte Regulierung** kann dazu beitragen, das Vertrauen der Bevölkerung hinsichtlich des Einsatzes algorithmischer Systeme zu stärken. In der öffentlichen Wahrnehmung gelten insbesondere selbstlernende Systeme als nicht kontrollierbar, was zu einer entsprechenden Skepsis vor der Technologie als solcher beiträgt.<sup>2</sup>

Primäre Adressaten der rechtlichen Regulierung sind nach Auffassung der DEK die **Hersteller** und **Betreiber** algorithmischer Systeme. Aufgrund der unmittelbaren Grundrechtsbindung des Staates ist bei der näheren Ausgestaltung der Regulierung allerdings zwischen **privatem und staatlichem Einsatz** algorithmischer Systeme zu differenzieren (→ dazu insb. unten 7). Angesichts des Modell- und Vorbildcharakters staatlichen Handelns wird der Bundesregierung empfohlen, beim Einsatz algorithmischer Systeme für staatliche Zwecke besondere Sorgfalt walten zu lassen.

#### 3.1 Systemkritikalität und Systemanforderungen

Ein risikoadaptierter Regulierungsansatz kann durch die Orientierung an dem Modell der Kritikalität eines algorithmischen Systems konkretisiert werden. Die **Systemkritikalität** setzt am Schädigungspotenzial des Systems an. Dieses bestimmt sich aus der Schwere und der Eintrittswahrscheinlichkeit des zu befürchtenden Schadens.

1 Vgl. hierzu insbesondere Tobias Krafft / Katharina Zweig - Transparenz und Nachvollziehbarkeit algorithmenbasierter Entscheidungsprozesse, Studie im Auftrag des Verbraucherzentrale Bundesverband e.V. (vzbv), 22.01.2019, S. 18 ff. (abrufbar unter: [https://www.vzbv.de/sites/default/files/downloads/2019/05/02/19-01-22\\_zweig\\_krafft\\_transparenz\\_adm-neu.pdf](https://www.vzbv.de/sites/default/files/downloads/2019/05/02/19-01-22_zweig_krafft_transparenz_adm-neu.pdf)).

2 Sarah Fischer / Thomas Petersen: Was Deutschland über Algorithmen weiß und denkt – Ergebnisse einer repräsentativen Bevölkerungsumfrage, Bertelsmann Stiftung, 2018 (abrufbar unter: <https://www.bertelsmann-stiftung.de/de/publikationen/publikation/did/was-deutschland-ueber-algorithmen-weiss-und-denkt/>).



Die **Schwere** zu befürchtender Schäden, etwa im Falle einer Fehlentscheidung, bezieht sich u.a. auf die Wertigkeit der betroffenen Rechtsgüter und Interessen (insbesondere z.B. das Recht auf informationelle Selbstbestimmung sowie freie Entfaltung der Persönlichkeit, das Grundrecht auf Leben und körperliche Unversehrtheit sowie auf Gleichbehandlung) und die Tiefe des potenziellen Schadens durch eine Rechtsverletzung. Zudem ist für die Bestimmung der Schwere des potenziellen Schadens die besondere Sensibilität der verwendeten Daten, die Höhe eines möglichen Schadens für Einzelne oder Gruppen (einschließlich immaterieller Schäden bzw. monetär schwer zu beiferner Nutzeneinbußen), die Zahl der Betroffenen, die Summe der potenziellen Schäden und der gesamtgesellschaftliche Schaden, der über eine reine Summierung von Einzelschäden weit hinausgehen kann, zu berücksichtigen. Dabei sollen die Auswirkungen des Einsatzes des algorithmischen Systems, je nach Anwendungsbereich, hinsichtlich ihrer ökologischen, sozialen, psychologischen, kulturellen, ökonomischen und juristischen Dimensionen betrachtet werden. Maßstabsetzend für die Wertigkeit sind dabei die allgemeinen ethischen Werte und Prinzipien (→ oben Teil B).

Die **Wahrscheinlichkeit** eines Schadeneintritts hängt auch von den nachfolgenden Systemeigenschaften und Faktoren ab:

- Rolle algorithmischer Berechnungen im Entscheidungsprozess (von der bloßen Inspiration menschlicher Akteure ohne Richtigkeitsanspruch bis hin zur algorithmdeterminierten Entscheidung, → siehe oben 1);
- Komplexität der Entscheidung (vom schlichten deterministischen Abbild der Realität über eine probabilistische Einschätzung der Realität bis hin zur multifaktoriellen und nicht-determinierten Prognose einer künftigen Realität);
- Wirkungen der Entscheidung (von einem bloß abstrakt denkbaren Handlungskontext über einen konkreten Handlungskontext bis hin zur unmittelbaren Implementierung); und
- Reversibilität der Wirkungen (von voller Reversibilität bis hin zur Irreversibilität).

Schwere und Wahrscheinlichkeit zu befürchtender Schäden können auch abhängig sein vom **staatlichen oder privaten Charakter** des Handelnden und – gerade in wirtschaftlichen Zusammenhängen – von der **Marktmacht** desjenigen Akteurs, der sich des algorithmischen Systems bedient, weil der staatliche oder private Charakter sowie die Marktmacht nicht nur für Grundrechtsbindung und gesamtgesellschaftlichen Schaden relevant ist, sondern auch über allfällige Ausweichmöglichkeiten betroffener Personen entscheidet. Mit der **Abhängigkeit der betroffenen Personen** von einem algorithmischen System, etwa hinsichtlich des Zugangs zu Märkten, Gütern und Dienstleistungen, steigt dessen Kritikalität. Die Beschränkung der Auswahlmöglichkeiten kann auf verschiedene Ursachen zurückzuführen sein. Zu nennen sind etwa Netzwerk-, Skalen- und Verbundeffekte, die sich wiederum in Marktmacht und (fehlenden) äquivalenten Alternativangeboten niederschlagen können.

Je höher die Systemkritikalität eines Systems ist, desto höher sind die **Anforderungen**, die aus regulatorischer Sicht an dieses System zu stellen sind. Diese Anforderungen werden insbesondere durch

- a) Korrektur- und Kontrollinstrumente;
- b) Vorgaben für die Transparenz algorithmischer Systeme und die Erklärbarkeit und Nachvollziehbarkeit der Ergebnisse; und
- c) Regelungen zur Zuordnung von Verantwortlichkeit und Haftung im Zusammenhang mit Entwicklung und Einsatz algorithmischer Systeme

ausgestaltet (→ siehe unten 4, 5 und 8).

Die Vielfalt, Komplexität und Dynamik algorithmischer Systeme stellt die Regulierung vor große Herausforderungen. Sie kann sich nicht auf einen beschränkten Instrumentenkasten stützen, sondern muss, je nach Kritikalität des Systems, **auf unterschiedlichen Regulierungsebenen ganz unterschiedliche Korrektur- und Kontrollinstrumente** in Stellung bringen, um die Ziele der Regulierung zu erreichen und die Risiken der Systeme beherrschbar zu machen. Das Spektrum möglicher Instrumente reicht dabei vom Verzicht auf spezialgesetzliche Vorgaben und „weiche“ Anreize für Selbstregulierung über behördliche Kontrollrechte bis zum Vorbehalt der menschlichen Letztentscheidung oder dem Verbot bestimmter Einsatzzwecke und -kontexte algorithmischer Systeme.

Zentrale Bausteine eines Korrektur- und Kontrollregimes für algorithmische Systeme sind Vorgaben für die **Transparenz** der Systeme und die **Erklärbarkeit** sowie **Nachvollziehbarkeit** ihrer Ergebnisse (→ oben 2.7). Auch insoweit bestimmt die Kritikalität des Systems die Reichweite etwaiger Informationsrechte und -pflichten. Wie die geforderten Informationen nachvollziehbar kommuniziert werden können, unterscheidet sich je nach Adressatenkreis der Systeme und damit auch nach Einsatzzweck und -kontext.

Aus ethischer und rechtlicher Sicht ist für den Umgang mit algorithmischen Systemen entscheidend, dass zu jedem Zeitpunkt eine klare Zuordnung von **Verantwortung** ihrer Auswirkungen zu menschlichen Entscheidungsträgern gewährleistet ist. Hierbei kommt insbesondere auch Regelungen zur **Haftung** eine zentrale Bedeutung zu, wobei die Frage nach der angemessenen Ausgestaltung eines Haftungsregimes für bestimmte digitale Produkte, Inhalte und/ oder Dienstleistungen erneut auch mit Blick auf die Kritikalität des Systems erfolgen muss (→ unten 8).

An der **Konkretisierung und Ausgestaltung** dieser differenzierten **Regulierungsanforderungen** müssen im Sinne der von der DEK eingenommenen Governance-Perspektive **alle relevanten Akteure** – Staat, Unternehmen, Entwickler und die Bevölkerung – partizipieren. Die DEK weist darauf hin, dass auch ohne spezielle Regulierung der Einsatz algorithmischer Systeme an den allgemeinen Rechtsnormen zu messen ist. Hierzu gehört insbesondere das zivilrechtliche Haftungsrecht, das bei Handlungen, die rechtlich geschützte Interessen verletzen, grundsätzlich zum Schadensersatz verpflichtet. Auch finden die Regelungen des Gesetzes gegen den unlauteren Wettbewerb Anwendung, etwa im Falle von Irreführungen von Verbrauchern, sowie das Strafrecht, wenn mithilfe algorithmischer Systeme Straftaten begangen werden. Bei der Prüfung der Voraussetzung dieser Normen kommt der Kritikalität der Systeme und den daraus abzuleitenden Systemanforderungen auch nach allgemeinen Maßstäben rechtliche Bedeutung zu.

Algorithmische Systeme kommen zum Einsatz, um spezifische Funktionen zu erfüllen. Um die Systemkritikalität zu bewerten, ist daher auch die **ethische Bewertung dieses Zwecks** von ausschlaggebender Bedeutung. Ist der Einsatzzweck ethisch unvertretbar, etwa weil er grundlegende Rechte und Freiheiten verletzt oder gegen die freiheitlich-demokratische Grundordnung verstößt, ergeben sich „rote Linien“ oder „absolute Grenzen“ – für algorithmische Systeme ebenso wie für Menschen. So ist beispielsweise ein der politischen Manipulation, dem Betrug oder der kollusiven Preisabsprache dienendes algorithmisches System per se als ethisch verwerflich anzusehen.



Dabei sind Einsatzzwecke oft vielschichtig, und einzelne ihrer Facetten – insbesondere was Nebenzwecke betrifft – können ethisch jeweils unterschiedlich zu bewerten sein. Die Herausarbeitung eines für die Bewertung maßgeblichen Einsatzzwecks setzt insofern oft schwierige **Wertungsentscheidungen** voraus. Die Bewertung des Einsatzzwecks algorithmischer Systeme wird bei digitalen Produkten dadurch erschwert, dass sich die Phasen der Entwicklung und der Implementierung im Markt zunehmend überschneiden; auch kann die Zweckbestimmung eines Produkts nach seiner Implementierung im Markt durch Updates oder den Einsatz in anderen Anwendungskontexten verändert werden.

## Komplexe Zweckbestimmung bei Medienintermediären

Manche Medienintermediäre, wie Suchmaschinen, sind im Zeitalter des Internets unverzichtbar, weil sie den Zugang zu Informationen im Netz ermöglichen, die Informationsflut kanalisieren und dem Einzelnen die Nutzung des Internet faktisch überhaupt erst ermöglichen. Insoweit sind ihre Zwecke wünschenswert und ethisch unkritisch. Medienintermediäre können aber in ihrer konkreten Ausgestaltung ethisch problematisch sein. Ihre Systeme stellen für Nutzer eine personalisierte Auswahl an Informationen bereit. Dies führt zu einer Auswahlentscheidung über die angezeigten Inhalte. Da damit aber die überwiegende Mehrzahl der Inhalte nicht oder nur nachrangig angezeigt wird, verengt sich das Wahrnehmungsspektrum des Einzelnen. In der Konsequenz entscheidet der Intermediär im Wege der Programmierung über den Kopf des Nutzers hinweg darüber, was dieser wahrnimmt. Soweit die Geschäftsmodelle der Medienintermediäre werbegetrieben sind, wie dies etwa in großen sozialen Netzwerken der Fall ist, besteht das Risiko, dass Betreiber ein wirtschaftliches Interesse daran haben, auch ethisch fragwürdige oder gar extremistische Inhalte zu verbreiten, weil diese eine höhere Verweildauer der Nutzer auf der Plattform versprechen, wodurch Werbeeinnahmen steigen. Es besteht durch das Zusammenspiel von Sortierung und Verengung des Wahrnehmbaren und der zusätzlichen Gefahr der Einflussnahme auf den Nutzer durch intransparente Drittinteressen die Möglichkeit der intransparenten Einflussnahme etwa auf die politische Willensbildung bis hin zu einer politischen Manipulation. Das ist eine erhebliche Gefahr für die freie Meinungsbildung als Grundlage der Demokratie.

### 3.2 Kritikalitätspyramide

Die DEK empfiehlt, den Kritikalitätsgrad algorithmischer Systeme einheitlich anhand eines **übergreifenden Modells** zu bestimmen. Der Kritikalitätsgrad soll Gesetzgeber und Gesellschaft bei der Suche nach geeigneten Regulierungsschwellen und -instrumenten anleiten, kann aber auch Entwicklern und Betreibern bei der

Selbsteinschätzung ihrer Produkte und Systeme Orientierung bieten und schließlich in Aus-, Fort- und Weiterbildung für die **Sensibilisierung und Schulung** unterschiedlicher Akteure eingesetzt werden. Die DEK unterscheidet insoweit mit Blick auf das Schädigungspotenzial algorithmischer Systeme – für private wie für staatliche Betreiber – **fünf Kritikalitäts-Stufen**:

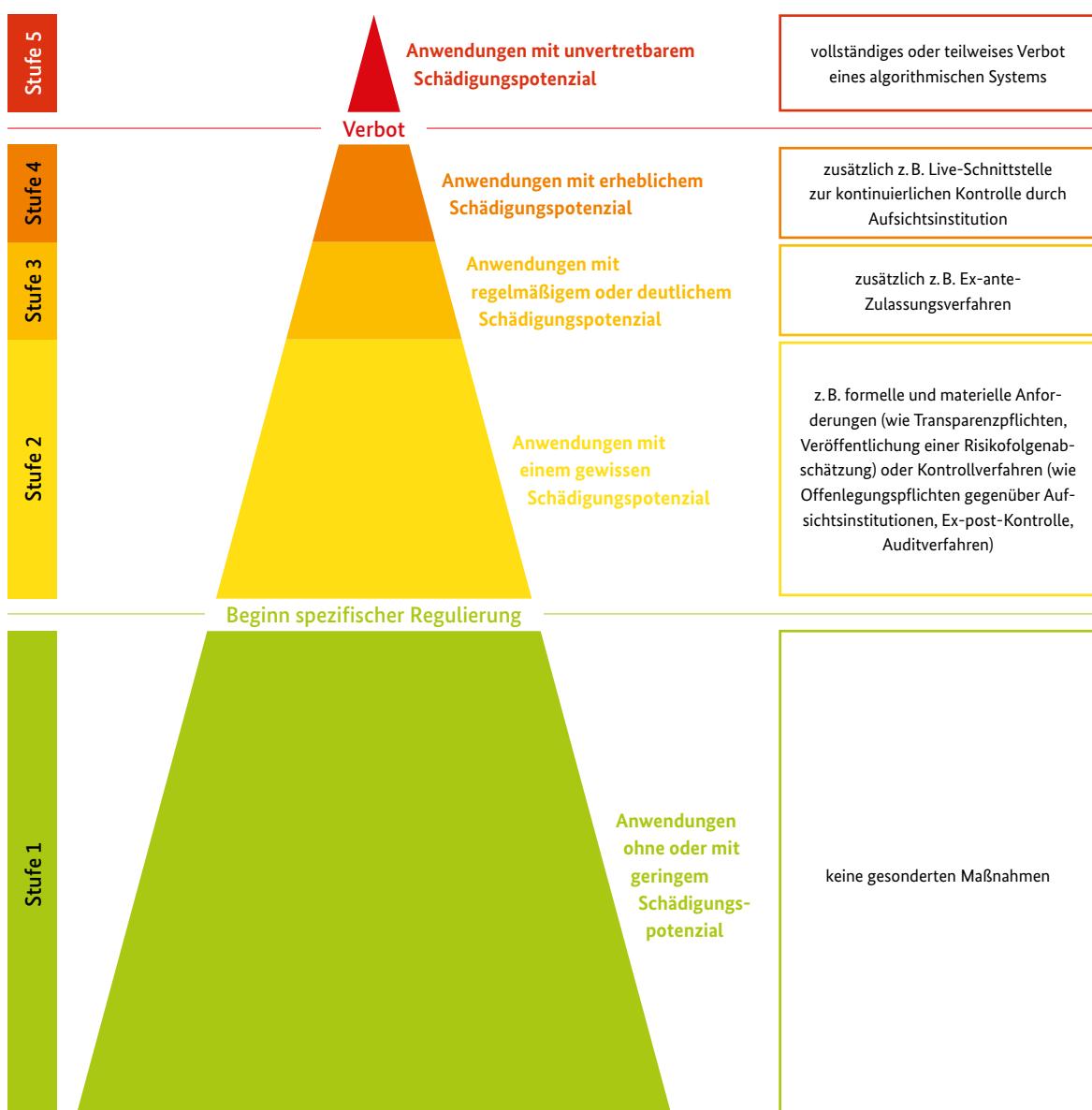


Abbildung 8:  
Kritikalitätspyramide und risikoadaptiertes Regulierungssystem für den Einsatz algorithmischer Systeme

In unproblematischen Anwendungskontexten wird es in der Regel nicht erforderlich sein, von den Entwicklern, Auftraggebern oder Betreibern zu verlangen, bestimmte Verfahren ethisch-rechtlicher Kontrolle zu durchlaufen. So sieht auch die DEK in der Vielzahl von **Anwendungen ohne oder mit nur sehr geringem Schädigungspotenzial** – also auf der untersten Stufe („Stufe 1“) der Kritikalitätspyramide – keine Notwendigkeit einer besonderen Kontrolle, welche über die allgemeinen Qualitätsanforderungen, die auch für Produkte ohne algorithmische Elemente gelten, hinausginge.

### Beispiel 13

*Die in einem Getränkeautomaten zum Einsatz gelangenden Algorithmen haben zwar auch ein gewisses Schädigungspotenzial, weil ein Nutzer z.B. keine Ware erhalten und sein Geld verlieren könnte. Dieses Schädigungspotenzial überschreitet aber nicht die Schwelle zu einem besonderen Schädigungspotenzial im Algorithmenkontext. Es ist ausreichend, hier auf die allgemeinen Mechanismen zu vertrauen, welche Vertragspartner zur Erbringung ihrer vertraglich geschuldeten Leistung oder Hersteller zur Produktion funktionierender Geräte verpflichten.*

Bei **Anwendungen mit einem gewissen Schädigungspotenzial** – also auf Stufe 2 in der Kritikalitätspyramide – kann und soll Regulierung einsetzen. Allerdings sind die hier erforderlichen Maßnahmen in ihrer Reichweite beschränkt. Mit Blick auf die niedrige Kritikalität gilt es hier besonders, eine übermäßige Belastung der Hersteller und Betreiber zu vermeiden, um technologische und soziale Innovationen sowie die Marktentwicklung nicht übermäßig zu behindern. Maßnahmen, die sich auf Stufe 2 anbieten können, umfassen etwa Ex-post-Kontrollen (beispielsweise in Form einer Input-Output-Kontrolle), insb. wenn ein begründeter Verdacht auf Fehlverhalten der Systeme besteht. Darüber hinaus sollte die Pflicht zur Erstellung und Veröffentlichung einer angemessenen Risikofolgenabschätzung bestehen (→ unten). Sektorspezifisch können ferner Offenlegungspflichten gegenüber Aufsichtsinstitutionen (einschließlich Einrichtung einer Schnittstelle zur Durchführung von Input-Output-Kontrollen durch eine Aufsichtsinstitution), gesteigerte Transparenzpflichten sowie Auskunftsrechte für Betroffene (→ dazu im Einzelnen) sinnvoll sein. Zu denken ist auch an Codes of Conduct, welche branchenspezifisch erarbeitet und dann von den zuständigen Aufsichtsbehörden genehmigt werden. Die Einhaltung wäre dann durch Stichproben sowie anlassbezogen durch die Aufsichtsbehörden zu prüfen (→ unten).

## Kritikalität bei Smart Mobility-Anwendungen

Ein Anbieter von Smart Mobility-Anwendungen greift auf einen über alle Fahrzeug- und Mobilitätsdaten generierten Datenpool zu. Sofern diese Daten ausschließlich zur Stauvorhersage genutzt werden, ist die Kritikalität als gering einzustufen. Durch den Einsatz von Smart Mobility ist aber auch der Verkehrsfluss steuerbar. Können Algorithmen etwa anhand der aus Fahrzeugdaten in Echtzeit ermittelten Gesamtauslastung des Mobilitätssystems aus Straße, Schiene, Wasser und Luft erkennen, welche Wegführung für

eine Fortbewegung von A nach B optimal ist, so kann dem Nutzer ein entsprechender Weg nach seinen Vorlieben (z.B. schnellste/umweltfreundlichste/günstigste etc. Route) vorgeschlagen werden. Es stellt sich aber auch die Frage, ob der Staat bestimmte Routen unter Berücksichtigung staatlich vorgegebener Kriterien für den Nutzer festlegen kann. Hier läge angesichts des veränderten Schädigungspotentials die Kritikalität höher und würde daher einer strengerer, kritikalitätsangemessenen Regulierung bedürfen.

**Beispiel 14**

*Dynamische Preissetzung (etwa nach den Kriterien von Angebot und Nachfrage) im Online-Handel, die aber keine Personalisierung von Preisen beinhaltet, hat ein meist geringes, aber doch die Relevanzschwelle überschreitendes Schädigungspotenzial, etwa betreffend einer versteckten Diskriminierung.*

Bei Anwendungen mit regelmäßigem oder deutlichem Schädigungspotenzial auf Stufe 3 der Kritikalitätspyramide, kann in spezifischen Fällen zusätzlich zu den bereits bei Stufe 2 zufordernden Mechanismen eine Ex-ante-Kontrolle in der Form eines Zulassungsverfahrens gerechtfertigt sein (→ unten). Aufgrund der hohen Dynamik mancher algorithmischer Systeme ist bei erteilter Zulassung eine regelmäßige Überprüfung erforderlich.

**Beispiel 15**

*Preisalgorithmen zur Festsetzung personalisierter Preise (d.h. Festsetzung des Preises nach auf den einzelnen Kunden zugeschnittenen, i.d.R. die maximale individuelle Zahlungsbereitschaft abschätzenden Kriterien) bringen ein deutliches Schädigungspotenzial mit sich, beispielsweise betreffend die Diskriminierung besonders vulnerabler Gruppen. Sie sollten allenfalls nach Durchlaufen eines Zulassungsverfahrens zum Einsatz gelangen können.*

Das Gleiche, was für Stufen 2 und 3 gilt, hat auch für Anwendungen mit erheblichem Schädigungspotenzial auf Stufe 4 zu gelten. Allerdings sind hier zusätzliche Kontroll- und Transparenzpflichten bis hin zu einer weitergehenden Veröffentlichung der in die algorithmische Berechnung einfließenden Faktoren und deren Gewichtung, der Datengrundlage sowie des algorithmischen Entscheidungsmodells in nachvollziehbarer Form zu fordern oder auch die kontinuierliche Kontrolle durch eine Live-Schnittstelle vorzusehen. Auch weitergehende Schutzmaßnahmen zur Schadensvermeidung sind erforderlich.

## Differenzierte Kritikalität bei Medienintermediären

Medienintermediäre verarbeiten und vermitteln mithilfe ihrer algorithmischen Filtersysteme sowohl meinungsrelevante Inhalte, die für die demokratische Willensbildung relevant sind, als auch Inhalte, die der Werbung, Kaufempfehlung oder Unterhaltung dienen. Sie stehen geradezu paradigmatisch für Konstellationen, in denen der Einsatz desselben algorithmischen Systems unterschiedliche Gefährdungspotenziale hat. Wenn es um Nutzerinteraktion im Konsumgüterbereich (insbes. Werbung oder Kaufempfehlungen) geht, besteht – in Abhängigkeit von dem verwendeten Personalisierungsmodell – ein geringes bis hohes

Gefährdungspotenzial. Sobald aus übergeordneten Interessen zur Erhaltung der freiheitlichen Ordnung ausgewogene Vielfalt erzeugt werden muss (insbesondere bei meinungsrelevanten Themen), ist das Gefährdungspotenzial bereits durch den Inhalt von vorne herein höher. Damit verändern sich zugleich die Regulierungsanforderungen. Bei Konsum- und Unterhaltungsangeboten muss, je nach verwendeten Personalisierungskriterien, Anwendungskontexten oder zu erwartenden Wohlfahrsteffekten, eine mehr oder weniger strenge Regulierung erfolgen.



### Beispiel 16

Auf Stufe 4 wären etwa algorithmische Systeme von Akteuren mit massiver Marktmacht einzustufen, die der Ermittlung der Kreditwürdigkeit eines individuellen Verbrauchers oder Unternehmers dienen. Ob eine Person einen Kredit erhält oder nicht, kann für ein individuelles Schicksal entscheidend sein. Die hohe Systemkritikalität wird auch begründet durch die Marktkonzentration auf wenige Anbieter und die Tendenz, dass sich ein Kreditgeber auf das Urteil eines bestimmten Akteurs verlässt.

Mit Blick auf die Kriterien für die Systemkritikalität kann für **Anwendungen mit unvertretbarem Schädigungs-potenzial** (Stufe 5) schließlich ein vollständiges oder teilweises **ex-ante-Verbot** des Einsatzes eines algorithmischen Systems infrage kommen. Zudem kann ein Verbot ex post als Sanktion für Verstöße gegen geltendes Recht oder die Nichteinhaltung der für die konkrete Systemkritikalität erforderlichen Systemanforderungen folgen.

### Beispiel 17

*Autonome Waffensysteme (Lethal Autonomous Weapons) werden vielfach als „rote Linie“ angesehen, weil die Tötung von Menschen nicht Maschinen überlassen werden dürfe. Das kann allerdings wohl nur gelten, soweit man von algorithmdeterminierten Tötungen ausgeht. Soweit autonome Waffensysteme menschliche Soldaten lediglich bei der Objekterkennung unterstützen oder sofern sie lediglich dazu dienen, einen Flugkörper trotz Seitenwinds in der Bahn zu halten, ist eine ethische „rote Linie“ nicht überschritten.*

Die Einordnung eines algorithmischen Systems in die Kritikalitätspyramide muss – unter Berücksichtigung der dynamischen Natur dieser Systeme – gegebenenfalls **regelmäßig überprüft** werden.

### 3.3 Regulierung algorithmischer Systeme durch horizontale Vorgaben im Recht der Europäischen Union und sektorale Konkretisierung

Algorithmische Systeme erfassen immer mehr Bereiche unseres individuellen und gesellschaftlichen Lebens. Die Zwecke algorithmischer Systeme und die möglichen Einsatzfelder sind dabei nicht fest definiert. So kann ein für die Gesichtserkennung bei Privatfotos entwickeltes System auch von staatlichen Ermittlungsbehörden für Zwecke der Strafverfolgung oder Gefahrenabwehr genutzt werden. Das legt nahe, den Herausforderungen algorithmischer Systeme nach dem Vorbild des Datenschutzrechts in Form **horizontaler Regulierung** zu begegnen, d. h. durch einen Rechtsakt, dessen sachlicher Anwendungsbereich allgemein algorithmische Systeme erfasst und der in personeller Hinsicht für **private und öffentliche Akteure** gleichermaßen gilt. Neben der hohen Symbolkraft spräche für eine horizontale Regulierung auch die Tatsache, dass Schutzlücken ausgeschlossen wären und gegenwärtig noch gar nicht absehbare Gefährdungskonstellationen erfasst wären. Eines der wichtigsten Argumente für eine derart übergreifende Regelung, die Grundprinzipien für alle algorithmischen Systeme festlegt, ist zudem, dass die Bürger so in allen Bereichen Erwartungsklarheit erhalten und der (europäische) Gesetzgeber diese Aufgabe in einem überschaubaren Zeitraum leisten kann.

Vor diesem Hintergrund **empfiehlt** die DEK der Bundesregierung, auf europäischer Ebene auf die Erarbeitung einer horizontalen Grundregelung im Form einer **EU-Verordnung für Algorithmische Systeme (EUVAS)** hinzuwirken. Der horizontale Rechtsakt sollte neben den zentralen Grundprinzipien für algorithmische Systeme, wie sie hier als Anforderungen an algorithmische Systeme entwickelt wurden, allgemeine materielle Regelungen zur Zulässigkeit und Gestaltung algorithmischer Systeme im Sinne der Systemkritikalität, zur Transparenz, zu Betroffenenrechten, zu organisatorischen und technischen Absicherungen und zu den Institutionen und Strukturen der Aufsicht bündeln.

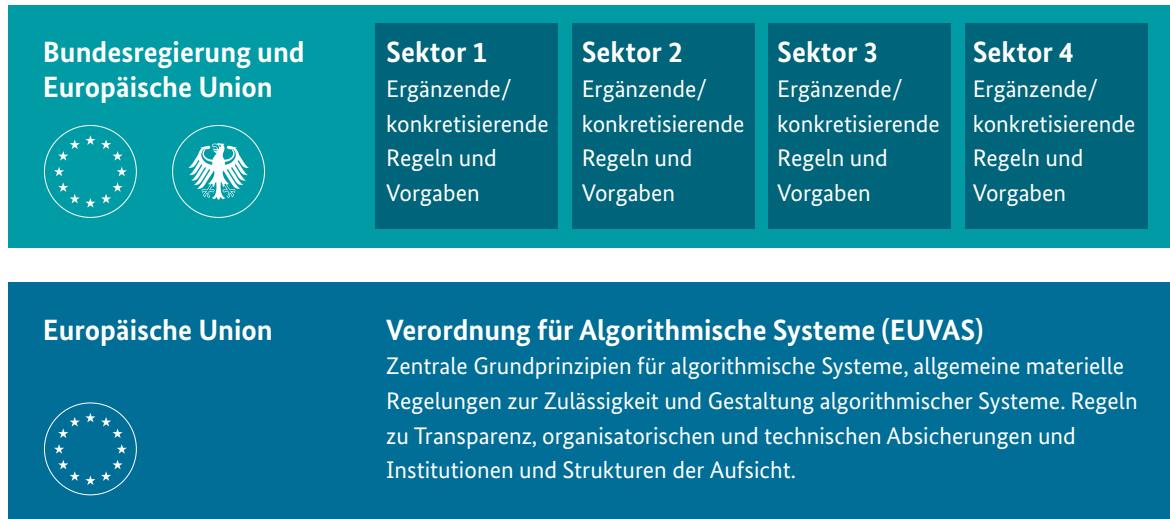


Abbildung 9:  
Regulierung algorithmischer Systeme durch horizontale Vorgaben im Recht der Europäischen Union und sektorale Konkretisierung

Zugleich empfiehlt die DEK der Bundesregierung, sich auf europäischer Ebene auch für **sektorale Regeln** einzusetzen und außerhalb der Kompetenzen der EU selbst im Rahmen der ihr zustehenden Gesetzgebungs- und Verwaltungskompetenzen entsprechende sektorale Rechtsakte zu erlassen, die am Gedanken der Systemkritikalität orientiert sind. (Abb. 9).

Eine **übergreifende EUVAS** wird sich auf wenige **Grundprinzipien** beschränken müssen, da anderenfalls der europäische Gesetzgeber überfordert würde. Bei einer zu detaillierten Regelung wäre er insbesondere mit der Frage konfrontiert, wie der kaum mehr überschaubaren Vielzahl der Systeme und der hochdynamischen Entwicklung der Technologie in einem allgemeinen Rechtsakt gerecht zu werden ist. Aus Sicht der Betroffenen tragen allgemeine Rechtsakte zudem das Risiko in sich, dass das administrative Pflichtenprogramm auch in Fällen Anwendung findet, in denen an sich kein hinreichendes Schädigungspotenzial besteht, weil die Differenzierungen zwischen riskanten und weniger riskanten Einsatzzielen – ebenso wie mögliche Ausnahmekonstellationen – in einem horizontalen Rechtsakt nicht derart feingranular vorgenommen werden können, wie sie sich in der Wirklichkeit darstellen.

Mit Blick auf beide Punkte wirkt der **ergänzende** Rückgriff auf in ihrem Anwendungsbereich beschränkte, dadurch aber leichter zu präzisierende **sektorale Normen** entlastend. Ein ergänzender, sektorale differenzierender Zugriff muss zudem die nach geltendem Recht zwischen EU, Bund und Ländern verteilten Gesetzgebungs- und Verwaltungszuständigkeiten berücksichtigen. Hinzu kommt, dass gerade mit Blick auf die Institutionen und Strukturen der behördlichen Kontrolle und Aufsicht aus unterschiedlichen Gründen die Zusammenführung der „Gesamtaufgabe“ in einer Behörde nicht in Frage kommt (→ unten ).



Neben der EUVAS ist daher der Erlass mehrerer **Rechtsakte mit spezifischen Vorgaben für einzelne Sektoren oder Gefährdungskonstellationen** erforderlich. Die Kombination einer allgemeinen Grundlagen-Regulierung mit weiteren sektorspezifisch-konkretisierenden Rechtsakten hat nach Auffassung der DEK den großen Vorteil, dass er den zwischen einzelnen Systemen und Einsatzkontexten differierenden Schutzbedarf differenziert abbilden kann. Dies entspricht dem Grundgedanken risikoadaptierter Regulierung, wonach die regulatorischen Anforderungen an algorithmische Systeme in Abhängigkeit von der spezifischen Systemkritikalität festzulegen sind. Auch im Datenschutzrecht gibt es im öffentlichen Bereich zahlreiche Spezialgesetze, die die allgemeinen Vorgaben der DSGVO sektorale ergänzen. Zwar ist es der Grundgedanke des Datenschutzrechts, dass es unter den Bedingungen der automatisierten Datenverarbeitung kein „belangloses“ Datum mehr gibt, weshalb Differenzierungen bei personenbezogenen Daten nach dem Grad der Schutzwürdigkeit oder Kritikalität kaum mehr unter Verzicht auf gemeinsame Grundregeln sinnvoll möglich sind. Es ist aber auch richtig, dass ein erhöhtes Schutzniveau in den verschiedensten Bereichen staatlichen Tätigwerdens durch eine Vielzahl von Spezialregelungen abgesichert wird. Einen ähnlichen Bedarf nach ergänzenden sektoralen Vorgaben gibt es auch für algorithmische Systeme. Deren Anwendung muss auch nicht daran scheitern, dass ihr Zweck und ihr Einsatzkontext wechseln können. Denn zum einen stößt eine solche Änderung gerade bei komplexeren Systemen an Grenzen. Zum anderen lässt sich ihnen regulatorisch dadurch begegnen, dass die Rechtsakte sachlich nicht an die ursprüngliche Zwecksetzung bzw. an den ursprünglichen Einsatzkontext, sondern an die **aktuelle Funktionalität des Systems** bzw. den **beabsichtigten neuen Einsatzzweck** des Systems anknüpfen. Zweck- und Kontextänderungen führen auf diese Weise ggf. zur Anwendung eines neuen regulatorischen Rahmens.

Von diesen primär pragmatischen Erwägungen unberührt ist allerdings die Forderung an den bzw. die Normgeber, bei ihren jeweiligen Vorhaben so weitgehend wie möglich auf **rechtsaktsübergreifende Kohärenz** zu achten. Dies gilt nicht nur für die hier entwickelten Regelungsansätze, d.h. insbesondere den Gedanken der Systemkritikalität, und die Betroffenenrechte. Auch die regulatorischen Infrastrukturen und Prozesse sollten so weit wie möglich einheitlich ausgestaltet sein.

# Zusammenfassung der wichtigsten Handlungsempfehlungen

## 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 verschärzte 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 Schädigungs-potenzial** (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.

## 4. Instrumente: Pflichten des Verantwortlichen und Rechte Betroffener

Um dem Einzelnen, aber auch Gruppen, wirksamen Schutz gegen die Gefahren algorithmischer Systeme angedeihen zu lassen, hält die DEK sowohl Transparenzanforderungen (→ s. im Folgenden 4.1) als auch weitere Vorgaben für algorithmische Systeme im Sinne eines wirksamen Schutzes gegen inhaltlich unangemessene oder unfaire Entscheidungen (→ 4.2.) für geboten.

### 4.1 Transparenzanforderungen

#### 4.1.1 Kennzeichnungspflichten („Ob“)

Ein zentrales Instrument, um Transparenz herzustellen, ist eine **Kennzeichnungspflicht**. Da der Grad der Informationsdichte einer Kennzeichnungspflicht gering ist, sind auch die Eingriffe in die Grundrechte der Betreiber, insbesondere ihrer Geschäftsgeheimnisse, weniger schwer als bei Auskunftsrechten. Dies rechtfertigt es nach Ansicht der DEK, eine Kennzeichnung bei kritischen Systemen (ab Stufe 2) als flächendeckende Pflicht für die Betreiber, und nicht als antragsabhängiges Recht einzelner Betroffener auszugestalten.

Die DEK hält die bestehenden Kennzeichnungspflichten der DSGVO<sup>3</sup> aufgrund des verhältnismäßig engen Anwendungsbereichs des Art. 22 DSGVO (mit seiner Anknüpfung an eine ausschließlich auf einer automatisierten Verarbeitung [...] beruhenden Entscheidung), auf den die Informationspflichten rekurren, für **nicht ausreichend**. Auch unterhalb der Schwelle des Art. 22 DSGVO können sich nämlich signifikante Auswirkungen für Betroffene einstellen. Das gilt für algorithmenbasierte und algorithmengetriebene Entscheidungen, also Konstellationen, in denen menschliche Entscheidungen Gefahr laufen, algorithmische Informationen und Entscheidungsvorschläge (insbesondere in Bereichen, in denen ein menschliches Abwegen erwartet wird) unreflektiert und standardmäßig zu übernehmen, oder sich nur in algorithmisch ermittelten und vorgegebenen Bahnen zu bewegen.

Da die DEK die Authentizität zwischenmenschlicher Kommunikation als Grundbedingung für einen vertrauensvollen Umgang miteinander in der Gesellschaft ansieht, sollte eine Kennzeichnungspflicht im Falle einer **Verwechslungsgefahr** zwischen Mensch und Maschine immer und somit unabhängig von der Systemkritikaltät gelten. Dies gilt etwa für digitale Sprachassistenten und Chatbots, die bisweilen kaum mehr als solche zu erkennen sind. Die Kennzeichnung bei Sprachassistenten kann beispielsweise sowohl durch die regelmäßige Offenlegung der maschinellen Natur (auch während einer laufenden Kommunikation) als auch durch die Verwendung einer maschinell klingenden Stimme erfolgen. Keine Verwechslungsgefahr (und daher auch kein Erfordernis nach einer Kennzeichnungspflicht) besteht nach Ansicht der DEK hingegen in Bereichen, in denen die Natur der Information irrelevant ist oder der Rezipient ohnehin eine maschinelle Stimme erwartet, wie beispielsweise bei Lautsprecheransagen an einem Bahnhof.

#### 4.1.2 Informationspflichten, Erklärungspflicht und Informationszugang („Wie“ und „Was“)

Während Kennzeichnungspflichten den Betreibern Transparenz darüber abverlangen, wann und in welchem Umfang („ob“) algorithmische Systeme überhaupt zum Einsatz kommen, richten sich Informationspflichten und **Auskunftsrechte** regelmäßig auf vertiefte Informationen zum Entscheidungsmechanismus („wie“) und den zugrundeliegenden Daten („was“) des algorithmischen Systems.

3 Art. 13 Abs. 2 lit. f, Art. 14 Abs. 2 lit. g und Art. 15 Abs. 1 lit. h i.V.m. Art. 22 DSGVO.



Informationspflichten und Auskunftsrechte über das Verhalten algorithmischer Systeme und den Weg der systeminternen Entscheidungsfindung sind aus der Sicht der Bürger wichtig, um Entscheidungen nachvollziehen und individuell überprüfen bzw. überprüfen lassen zu können. Erst mit ihrer Hilfe können betroffene Personen ihre Rechte wahrnehmen und eine Entscheidung fundiert angehen. Die folgenden Transparenzanforderungen gelten für private und hoheitliche Betreiber algorithmischer Systeme gleichermaßen. Auf besondere Anforderungen, die an die Transparenz hoheitlich genutzter Systeme zu stellen sind, wird unten unter 7. näher eingegangen.

#### **4.1.2.1 *Informationspflichten und Auskunftsrechte***

Dort, wo personenbezogene Daten verarbeitet werden, stehen Art. 13, 14 und 15 DSGVO bereits Informationspflichten und Auskunftsrechte vor. Im Falle einer automatisierten Entscheidung im Sinne des Art. 22 DSGVO verleiht die DSGVO den betroffenen Personen einen Anspruch auf „aussagekräftige“ Informationen über die „involvierte Logik“, die „Tragweite“ und die „angestrebte Auswirkung“ der Verarbeitung.<sup>4</sup>

Nach Auffassung der DEK sollte der Rechtsgedanke dieser Normen – ebenso wie im Falle der Kennzeichnungspflichten (→ oben) – auch außerhalb des engen Anwendungsbereichs des Art. 22 Abs. 1 DSGVO Anwendung finden und fester Bestandteil der hier vorgeschlagenen EUVAs (→ oben) werden. Dabei hängt es von der **Kritikabilität des Systems** ab, welchen Umfang eine derartige Informationspflicht hat. Bei Anwendungen mit einem geringen Schädigungspotential werden kurze Stellungnahmen zur Entscheidungslogik genügen, etwa zur verwendeten Datengrundlage oder allgemeinen Gewichtung bestimmter Faktoren mit Blick auf das Ergebnis. Je risikoträchtiger das System ist, desto weiter reichen grundsätzlich die Offenlegungspflichten.

Je persönlichkeitssensibler die Entscheidung ist, desto eher ist eine auf den Einzelfall bezogene Detailauskunft angezeigt. Es ist dabei allerdings auch zu bedenken, dass die Erteilung detaillierter Informationen über die Faktoren und ihre Gewichtung auch ethisch möglicherweise bedenkliche Steuerungseffekte für die private Lebensführung des Betroffenen mit sich bringen können. Darüber hinaus könnten die erlangten Informationen vom Betroffenen dazu genutzt werden, ein algorithmisches System, das eine wichtige Aufgabe erfüllt, zu unterlaufen.

Die **technischen und organisatorischen Anforderungen**, die zu erfüllen sind, um diesen weitgehenden Informationspflichten nachkommen zu können, müssen von Anfang an in die Konzeption von algorithmischen Systemen einfließen. Denn deren rechtmäßiger Betrieb lässt sich nur sicherstellen, wenn die entsprechend notwendigen „aussagekräftigen“ Informationen beim Einsatz des Systems auch erteilt werden können.

Bei der Ausgestaltung von Informationspflichten und Auskunftsrechten, um die Transparenz algorithmischer Systeme zu stärken, ist zu beachten, dass bei Verbrauchern keine speziellen technischen Fähigkeiten und Kenntnisse vorausgesetzt werden dürfen. Daher gilt es bei jeder Ausweitung der Auskunftsrechte zu bedenken, dass dies aus Sicht der Betroffenen nur dann die Transparenz steigert, wenn die Informationen **adressatengerecht** aufbereitet sind.

4 Art. 13 Abs. 2 lit. f, Art. 14 Abs. 2 lit. g und Art. 15 Abs. 1 lit. h DSGVO.

#### **4.1.2.2 Erklärungspflichten**

Jedenfalls in bestimmten Bereichen komplexer algorithmischer Systeme kann es sachgerecht sein, dem System zusätzlich zur allgemeinen Erläuterung der Logik und Tragweite des Systems eine Erläuterung der konkreten Gründe für das Zustandekommen einer Empfehlung oder Entscheidung des Systems abzuverlangen. Einer derartigen individuellen Erklärung bedarf es vor allem dann, wenn die Entscheidung persönlichkeits sensible Bereiche betrifft oder sonst eine besondere grundrechtliche oder sozioökonomische Tragweite hat. 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 (explainable oder explicable AI) zu stärken, und fordert die Bundesregierung auf, derartige Projekte zu fördern.

In bestimmten Situationen ist nach Auffassung der DEK ein Anspruch auf „**kontrafaktische Erklärungen**“ (counterfactual explanations) erwägenswert, wie er teilweise in der Literatur diskutiert wird.<sup>5</sup> Danach werden betroffenen Personen jene Faktoren der Entscheidungsfindung mitgeteilt, die mit Blick auf eine für sie negative Entscheidung den positiven Unterschied gemacht hätten, also zum eigentlich gewünschten Ergebnis geführt hätten. Im Falle der auf der Nutzung eines algorithmischen Systems basierenden Ablehnung eines Antrags auf Kreditgewährung hätte der Betroffene etwa einen Anspruch darauf, vom Betreiber zu erfahren, welche der vom System berücksichtigten Faktoren wie hätten anders sein müssen, damit der Antrag positiv ausgefallen wäre. Die DEK weist allerdings darauf hin, dass dieser Ansatz gegenüber komplexeren Systemen rasch an seine Grenzen gelangt, müssten doch dem Betroffenen hier sehr viele verschiedene „kontrafaktische“ Szenarien mitgeteilt werden, um ihm ein einigermaßen vollständiges Bild zu vermitteln; anderenfalls droht eher Desinformation, bedenkliche Steuerung oder gar Manipulation, indem aus strategischen oder erzieherischen Gründen bestimmte Aspekte in den Vordergrund gerückt werden.

Als allgemeiner Baustein einer Regulierung algorithmischer Systeme eignet sich das Konzept der „kontrafaktischen Erklärung“ daher nach Auffassung der DEK bei dem aktuellen Stand der technischen Entwicklung nicht; für spezielle Verarbeitungssituationen wäre ein Einsatz jedoch denkbar.

#### **4.1.2.3 Informationszugang für nicht unmittelbar betroffene Personen**

Zusätzlich empfiehlt es sich nach Auffassung der DEK, in bestimmten Sektoren, in denen nicht nur individuelle, sondern in besonderem Maße auch gesellschaftliche Interessen betroffen sind, auch nicht unmittelbar betroffenen Personen ein Recht auf Zugang zu den Informationen über die algorithmischen Systeme einzuräumen. Das gilt insbesondere, wenn ihr Einsatz **Relevanz für die öffentliche Meinungsbildung** entfaltet oder große **Wohlfahrts-Effekte** für die Bevölkerung zur Folge hat. Entsprechende Rechte werden in erster Linie für journalistische und Forschungszwecke in Frage kommen und sind zudem mit Blick auf die betroffenen Interessen der Betreiber durch hinreichende Schutzmaßnahmen zu flankieren.

Unter Umständen, insbesondere beim staatlichen Einsatz von Systemen mit einem erheblichen Schädigungspotential, sind nach Ansicht der DEK darüber hinaus auch **voraussetzungslose Informationszugangsansprüche** und **Veröffentlichungspflichten** vorstellbar.

5 Sandra Wachter / Brent Mittelstadt / Chris Russel: Harvard Journal of Law & Technology, 2018 (31:2), S. 841, 841 ff.



#### **4.1.2.4 Anforderungen an die Ausgestaltung, insbesondere Abwägung mit den Rechten der Betreiber**

Bei der Ausgestaltung der Informations- und Erklärungspflichten und Auskunftsrechte ist stets zu berücksichtigen, dass diese auch die **rechtlich geschützten Interessen der Betreiber** algorithmischer Systeme sowie derjenigen, die deren Ergebnisse einsetzen, beeinträchtigen können. Dazu gehört allen voran der Schutz von Geschäftsgeheimnissen sowie das Interesse, Manipulationen an den Systemen und beim Gebrauch der Systeme zu verhindern. Private Betreiber können sich zwar im Grundsatz darauf berufen, dass sie über Ergebnisse eines algorithmischen Systems ihre eigene freie Willens- und Vertragsentscheidung definieren. Das entbindet sie jedoch nicht von der Kontrolle, ob ihr Handeln rechtskonform ist, denn das Grundrecht auf allgemeine Handlungsfreiheit findet in den Diskriminierungsverboten (insbesondere das AGG), den Grundrechten der betroffenen Personen oder Dritter und allgemein den – auch vertragsspezifischen – Vorgaben der Rechtsordnung eine Grenze. Zudem sind Transparenzrechte stets mit den datenschutzrechtlichen Vorgaben zum Schutz der im System gespeicherten personenbezogenen Daten Dritter in Ausgleich zu bringen.

Die DEK sieht es daher als sachgerecht an, dass der Gesetzgeber Transparenzpflichten durch Regelungen flankiert, die auf Initiative der Betreiber oder auch möglicherweise betroffener Dritter eine **Abwägung der kollidierenden Rechte und Interessen** mit dem Transparenzinteressen der betroffenen Personen oder sonstiger anspruchsberechtigter Privater ermöglicht. **Starre Vorrangregeln**, etwa eine generelle Präferenz für den Schutz von Geschäftsgeheimnissen im Verhältnis zu den Transparenzinteressen, sind hingegen nach Auffassung der DEK (trotz des damit womöglich verbundenen Gewinns an Rechtssicherheit) **nicht sachadäquat**. In jedem Fall, in dem sich Betreiber oder Dritte auf kollidierende Interessen berufen, ist sorgfältig zu prüfen, ob diesen Interessen nicht durch konkrete Schutzmaßnahmen Rechnung getragen werden kann, bevor eine Transparenzpflicht ganz verneint wird. Im Falle auskunftsberichtigter Privatpersonen sind die Anforderungen an die Schutzmaßnahmen und deren Nachweis so zu gestalten, dass sie auch für verletzliche Verbraucher keine prohibitive Schwelle zur Erlangung von Informationen darstellen. Drittinteressen sind etwa durch Anonymisierung zu schützen.

#### **4.1.3 Risikofolgenabschätzung**

Die Folgenabschätzung i.S.d. Art. 35 Abs. 1 DSGVO umfasst ausschließlich Informationen zu den Folgen für den Schutz *personenbezogener Daten*, jedoch keine umfassende Risikoanalyse eines algorithmischen Systems. Bei algorithmischen Systemen ab einem gewissen Schädigungspotenzial (ab Stufe 2) ist es jedoch sachgerecht und zumutbar, dem Anbieter/Anwender eine angemessene Risikofolgenabschätzung zur Einschätzung des mit einem System verbundenen Risikos und ihre Veröffentlichung gesetzlich abzuverlangen. Je kritischer das System, desto umfangreicher muss die Risikofolgenabschätzung ausfallen. Sie sollte auch eine Abschätzung der **Risiken für Selbstbestimmung, Privatheit, körperliche Unversehrtheit, persönliche Integrität sowie für Vermögen, Eigentum, und Gleichbehandlung** umfassen und auch Qualitätsmaße und Fairnessmaße zu den Daten und zur Modellgüte enthalten, etwa zu Bias oder (statistischen) Fehlerquoten (insgesamt oder für bestimmte Teilgruppen), die ein System bei der Vorhersage/Kategorienbildung aufweist.

## Use Case: Personalisierte Preise I – Transparenzanforderungen

Der zunehmende Einsatz von Preissetzungsalgorithmen im Online-Handel stellt nicht nur das Verbraucherschutzrecht, sondern auch das Wettbewerbsrecht vor Herausforderungen: Preissetzungsalgorithmen können den Markt überblicken, um in Echtzeit Preise an Nachfrage und die Angebote der Wettbewerber anzupassen.

Im Online-Handel können Anbieter dadurch personalisierte Preise (für einzelne Nutzer oder Gruppen) direkt oder über individuelle Rabatte ausspielen.

Algorithmische Systeme lassen sich beispielsweise gezielt dazu nutzen, die maximale Zahlungsbereitschaft der Konsumenten abzuschöpfen, oder Nutzer dazu zu bewegen einen Kaufvorgang nicht abzubrechen. Grundlage dieser Personalisierung sind Scoringverfahren, etwa auf der Basis von Echtzeitanalysen des Surfverhaltens der Nutzer oder anderweitig gesammelter Daten. Die zugrunde liegenden algorithmischen Systeme sind i.d.R. „Blackboxes“, so dass für Außenstehende die Datengrundlage und Entscheidungslogik der Preisbildung nicht nachvollziehbar sind. Somit besteht ein Risiko preislicher Diskriminierung, etwa von geschützten Bevölkerungsgruppen im Sinne des AGG.

Das Schädigungspotenzial durch höhere personalisierte Preise für einzelne betroffene Verbraucher kann stark variieren. Nichtsdestotrotz können selbst geringe Preisaufschläge für einzelne Güter und Dienstleistungen in der Summe für die einzelnen Betroffenen und für die betreffenden Bevölkerungsgruppen zu beträchtlichen Wohlfahrtsverlusten führen. Insbesondere kann es durch lernende Systeme, etwa über Signaling, auch zu quasi-abgestimmten hohen Marktpreisen kommen. Wenn Wettbewerber Preise oder

Konditionen auf dem Umweg über Algorithmen abstimmen, schadet das dem Wettbewerb, der Innovationskraft der Volkswirtschaft und schlussendlich dem Verbraucher; das gilt sowohl für die beabsichtigte Nutzung von Algorithmen zur Preisbeeinflussung als auch dann, wenn Parallelverhalten und hohe Preise (Tacit Collusion) ohne eine solche konkrete Absicht durch lernende Algorithmen zustande kommen und keine direkte Preisabsprache durch Menschen stattfand.

Es reicht nicht aus, wenn diese hohe Kritikalität insgesamt nur Transparenzanforderungen und Kennzeichnungspflichten für Pricing-Systeme auslöst. Auch eine umfassende Folgenabschätzung kann dazu beitragen, Diskriminierungsrisiken eines algorithmischen Pricing-Systems zu erkennen: Ist die verwendete Datengrundlage bekannt, nach denen personalisierte Preise berechnet werden, sollten unabhängige Experten prüfen können, ob diese mit geschützten Bevölkerungsgruppen korrelieren (sog. Proxys), d.h. ob z.B. Frauen oder bestimmte religiöse Gruppen höhere Preise bezahlen müssen. Wenn Verbraucher zudem über Kennzeichnungspflichten darauf aufmerksam gemacht werden, dass Preise bzw. Rabatte personalisiert ausgespielt werden, könnten die Betroffenen über Auskunftsrechte, die für „ihren“ Preis verwendeten Daten auf Richtigkeit oder mögliche diskriminierende Faktoren hin überprüfen.

Auch ist die Transparenz über preisrelevante Faktoren wichtig, um die steuernden Effekte individualisierter Preissetzung auf das Verhalten der einzelnen Verbraucher zu beobachten, da diese freiheitsrelevante Ausmaße annehmen können.



#### 4.1.4 Pflicht zur Dokumentation und zur Protokollierung

Je komplexer, dynamischer und verteilter einzelne IT-Systeme einen Input in einen Output verwandeln, desto wichtiger ist es aus regulatorischer Sicht, die konkreten Ursachen für eine bestimmte Entscheidung nachvollziehbar zu machen. Nur dann lassen sich Fehler aufdecken und Rechtsverletzungen effektiv ahnden. Ein Ansatzpunkt, um die Wirkweise softwarebasierter Verfahren besser zu verstehen, ist es, einzelne Programmschritte digital mitzuschneiden und für Prüfzwecke zu verwenden. Dies kann im Bereich der Verarbeitung personenbezogener Daten auch gemäß dem Datenschutzrecht geboten sein, um das Gebot der Rechenschaftspflicht umzusetzen.

Zum einen sollte eine solche Anforderung von Dokumentation und Protokollierung in Bezug auf die verwendeten Datensätze und Modelle, die Granularität, die Aufbewahrungszeiten und die Verwendungszwecke im Datenschutzrecht konkretisiert werden, damit die Verantwortlichen und Auftragsverarbeiter Rechtsklarheit erhalten. Zum anderen sollte für Systeme, die ein erhebliches Schädigungspotenzial haben (Stufe 4), eine Pflicht etabliert werden, die Programmabläufe 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).

#### 4.2 Sonstige Vorgaben für algorithmische Systeme

##### 4.2.1 Allgemeine qualitative Vorgaben an algorithmische Systeme

Der Normgeber sollte Betreibern ein Mindestmaß an **technischen und mathematischen prozeduralen Qualitätsgarantien** abverlangen, welche die Rechtmäßigkeit der algorithmisch ermittelten Ergebnisse durch Verfahrensvorgaben absichern. Dazu können insbesondere Vorgaben für das mathematische Modell und spezifische Verarbeitungsmethoden oder Vorgaben für Korrektur- und Kontrollmechanismen oder für die Datenqualität sowie die Sicherheit des Systems gehören. Um die widerstreitenden Grundrechtspositionen des Softwarebetreibers sowie der Entscheidungadressaten auszutarieren, sollten die Anforderungen an die Validität der mathematischen Modelle sowie die Sachnähe der zugrunde gelegten Informationen **mit dem Schädigungspotenzial algorithmischer Systeme steigen**.

Bei algorithmenbasierten und algorithmengetriebenen Entscheidungen bedarf es auch eines **kompetenz-sensitiven Designs**. Dieses kann den bewussten Einsatz zwingend zu absolvierender **Trainingsmodule** beinhalten. Auch hat es sich etwa bei Entscheidungsassistenten insbesondere bewährt, systemische **Rollenwechsel** einzuführen, d.h. dem Anwender etwa immer wieder auch einmal die Erstentscheidung ohne Kenntnis des algorithmischen Entscheidungsvorschlags zuzuweisen. Eine für den einzelnen Anwender möglicherweise unangenehme Variante ist diejenige des **Aufmerksamkeitstests**, d.h. programmiert falsche Entscheidungsvorschläge der Maschine einzustreuen, deren Eigenschaft als Aufmerksamkeitstest noch rechtzeitig aufgedeckt wird, bevor es zu Auswirkungen für andere Menschen kommen kann.

Ferner ist zu gewährleisten, dass Verbesserungsprozesse fair und im Sinne aller Betroffener durchgeführt werden; insbesondere ist sicherzustellen, dass geeignete

**Feedbackschleifen** auch den Interessen der betroffenen Personen, nicht nur der Betreiber, Rechnung tragen. Hinsichtlich der Datenqualität sind auch Vorgaben angezeigt, inwieweit für bestimmte Anwendungsbereiche die Nutzung von Schätz- oder sog. Proxy-Daten (Teil C, 2.2.2 f.) zulässig oder verboten sein sollte.

Zusätzlich zu den Anforderungen, die der eigentliche Zweck der Verarbeitung an das algorithmische System stellt, sollten bei der Gestaltung die Anforderungen der **Sicherheit** erfüllt werden. Dazu sollten die individuellen Anforderungen sämtlicher Beteiligter Berücksichtigung finden, um bei der Konzeptionierung, Implementierung und im Betrieb die geeigneten Gestaltungsentscheidungen zu treffen. Die Einschätzung der Risiken obliegt zwar in der Regel vorrangig dem Betreiber des Systems, doch kann er dies nur leisten, wenn er auf eine ausreichende Dokumentation, z. B. eine Risikofolgenabschätzung des Herstellers, zurückgreifen kann. Nötig ist auch die Klarheit darüber, wer für welchen Bereich verantwortlich ist. Die DEK empfiehlt dabei in als kritisch identifizierten Bereichen rechtliche Vorgaben bzgl. der

- Mindeststandards an erforderlicher Sicherheit und den zu treffenden Maßnahmen;
- Spezifika, wie und unter welchen Voraussetzungen Testverfahren (etwa zur Identifikation von Bias bzw. diskriminierenden Verzerrungen) algorithmischer Systeme bei Herstellern oder Betreibern auszustalten und durchzuführen sind;
- Rechtsfolgen bei Sicherheitslücken oder anderen Fehlern;
- Dokumentationspflichten hinsichtlich der Funktionsweise und der Tests, die Anwender erhalten, um das Risiko abschätzen zu können; und

- Verpflichtung, Systemaktualisierungen in einem definierten Zeitraum durchzuführen und darüber zu berichten.

#### 4.2.2 Besondere Schutzmaßnahmen beim Einsatz algorithmischer Systeme im Kontext menschlicher Entscheidungen

Der Mensch darf nicht zum Objekt der Technik werden. Dieser für die Regulierung algorithmischer Systeme zentrale Grundsatz entfaltet seine Wirkung insbesondere dort, wo algorithmische Systeme zum Einsatz kommen, um menschliche Entscheidungen zu unterstützen oder um Entscheidungsprozesse zu automatisieren, d. h. menschliche Entscheidungen durch technische Prozesse zu ersetzen.

Im geltenden Recht kodifiziert Art. 22 DSGVO diesen Grundsatz bereits für bestimmte algorithmische Systeme, die in den Anwendungsbereich der DSGVO fallen: Niemand darf einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen werden, die ihm gegenüber rechtliche oder andere erhebliche Folgen hat – es sei denn, es ist für den Abschluss oder die Erfüllung eines Vertrags notwendig, der Betroffene hat explizit eingewilligt oder es gibt eine gesetzliche Erlaubnis. Soweit eine solche vollständig automatisierte Entscheidung zulässig ist, muss der Verantwortliche Schutzmaßnahmen treffen, um die Rechte und Interessen der betroffenen Personen zu wahren.<sup>6</sup> Zudem gelten verschärzte Informationspflichten und Auskunftsrechte.<sup>7</sup>

<sup>6</sup> Vgl. Art 22 Abs. 3 DSGVO.

<sup>7</sup> Vgl. Art. 13 Abs. 2 lit. f DSGVO, Art. 14 Abs. 2 lit. g DSGVO und Art. 15 Abs. 1 lit. h DSGVO.



Gegenwärtig besteht aus Sicht der DEK in Bezug auf diese Normen an verschiedenen Punkten noch **Klarstellungsbedarf**. Die mit Art. 22 DSGVO – „einschließlich Profiling“ – verbundenen Informationspflichten und Auskunftsrechte sollten sich auch auf die automatisierte **Profilbildung als solche** beziehen. So sehen sich beispielsweise einzelne Wirtschaftsauskunfteien nicht von diesen Normen erfasst, da sie lediglich eine Profilbildung vornähmen, die „Entscheidungen“ aber erst durch die Unternehmen, die beispielsweise einen Kreditscore abfragen, getroffen würden. Diese Argumentation trägt der Intention der DSGVO aus der Sicht der DEK jedoch nicht ausreichend Rechnung. Denn die langfristigen Auswirkungen einer solchen Profilbildung auf die Betroffenen können zum einen erheblich sein, zum anderen hebt die DSGVO die Profilbildung besonders hervor. Soweit die Datenschutzbehörden und Gerichte das geltende Recht im Wege einer am Schutzzweck der DSGVO orientierten Auslegung entsprechend weit anwenden können, ist dies zu begrüßen. Parallel dazu ist jedoch aufgrund der hohen Grundrechtssensibilität dieser Frage der demokratisch legitimierte Gesetzgeber aufgerufen, die rechtlichen Rahmenbedingungen zeitnah weiter zu konkretisieren, um möglichst schnell Rechtssicherheit zu schaffen. Die DEK empfiehlt der Bundesregierung, sich hierfür im Rahmen der Evaluation der DSGVO einzusetzen.

**Klarstellungs- und Konkretisierungsbedarf** besteht auch hinsichtlich der Frage, wann eine Entscheidung gemäß **Art. 22 DSGVO** „ausschließlich“ auf einer automatisierten Verarbeitung personenbezogener Daten „beruht“ und wie weit der Begriff der „Beeinträchtigung in ähnlicher Weise“ sowie die Schutzrechte des Art. 22 Abs. 3 DSGVO reichen. Die DEK empfiehlt der Bundesregierung, sich bei der Evaluation der DSGVO dafür einzusetzen, dass der Anwendungsbereich des Art. 22 DSGVO eine Konkretisierung erfährt. Das Schädigungspotential algorithmenderminierter Entscheidungssysteme, die ursprünglich das Leitbild des Art. 22 DSGVO gebildet hatten, unterscheidet sich insbesondere nicht kategorial von demjenigen vieler algorithmengetriebener Entscheidungssysteme. Dafür ist auch die Neigung menschlicher Akteure, Empfehlungen algorithmischer Systeme schlicht zu übernehmen und bestehendes Ermessen nicht auszuüben, mitverantwortlich.

Im Lichte des im Einzelnen stark differierenden Schädigungspotentials algorithmenbasierter Systeme erscheint es der DEK nicht angemessen, das Verbotsprinzip des Art. 22 DSGVO generell auszuweiten. Insbesondere eignet sich der Grundsatz menschlicher Letztentscheidung aus Art. 22 Abs. 3 DSGVO nicht für alle algorithmischen Systeme gleichermaßen. So wäre für algorithmische Systeme, bei denen keine „Entscheidung“ des Systems im Sinne der bisherigen Fassung des Art. 22 Abs. 1 DSGVO vorliegt, auch ein Recht auf menschliche Letztentscheidung regelmäßig wenig praktikabel und zudem oft auch nicht wünschenswert. Stattdessen empfiehlt die DEK ein risikoadaptiertes Regulierungsregime, das dem Einzelnen angemessene Schutzgarantien (insbesondere gegen Profiling) und Verteidigungsmöglichkeiten gegen Fehler und Bedrohungen seiner Rechte vermittelt.

Der Rechtsgedanke, dass der Mensch nicht zum Objekt technischer Systeme werden darf, sollte auch in dem horizontalen EU-Rechtsakt einer EUVAS (→ oben 3.3) zur risikoadaptierten Regulierung algorithmischer Systeme, den die DEK anregt, sowie in den begleitenden sektoralen Rechtsakten einen **zentralen normativen Ankerpunkt** bilden. In diese Rechtsakte sind daher Regelungen aufzunehmen, die auch außerhalb des Anwendungsbereichs des Art. 22 DSGVO Vorgaben für algorithmenbasierte Entscheidungssysteme treffen. Soweit die neue Regulierungsschicht algorithmische Systeme miterfasst, die auch in den – gegebenenfalls im Lichte der hiesigen Empfehlungen modifizierten – Anwendungsbereich des Art. 22 DSGVO fallen, ist auf eine präzise **Synchronisierung der Regelungssysteme** zu achten.

#### 4.2.3 Recht auf angemessene algorithmische Schlussfolgerungen?

Die Prozesse datenbasierter Generierung sog. **algorithmischer Schlussfolgerungen** über die vermeintlichen Interessen, Neigungen und Charaktereigenschaften individueller Personen, insbesondere von Verbrauchern, verdienen aus Sicht der DEK höchste gesellschaftliche und politische Aufmerksamkeit. In der digitalen Wirtschaft sind derartige Schlussfolgerungen ubiquitär. Für viele digitale Geschäftsmodelle, die auf die feingranulare Personalisierung bestimmter Angebote oder Dienste ausgerichtet sind, sind sie geradezu kennzeichnend. Viele Verbraucherinnen und Verbraucher schätzen den Komfort solcher Angebote und Dienste, doch ergeben sich aus ihnen auch Gefahren, wenn Schlussfolgerungen auf einer falschen Datenbasis erfolgen oder infolge der Unzulänglichkeit anderer Systemkomponenten sonst Ergebnisse erzielt werden, die inhaltlich unangemessen sind.

Um den Gefahren zu begegnen, die durch bestimmte algorithmische Schlussfolgerungen erwachsen können, wollen manche dem Betroffenen ein „Recht auf angemessene Schlussfolgerungen“ normativ verbürgen.<sup>8</sup> Dieser Vorschlag sieht ein Gesamtpaket an Maßnahmen vor, das den jeweils Betroffenen ein wirksames Kontrollinstrument über die Schlussfolgerungen an die Hand geben soll, die Betreiber algorithmischer Systeme über sie erstellt haben. Neben einem materiellen Recht, angemessenen Schlussfolgerungen unterworfen zu werden, sieht es eine Pflicht des Betreibers vor, den Betroffenen ohne Auskunftsverlangen darüber unterrichten müssen, dass und wieso die gezogenen Schlussfolgerungen „angemessen“ waren.

Die Datenethikkommission begrüßt die Diskussion, die der Vorschlag eines solchen „Rechts auf angemessene Schlussfolgerungen“ angestoßen hat. Sie gibt jedoch zu bedenken, dass ein derartiges Recht verfassungsrechtlich geschützte Interessen der Betreiber algorithmischer Systeme tangieren kann. Auf diese Schutzpositionen ist nach Auffassung der Datenethikkommission bei einer etwaigen regulatorischen Ausgestaltung des Vorschlags Rücksicht zu nehmen, etwa durch eine Beschränkung des Anwendungsbereichs auf Systeme, die aufgrund ihrer Teilhabe- und Grundrechtsrelevanz eine hohe Kritikalität aufweisen.

#### 4.2.4 Gesetzlicher Diskriminierungsschutz

Ein wesentliches Ziel der Regulierung algorithmenbasierter, -getriebener und -determinierter Entscheidungssysteme besteht darin, die Diskriminierung eines Menschen aufgrund eines in Art. 3 Abs. 3 GG bzw. Art. 21 Abs. 1 GRCh genannten Merkmals – und darüber hinaus jede sachlich nicht gerechtfertigte Ungleichbehandlung – zu verhindern sowie die persönliche Integrität von Betroffenen zu schützen. Während staatliche Stellen bei jeder Form hoheitlichen Handelns unmittelbar einer **Grundrechtsbindung** und damit auch einem umfassenden Diskriminierungsverbot unterliegen, bedarf es bei privaten Akteuren dafür einer einfachgesetzlichen Grundlage. Den Regelungstechnischen Anknüpfungspunkt dafür markiert grundsätzlich das **Allgemeine Gleichbehandlungsgesetz (AGG)** – flankiert durch Generalklauseln des Privatrechts, etwa zu sittenwidrigen Verträgen.

Damit eine Ungleichbehandlung unter Privaten dem AGG unterfällt, muss es sich zum einen um eine Ungleichbehandlung aufgrund eines **sensiblen Merkmals** handeln (Rasse, ethnische Herkunft, Geschlecht, Religion, Behinderung, Alter, sexuelle Identität); zum anderen muss der **situative Anwendungsbereich** eröffnet sein (Beschäftigungskontext oder Zugang zu Gütern und Dienstleistungen, einschließlich Wohnraum, die der Öffentlichkeit zur Verfügung stehen).

<sup>8</sup> Omer Tene / Jules Polonetsky: Northwestern Journal of Technology and Intellectual Property, 2013 (11:5), S. 240, 270 f.; Sandra Wachter / Brent Mittelstadt: Columbia Business Law Review, 2019 (2), S. 1, 1 ff. Der Vorschlag besteht aus einer materiellen Komponente und einer Verfahrenskomponente.



Zwar erfassen die Normen des AGG im Grundsatz bereits nach geltendem Recht Ungleichbehandlungen durch algorithmische Systeme. Allerdings sind nicht alle diskriminierungsanfälligen Sachmaterien in den Anwendungsbereich des AGG einbezogen und erfasst das AGG nicht sämtliche sensiblen Konstellationen, in denen algorithmisch ermittelte Ergebnisse eine Diskriminierung auslösen oder begünstigen (z. B. im Falle der Vergabe eines Immobilienkredits aufgrund einer individuellen Risikoprüfung). Es ist daher erwägswert, den **situativen Anwendungsbereich des AGG** etwa auf alle automatisierten Entscheidungsverfahren auszudehnen oder einzelne Sachbereiche besonders persönlichkeitsensibler algorithmischer Schlussfolgerungen ergänzend aufzunehmen.<sup>9</sup> Dies betrifft vor allem solche Sachbereiche, welche die Lebensgestaltung nachhaltig beeinträchtigen können, wie z. B. Verbraucherverträge, die auf der Grundlage eines Scorings zustande kommen oder auf besonders risiko-trächtigen Verfahren basieren, Methoden der Gesichtserkennung oder Preisdiskriminierung in bestimmten Lebensbereichen wie der Gesundheitsversorgung. Der gleichfalls grundrechtlich geschützten allgemeinen Handlungsfreiheit des vertraglichen Gegenübers ist dabei angemessen Rechnung zu tragen.

Zu diskutieren ist auch, ob im Zusammenhang mit algorithmischen Systemen der Gesetzgeber die Beschränkung auf bestimmte Diskriminierungsmerkmale aufgeben sollte. In diskriminierenden Effekten algorithmischer Systeme spiegelt sich nur teilweise eine in der Gesellschaft bestehende Verzerrung hinsichtlich **klassischer Diskriminierungsmerkmale** wider, etwa soweit die Verzerrung in den Trainingsdaten oder im verwendeten Modell liegt. Dies wäre etwa der Fall, wenn ein zur Bewerberauswahl verwendetes System anhand der Daten erfolgreicher Führungskräfte der Vergangenheit trainiert wurde, die ganz überwiegend männlich waren. Allerdings geht das Diskriminierungspotenzial algorithmischer Systeme deutlich darüber hinaus, z. B. wenn eine Benachteiligung systematisch an nicht gesetzlich verbotene Gruppenmerkmale (z. B. Wohnadresse in einem bestimmten Bezirk) oder gar an im Wege der Mustererkennung ermittelte, aber eher zufällige Korrelationen anknüpft. Teilweise lassen sich diese Konstellationen bereits über die Figur der **mittelbaren Diskriminierung** in den Griff bekommen. Insoweit bedarf es dann gegebenenfalls ergänzend geeigneter Beweiserleichterungen. Teilweise stellen sich hier aber auch ganz neue Gerechtigkeitsfragen. Diese betreffen nicht nur die Verteilung von Chancen zu Lasten traditionell marginalisierter Gemeinschaften, sondern auch den Ausschluss von Gruppen, die anhand mehr oder weniger zufälliger Merkmale zusammengewürfelt sind: Die Eigenheiten maschinellen Lernens schaffen **neue Diskriminierungsmerkmale**, die aber dadurch, dass trainierte Algorithmen auch in anderen Einsatzbereichen verwendet werden, enorme Breitenwirkung entfalten können.

9 Mario Martini: Juristenzeitung (JZ), 2017, S. 1017, 1021.

Daher ist es angezeigt, eine Erweiterung des Diskriminierungsschutzes auf jede systematische und sachlich ungerechtfertigte Benachteiligung aufgrund eines Gruppenmerkmals zu erwägen. Die DEK empfiehlt der Bundesregierung, auch diesbezüglich eine entsprechende **Erweiterung des AGG oder alternativ die Verankerung in künftiger, spezieller Algorithmen-Gesetzgebung zu prüfen**. Eine besondere regulatorische Schwierigkeit geht dabei davon aus, dass eine – prinzipiell nicht abgeschlossene – Fülle von Gruppenmerkmalen existiert, die eine derartige algorithmische Diskriminierung nach sich ziehen können und damit einziges Abgrenzungskriterium zwischen diskriminierungsrechtlich relevanten und irrelevanten Benachteiligungen der systematische Charakter wäre. Eine entsprechende Regelung des materiellen Diskriminierungsschutzes müsste daher jedenfalls einerseits durch entsprechende Auskunfts- und Begründungspflichten und andererseits durch verschiedene Mechanismen interner und externer Kontrolle flankiert sein, für welche die neue Regelung den materiellen Prüfungsmaßstab bilden würde. Die Folgen einer derartigen Regulierung auf alle Beteiligten wären in jedem Fall sorgfältig abzuschätzen und abzuwagen.

Ganz unabhängig von der Frage einer tatbestandlichen Erweiterung ist zu erwägen, ob die **Beweisregelungen** den Charakteristika algorithmischer Systeme bereits hinreichend gerecht werden. Zwar erfordert die Feststellung einer mittelbaren Diskriminierung weder den Nachweis einer diskriminierenden Absicht noch einen eindeutigen Kausalitätsnachweis. Vielmehr reicht es aus Sicht der Geschädigten aus, eine Korrelation zwischen den Entscheidungen und sensiblen Kriterien aufzuzeigen. Beim Einsatz algorithmischer Systeme ist aber dieser Nachweis für die Betroffenen in der Regel schwer zu erbringen.

Daher empfiehlt die DEK dem Gesetzgeber, die Anforderungen an diesen Nachweis einer Diskriminierung durch den Betreiber algorithmischer Systeme klarstellend gesetzgeberisch zu regeln und ggf. für Betroffene noch weiter abzusenken. Darum ist das AGG stets zusammen mit **Auskunftsrechten und Begründungspflichten** (→ siehe ) zu denken, ohne die dem Geschädigten eine Wahrnehmung seiner Rechte oft nicht möglich sein wird. Den dadurch betroffenen Schutzinteressen Dritter sowie der Verwender der Systeme muss dabei hinreichend Rechnung getragen werden.

#### 4.2.5 Präventives behördliches Zulassungsverfahren für besonders riskante algorithmische Systeme

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.



# Zusammenfassung der wichtigsten Handlungsempfehlungen

## 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 Verwechslungsgefahr zwischen Mensch und algorithmischem System bestehen.

**46**

Das Recht einer betroffenen Person auf aussagekräftige **Informationen** über die „involveierte 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.

**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 algorithmdeterminierten 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.

**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).

**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.

**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.

**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.

## 5. Institutionen

Die Verantwortlichkeit für den ethisch vertretbaren und rechtmäßigen Einsatz algorithmischer Systeme muss nach Auffassung der DEK auf mehrere Schultern verteilt werden. Die gegenwärtig bereits bestehenden Institutionen und Aufsichtsstrukturen sind nicht ausreichend darauf vorbereitet, um die abgestufte Kontrolle algorithmischer Systeme hinreichend effektiv wahrnehmen zu können. Daher fordert die DEK die Bundesregierung dazu auf, die bestehenden Institutionen und Strukturen im Rahmen ihrer Zuständigkeit zu stärken, neu auszurichten und, wo erforderlich, auch neue Institutionen und Strukturen zu schaffen.

### 5.1 Behördliche Kompetenzen und fachliche Expertise

#### 5.1.1 Verteilung der Aufsichtsaufgaben im sektoralen Kontrollverbund

Die DEK empfiehlt der Bundesregierung, die behördlichen Aufsichtsaufgaben und Kontrollbefugnisse im Grundsatz jeweils den Behörden zuzuweisen, die bereits **sektorspezifische Sachkompetenzen** haben. Gleichermaßen sollte aus Sicht der DEK bei jenen Materien geschehen, die in die Verwaltungskompetenz der Länder fallen.

Konkret hält es die DEK für sinnvoll, die Aufsicht über den Einsatz algorithmischer Systeme durch Private in den Bereichen der digitalen Wirtschaft, in denen bereits Behörden mit sektorspezifischen Zuständigkeiten existieren, an die **bestehenden Behörden** anzubinden. Zu denken ist hier an Behörden wie die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), die Bundesnetzagentur (BNetzA), das Bundesamt für Sicherheit in der Informationstechnik (BSI) oder das Kraftfahrtbundesamt (KBA). Eine besondere Stellung kommt ferner dem Bundeskartellamt (BKA) und den Datenschutzaufsichtsbehörden zu, die je horizontale, d.h. über die verschiedenen Wirtschaftsbereiche hinweg reichende Zuständigkeiten innehaben.

Um die Tätigkeit der mit Algorithmenaufsicht befassten Behörden zu koordinieren, hält die DEK einen „**Kontrollverbund für kritische algorithmische Systeme**“ auf nationaler und EU-Ebene für sachgerecht. Für diese Zwecke sind insbesondere Regelungen zur Verteilung von Zuständigkeiten im Verbund, zum Informationsaustausch, zur Organisation verbundförmig durchgeföhrter Verwaltungsverfahren und zum Rechtsschutz sachgerecht.

Um Aufsichtslücken zu vermeiden, fordert die DEK Bund und Länder dazu auf, Bereiche zu identifizieren, in denen für eine Kontrolle kritischer algorithmischer Systeme **bisher keine hinreichend sektorspezifisch-sachkundige Behörde** existiert, für die eine Zuweisung der Kontrollaufgabe nahe liegt. Regelmäßig wird es in diesen Fällen nach Auffassung der DEK zweckmäßig sein, bei einem entsprechenden Kontrollbedarf eine der horizontal zuständigen Behörden mit der Materie zu betrauen. Im Falle algorithmischer Systeme, die sensible personenbezogene Daten verarbeiten, können etwa die Datenschutzbehörden sachadäquate Kompetenzträger sein. Im Einzelfall hält es die DEK jedoch für möglich, dass es erforderlich ist, ganz neue behördliche Kontrollstrukturen aufzubauen. Im Lichte der sich stetig wandelnden technischen Entwicklungen sollten Bund und Länder diese Überprüfung regelmäßig vornehmen.

Um ihrer Aufgabe der Aufsicht über algorithmische Systeme wirkungsvoll nachzukommen, stehen Behörden vor einer strukturellen Herausforderung: Der Gegenstand ihrer Aufsicht weist eine hohe technische Komplexität auf und unterliegt dynamischen Veränderungsprozessen. Die DEK hält daher die **praktische Befähigung der Behörden** für besonders wichtig. Sie empfiehlt der Bundesregierung nachdrücklich, die auf Bundesebene zuständigen Behörden mit den erforderlichen finanziellen, personellen und technischen Ressourcen auszustatten. Der Entwurf eines Besoldungsstrukturenmodernisierungsgesetzes, das ab 2020 die Gehälter und Zulagen von IT-Fachkräften im öffentlichen Dienst erhöhen und neu regeln soll, ist als erster Schritt ausdrücklich zu begrüßen. Im Lichte der erheblichen Herausforderung, gut geschulte Fachkräfte für die Verwaltung zu gewinnen, werden jedoch weitere Maßnahmen zeitnah erforderlich sein.

Darüber hinaus empfiehlt die DEK der Bundesregierung, eine behördliche Einheit in Form eines **Kompetenzzentrums Algorithmische Systeme** zu etablieren, welche die sektoralen Behörden bei der Aufgabe unterstützt, algorithmische Systeme zu überwachen. Die Aufgabe einer solchen Einrichtung sollte es nicht nur sein, das für die Aufsicht über kritische algorithmische Systeme erforderliche sachlich-methodische Wissen zu gewinnen, auszuwerten, weiterzuentwickeln und weiterzugeben. Das Kompetenzzentrum sollte (in Abstimmung und auf Anforderung der sektorspezifischen Behörden) vor allem die sektorspezifischen Aufsichtsbehörden beim Aufbau der Expertise unterstützen, die erforderlich ist, um die Aufgaben zu erledigen und algorithmische Systeme mit Blick auf ihre Kritikalität zu evaluieren. Dies erstreckt sich insbesondere auf die Aufgabe des Kompetenzzentrums, **Kriterien, Verfahren und Werkzeuge** für die Kontrolle algorithmischer Systeme fortzuentwickeln. Dazu gehören auch **Maßstäbe, um die Kritikalität zu beurteilen**, und die Konformität kritischer algorithmischer Systeme zu prüfen. Ein solches Kompetenzzentrum nimmt darüber hinaus wichtige **vermittelnde Beratungsfunktionen** war: Es berät im Rahmen ihrer Möglichkeiten nicht nur Stellen des Bundes, der Länder und Kommunen, sondern auch der Hersteller, Betreiber, Anwender und betroffener Personen im Umgang mit und bei der Entwicklung von algorithmischen Systemen. Darüber hinaus nimmt sie an internationalen und europäischen Initiativen zum Aufbau hinreichender Kontrollexpertise einschließlich Normierungsverfahren teil. Eigene Aufsichtsbefugnisse hat das Kompetenzzentrum demgegenüber nicht. Diese verbleiben bei den sektoralen Aufsichtsbehörden. Die Serviceeinheit sollte entweder als eigenständige Bundesbehörde neu errichtet werden oder an eine bestehende Querschnittsbehörde, wie etwa das BSI, angebunden werden.

Perspektivisch erscheint es nach Auffassung der DEK sinnvoll, auch auf der **Ebene der Europäischen Union** eine entsprechende Stelle, etwa in Form einer Agentur, anzusiedeln. Hierauf sollte die Bundesregierung hinwirken.

Soweit staatliche Stellen sich bei der Erledigung ihrer Aufgaben und zusätzlich zum Aufbau eigenen Sachverständes auch der **Expertise Privater** bedienen wollen oder in die Aufgabenerledigung Private einbeziehen wollen, stehen dem nach Auffassung der DEK keine prinzipiellen Hindernisse entgegen, solange die allgemeinen verfassungs- und verwaltungsrechtlichen Vorgaben für derartige Kooperationen beachtet werden. Im Gegen teil können entsprechende Kooperationen, etwa auch in Form der Beleihung, genutzt werden, um dem gegenwärtigen Mangel an Fachkräften und Fachkenntnissen in der Verwaltung entgegenzuwirken.

### 5.1.2 Aufgabenangemessene Ausgestaltung der Kontrollbefugnisse

Den jeweils zuständigen Behörden sollte der Normgeber die zur Aufsicht über algorithmische Systeme notwendigen **Eingriffsbefugnisse**, u.a. Auskunfts-, Einsichts- und Zugangsrechte, hinreichend klar **durch Gesetz zuweisen**. Blaupausen für derartige behördliche Befugnisse zur inhaltlichen Kontrolle bestehen in verschiedenen Rechtsgebieten.<sup>10</sup>

Die zuständigen Aufsichtsbehörden müssen jederzeit die Möglichkeit haben, algorithmische Systeme in sensiblen Anwendungsfeldern oder solche mit hohem Schädigungspotenzial zu **überprüfen**. Die dabei zur Anwendung kommenden Überprüfungs- und Testverfahren müssen insbesondere Systeme umfassen, bei denen eine Interaktion mit dem Nutzer erfolgt. Dies kann beispielsweise über standardisierte Schnittstellen erfolgen. Mit diesem Zugang lassen sich sog. Input-Output-Tests durchführen, die z.B. prüfen, ob ein algorithmisches System systematisch Gruppen benachteiligt. Dies ist insbesondere bei lernenden Systemen sinnvoll, die im Laufe der Zeit ihre internen Regeln anpassen. Dabei muss sichergestellt sein, dass die Prüfung von lernenden Systemen nicht zu einer Änderung des Regelsystems führt, indem das System während der Prüfung aus den Prüfungsdaten lernt.

<sup>10</sup> Beispielsweise regelt Art. 58 DSGVO die Untersuchungsbefugnisse der Datenschutzaufsicht, § 32e GWB regelt die Sektoruntersuchungen durch das Bundeskartellamt. Die Kontrolle des Hochfrequenzhandels durch Finanzaufsichtsbehörden basiert auf § 6 Abs. 4 WpHG, § 3 Abs. 4 Satz 4 Nr. 5 BörsG n.F. i.V.m. § 7 Abs. 3 BörsG.



Bei der gesetzlichen Kompetenzzuweisung ist sicherzustellen, dass die Aufsichtsbehörden im Falle eines festgestellten Rechtsverstoßes die Befugnis haben, die Betreiber der algorithmischen Systeme zu verpflichten, die Systeme rechtskonform zu gestalten (zum Beispiel durch Anpassung der Datenbasis) und ggf. **Sanktionen** auszusprechen. Die Aufsichtsbehörden sollen, sofern dies im Einzelfall verhältnismäßig ist, auch behördliche **Verbote** des Einsatzes rechtswidriger algorithmischer Systeme (oder ihrer Komponenten) aussprechen können.

### 5.1.3 Kritikalitätsangemessene Kontrolltiefe

Wer das Verhalten eines algorithmischen Systems wissentlich überprüfen will, muss **alle Elemente des algorithmischen Systems** im Blick haben. Eine behördliche Überprüfung kann sich – und muss sich ggf. – auf die Trainingsdaten und verwendeten Lernverfahren, das finale Regelmodell sowie die verwendeten Inputdaten und Outputdaten, die den Entscheidungen zugrunde liegen, erstrecken. Um Biases oder (statistische) Fehlerquoten (insgesamt oder für bestimmte Teilgruppen) zu identifizieren, die ein System aufweist, können zudem Qualitätsmaße zur Datengrundlage und Modellgüte (Trainingsmodell, finales Entscheidungsmodell) Berücksichtigung finden. In methodischer Hinsicht kann eine Prüfung durch Analyse großer Datenmengen, die Prüfung der Gewichtung von Faktoren in komplexen multidimensionalen Modellen sowie eine Input-Throughput-Output-Analyse erfolgen.

Aufgrund der Komplexität der Materie und involvierten Datenmengen, kann der Einsatz von Kontrollalgorithmen die Effizienz und Effektivität der Überprüfung erheblich steigern. Sie können systematisch nach auffälligen Mustern in der Datenbasis und den Ergebnissen eines algorithmischen Systems suchen, die beispielsweise Aufschluss über eine Diskriminierung geben können.

Welches Maß an Kontrolltiefe im konkreten Fall erforderlich ist, sollte sich nach dem Einsatzbereich und der Kritikalität des Systems bestimmen. Bei Systemen, die nur ein gewisses Schädigungspotential aufweisen (Stufe 2), kann es ausreichen, wenn der Gesetzgeber die behördliche Kontrolle auf eine Ergebniskontrolle im Falle eines dokumentierten Fehlversagens des Systems beschränkt. In Bereichen, die ein hohes Schädigungspotential aufweisen, kann es hingegen erforderlich sein, den Systembetreibern vorzuschreiben, eine standardisierte Schnittstelle vorzuhalten.

Ob eine behördliche Kontrolle Betriebs- und **Geschäftsgeheimnisse** der Systembetreiber oder **Persönlichkeitsrechte** Dritter berührt, spielt nach Ansicht der DEK bei der behördlichen Kontrolle auf keiner Stufe der Kritikalitätspyramide eine Rolle. Da Aufsichtsbehörden verpflichtet sind, die im Wege der Kontrolle gewonnenen Informationen als Teil des Amtsgeheimnisses vertraulich zu behandeln, stehen diese Gesichtspunkte einer weitreichenden Befugnis zur vollständigen und detaillierten Überprüfung auf gesetzlicher Grundlage nicht entgegen.

Testergebnisse sachgerecht zu interpretieren, ist aus technischer Sicht alles andere als trivial. Insbesondere ist nicht immer eindeutig, ob sie wirklich einen Fehler eines algorithmischen Systems ans Tageslicht befördern. Das schränkt ihre Beweisfunktion ein. Es bedarf deswegen auch einer Verständigung über die Qualität und den Erkenntniswert der unterschiedlichen Testverfahren und Audits – insbesondere darüber, welcher Beweiswert ihnen in gerichtlichen Verfahren zukommt, um Betroffenenrechte durchzusetzen. Die DEK empfiehlt daher der Bundesregierung Initiativen zu unterstützen, die – ggf. nach Anwendungsbereichen differenzierte – **technisch-statistische Standards für Testverfahren und Audits entwickelt**. Dem Kompetenzzentrum Algorithmische Systeme (→ siehe dazu bereits oben 5.1.1) sollte bei diesen Bemühungen eine führende Rolle zukommen.

## Use Case: Personalisierte Preise II – Ex-post Kontrolle durch Aufsichtsinstitutionen

Aufsichtsinstitutionen könnten überprüfen, ob sich algorithmische Pricing-Systeme im Online-Handel rechtskonform verhalten oder etwa geschützte Bevölkerungsgruppen (im Sinne des Allgemeinen Gleichbehandlungsgesetzes (AGG)) diskriminieren. So könnten Aufsichtsbehörden nach auffälligen Mustern in der Datenbasis und den ausgegebenen Preisen suchen, die Aufschluss über eine mögliche Diskriminierung geben können.

Dafür muss die Aufsicht nicht die (möglicherweise hochkomplexen) Regeln des zugrunde liegenden Algorithmus über eine Analyse des Codes nachvollziehen.

Eine effektive Kontrolle kann mit Hilfe statistischer Tests erfolgen. Diese analysieren, wie sich ausgegebene Preise – ceteris paribus – in Abhängigkeit von Input-Daten ändern, die mit bestimmten Bevölkerungsgruppen assoziiert werden. Gibt das System beispielsweise für Verbraucher höhere Preise aus, wenn bei deren Input-Daten nur das Geschlecht von „männlich“ auf „weiblich“ geändert wird oder korrelieren die ausgegebenen Preise mit durch das Gleichstellungsrecht geschützten Eigenschaften einzelner Bevölkerungsgruppen (etwa über sog. Proxys), lässt sich das mathematisch-statistisch ermitteln.<sup>11</sup>

<sup>11</sup> Vgl. Gesellschaft für Informatik: Technische und rechtliche Betrachtungen algorithmischer Entscheidungsverfahren. Gutachten der Fachgruppe Rechtsinformatik der Gesellschaft für Informatik e.V. im Auftrag des Sachverständigenrats für Verbraucherfragen, Berlin, URL: [www.svr-verbraucherfragen.de/wp-content/uploads/GI\\_Studie\\_Algorithmenregulierung.pdf](http://www.svr-verbraucherfragen.de/wp-content/uploads/GI_Studie_Algorithmenregulierung.pdf) [Zugriff: 07.03.2019] S. 63 ff.

## 5.2 Unternehmerische Selbstregulierung und Ko-Regulierung

Algorithmische Systeme flächendeckend gesetzgeberisch regulatorisch zu erfassen, ist weder möglich noch notwendig. Vielmehr können grundsätzlich auch verschiedene Modelle der Selbst- und Ko-Regulierung für bestimmte Konstellationen ergänzend adäquate Antworten liefern. Ko-Regulierung zeichnet sich dadurch aus, Regulierungswege zwischen staatlicher Regulierung und privater Selbstregulierung zu beschreiten. Prägend ist das Zusammenwirken einer staatlich-hoheitlichen Komponente und einer privat-institutionellen Komponente.

### 5.2.1 Selbstregulierung und -zertifizierung

Selbstregulierung in Form einer internen Überprüfung durch den Hersteller oder Betreiber des algorithmischen Systems empfiehlt sich aus Sicht der Datenethikkommision bereits für die unterste Stufe der Kritikalitätspyramide. Dies kann durch eine Selbstzertifizierung der Hersteller oder Betreiber auf der Grundlage spezifischer Standards für algorithmische Systeme unterstützt werden. Der Vorteil eines solchen Systems liegt dabei insbesondere darin, dass die Selbstzertifizierungseinrichtungen aufgrund ihrer **inhaltlichen Nähe zu spezifischen Thematiken** über das notwendige Know-how verfügen. So können Experten auch aus betroffenen Unternehmen selbst bei der Entwicklung die rechtlichen Maßstäbe und die Kontrolle ihrer Einhaltung berücksichtigen und diesen unternehmerischen Sachverstand gegebenenfalls auch institutionell in die Regulierungsmechanismen einbinden. Freilich gewährleistet eine rein interne und freiwillige Selbstkontrolle keine unabhängige Überwachung und stellt im Falle von Verstößen keine effektive Sanktionsierung sicher.



Ergänzen ließe sich die Selbstregulierungsarchitektur durch ein Modell der regulierten Selbstkontrolle, das externe Standards für das Qualitäts- und Risikomanagement der Selbstkontrolle vorgibt, die sodann auch extern überwachbar sind. Ein vergleichbares System sieht die DSGVO vor. So eröffnet Art. 40 DSGVO die Möglichkeit, Generalklauseln der DSGVO zu konkretisieren und auf bestimmte, für die Adressaten der Verhaltensregeln bedeutsame Lebenssachverhalte anwendbar zu machen sowie branchenintern Mindeststandards zu setzen. Um die damit beabsichtigte Effektivität der Regulierung gewährleisten zu können, muss eine wirksame Überwachung sicherstellen, dass die genehmigten Verhaltensregeln aus Art. 40 DSGVO tatsächlich eingehalten werden. Verpflichtend müssen nicht nur die materiellen Verhaltensregeln, sondern auch die prozeduralen Vorschriften zur Überwachung, Steuerung und Sanktionierung für den Fall der Nichteinhaltung festgelegt werden.

Sofern ein Anbieter sich der freiwilligen Selbstkontrolle anschließt und das dort vereinbarte Verfahren nachweislich einhält, kann der Normgeber Privilegien bei Aufsichtsmaßnahmen gewähren. Bedingung eines solchen Vorgehens ist, dass Anbieter in Wahrnehmung ihrer unternehmerischen Verantwortung im Zusammenwirken mit einer privaten Selbstkontrolleinrichtung Verfahrensstandards entwickeln, welche die Aufsicht anerkennt. Die Einbindung zivilgesellschaftlicher Organisationen in die Erarbeitung ist dabei erforderlich, um die Bürger- und Verbraucherinteressen angemessen zu repräsentieren und berücksichtigen zu können.

### 5.2.2 Erarbeitung eines Verhaltenscodex

Als Teil des Konzepts regulierter Selbstregulierung ist ein sog. **Algorithmic Accountability Codex** erwägenswert, der dem Comply-or-explain-Ansatz folgt, wie er aus anderen Teilen der Rechtsordnung bekannt ist. Er könnte die Regulierungsadressaten dazu verpflichten, sich dazu zu erklären, ob und inwieweit sie den Empfehlungen des Kodex folgen oder nicht.<sup>12</sup> An falsche Erklärungen knüpfen sich dann Sanktionen. Auf diese Weise könnte ein zu erarbeitender Kodex Bindungswirkung entfalten, indem er Unternehmen und Behörden für die Folgen des Einsatzes algorithmischer Systeme in die Verantwortung nimmt. Dieser Kodex kann sich zum Beispiel im Kontext von sog. Corporate Digital Responsibility-Leitlinien (→ hierzu oben Teil D, 2) herausbilden oder umgekehrt auch solche Leitlinien beeinflussen. Dabei wird sich zeigen, welche Granularität für Kodizes und Leitlinien sich als praktikabel erweist bzw. für welche bereichsspezifischen ethischen Herausforderungen ein eigener Kodex sinnvoll sein kann.

Maßgeblich für eine Steuerungsfunktion eines Kodex sind die Qualität der definierten Anforderungen und die Rahmenbedingungen, also die Kontrollmöglichkeiten durch unabhängige Externe und die Sanktionsfähigkeit bei Verstößen. Einen solchen Kodex zu erarbeiten, sollte die Aufgabe eines unabhängigen paritätisch besetzten Gremiums sein. Das Gremium müsste gleichermaßen Hersteller, Betreiber, Wissenschaft und die Zivilgesellschaft einbinden. Ob die „Regierungskommission Deutscher Corporate Governance Kodex“ ([www.dcgk.de](http://www.dcgk.de)) hierfür als Vorbild dienen kann, bleibt zu prüfen.

Darüber hinaus oder alternativ kommen bindende Erklärungen der Hersteller und Betreiber algorithmischer Systeme untereinander in Betracht.

12 Mario Martini: Juristenzeitung (JZ), 2017, S. 1017, 1022 f.

### 5.2.3 Gütesiegel für algorithmische Systeme

Um eine wirksame Algorithmenregulierung zu unterstützen, ist es sinnvoll, Gütesiegel für algorithmische Systeme zu etablieren. Dabei kann es sich um freiwillige oder verpflichtende Schutzzeichen handeln. Sie machen dem Nutzer transparent, inwieweit ein algorithmisches System bestimmte Anforderungen erfüllt. Zu klären ist dabei, wer die Anforderungen eines Gütesiegels bestimmt und wer dafür im Detail zuständig ist, die mit dem Gütesiegel verbundenen Anforderungen zu erfüllen und inwieweit Verstöße sanktionsbewehrt sind. Ebenso wie im Falle eines Algorithmic Accountability Codex sollte die Aufgabe, die Anforderungen eines Gütesiegels zu definieren, in den Händen einer unabhängigen, paritätisch besetzten Kommission liegen, die sich aus der Reihe der Betreiber algorithmischer Systeme, Wissenschaft und Zivilgesellschaft zusammensetzt.

### 5.2.4 Ansprechpartner für algorithmische Systeme in Unternehmen und Behörden

Unternehmen und Behörden, die mit kritischen algorithmischen Systemen (ab Stufe 2) arbeiten, sollten (jedenfalls ab einer bestimmten Unternehmens- bzw. Behördengröße) einen Ansprechpartner benennen müssen, der für die Kommunikation mit Behörden zur Verfügung steht und zu einer Mitwirkung verpflichtet ist. In jedem Fall muss der Ansprechpartner **spezifischen Sachverstand** haben. Er überwacht die Verwendung von algorithmischen Systemen intern und berät die Unternehmens- und Behördenleitung. Er ist in seiner Funktion unabhängig. In Anlehnung an den Datenschutzbeauftragten könnte er als Bindeglied zwischen Aufsicht, Betreiber eines algorithmischen Systems und betroffenen Personengruppen fungieren. Dies trägt zusätzlich dazu bei, in Unternehmen und Behörden für ein stärkeres Problembewusstsein und für einen erhöhten Kontrolldruck von innen heraus zu sorgen.

### 5.2.5 Einbindung zivilgesellschaftlicher Akteure

Um sicherzustellen, dass bei der Überprüfung von algorithmischen Systemen die Interessen der Zivilgesellschaft und der betroffenen Unternehmen angemessen Berücksichtigung finden, sollten **Beiräte** bei den sektorspezifisch zuständigen Behörden eingerichtet werden und zivilgesellschaftliche Akteure sollten auch etwa im Zusammenhang eines Kodex beteiligt werden. In diesen Beiräten sollten Vertreter zivilgesellschaftlicher Organisationen und Benannte der Unternehmen in einem ausgewogenen Verhältnis vertreten sein, um sicherzustellen, dass sowohl den Interessen betroffener Individuen und Gruppen als auch denen betroffener Unternehmen bei der Prüfung angemessen Rechnung getragen wird.

## 5.3 Technische Standardisierung

Normungsorganisationen wie ISO/IEC, IEEE, IETF, ITU, ETSI, W3C, CEN oder DIN, die technische Standards für Informations- und Kommunikationstechnologien setzen, können aus Sicht der DEK einen wichtigen Beitrag dazu leisten, die Anforderungen an algorithmische Systeme bereichsspezifisch zu konkretisieren. Technische Standards, die ethische und rechtliche Anforderungen berücksichtigen, können die Rechtssicherheit derjenigen Unternehmen, die die algorithmischen Systeme entwickeln und einsetzen. Zudem können sie in Einzelbereichen auch die Anforderungen an die Rechtmäßigkeit von algorithmischen Systemen handhabbar in konkrete Handlungsanweisungen übersetzen.

Die DEK sieht technische Standards grundsätzlich als ein sinnvolles Instrument zwischen „klassischer“ staatlicher Regulierung und rein privater Selbstregulierung an. Sie empfiehlt daher der Bundesregierung, in geeigneter Weise auf die Entwicklung und Verabschiedung technischer Standards hinzuwirken, die vor Risiken schützen, welche von algorithmischen Systemen ausgehen.



Die Bundesregierung sollte aus Sicht der DEK allerdings auch die **Grenzen technischer Normung** nicht aus den Augen verlieren (→ oben Teil D, 6). Technische Normen können weder die Definition klarer gesetzlicher Anforderungen an algorithmische Systeme noch die behördliche Aufsicht über den Einsatz derartiger Systeme ersetzen. An dem Grundsatz, dass gesetzliche Vorgaben umso de taillierter ausfallen müssen, je intensiver Grundrechte von B Bürgern betroffen sind, gilt es schon aus verfassungs rechtlichen Gründen festzuhalten. Konkret bedeutet das, dass zunächst der Gesetzgeber den gesetzlichen Rahmen abstecken muss – nicht Gremien zur technischen Standardsetzung. Darin manifestiert sich nicht zuletzt ein Integritätsschutz der Entscheidungsfindung, da durch die aktive Beteiligung der Vertreter von Branchen bzw. betroffenen Unternehmen neben großem technischen Sachverstand natürlich auch die Interessen dieser Unternehmen bzw. Branchen in die Formulierung der technischen Norm häufig ungefiltert einfließen.

Wer sich nicht an Regulierungsvorgaben hält, der erlangt im Wettbewerb unter Umständen einen – allerdings unlauteren – Vorteil. Um einen „Vorsprung durch Rechtsbruch“ zu verhindern, sollten Wettbewerbs- und Verbraucherverbände die Möglichkeit haben, solche Rechtsverletzungen abzustellen.

#### 5.4 Institutioneller Rechtsschutz (insbesondere Verbandsklagerechte)

Die in Deutschland bewährten Klagerechte von Wett bewerbern und von Wettbewerbs- und Verbraucherver bänden sind ein zentraler Baustein einer **zivilgesellschaft lichen Kontrolle** des Einsatzes algorithmischer Systeme. Besonders legitimierte zivilgesellschaftliche Akteure können durch private Klagerechte die Einhaltung von Rechtsvorschriften im Bereich des Vertragsrechts und des Lauterkeitsrechts sicherstellen, ohne hierbei auf das Tätigwerden von Behörden oder die Mandatierung durch einzelne Betroffene angewiesen zu sein. Dieser zivilrecht liche Ansatz ist besonders marktnah und reaktionsschnell sowie dadurch im internationalen Vergleich erfolgreich. Verbände sind grundsätzlich politisch und administrativ unabhängig und können so eigenverantwortlich dafür ein treten, dass die Wettbewerbsordnung und das Verbraucherrecht im gemeinsamen Interesse von Verbrauchern und Unternehmen effizient vor unlauteren und verbraucherschädigenden Geschäftspraktiken geschützt wird.

# Zusammenfassung der wichtigsten Handlungsempfehlungen

## 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 erwägswert, 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.

## 6. Besonderes Augenmerk: Algorithmische Systeme bei Medienintermediären

### 6.1 Die Relevanz für den demokratischen Prozess am Beispiel sozialer Netzwerke

Längst sind soziale Netzwerke, Suchmaschinen und ähnliche Dienste aus dem Alltag vieler Menschen nicht mehr wegzudenken: Sie ermöglichen Nutzern, sich in Echtzeit über das Neueste aus den Nachrichten und dem Freundeskreis zu informieren, sind Plattformen etwa für Selbstdarstellung und Kommunikation, dienen der Unterhaltung und der wirtschaftlichen Betätigung, einschließlich der Werbung.

In der Summe entwickeln sie eine immer größere Bedeutung für die private und öffentliche Meinungsbildung. Um der Masse an Informationen Herr zu werden, nutzen die Betreiber derartiger Dienste algorithmische Systeme. Diese sollen unter anderem die Interessen, Neigungen und Überzeugungen der Nutzer erkennen, die für sie potenziell relevanten Beiträge identifizieren, ihnen ähnliche Beiträge präsentieren, um Interaktionen mit dem Netzwerk hervorzurufen, sowie illegale oder anstößige Beiträge ausfiltern. Das wirtschaftliche Ziel besteht in erster Linie darin, hohe Werbeeinnahmen zu generieren.

Abhängig von ihrer Reichweite und ihren Inhalten können Medienintermediäre einen tiefgreifenden Einfluss auf den demokratischen Prozess haben. So nutzen immer mehr Menschen soziale Netzwerke auch, um sich über Politik und Weltgeschehen zu informieren. Dabei eröffnen soziale Netzwerke den Nutzern neue Möglichkeiten der Partizipation an der Informationsgesellschaft. In diesem Sinne sind sie **Medium und Faktor für Informationen und Meinungsaustausch**.

Zugleich stellt die Konzentration der öffentlichen Debatte auf einigen wenigen privaten Plattformen aber auch eine Herausforderung für die Demokratie dar. Denn als Wirtschaftsakteure haben die privaten Betreiber sozialer Netzwerke ein Interesse daran, den Zugang zu ihrem Netzwerk und das Verhalten darauf in erster Linie nach ökonomischen Gesichtspunkten auszurichten, statt gesellschaftliche Interessen an einem vielfältigen, am Gemeinwohl orientierten Meinungsbildungsprozess in den Vordergrund zu rücken. Der Einsatz algorithmischer Systeme, die **überwiegend an ökonomischen Kriterien orientiert** sind, kann dabei negative Folgen für die Meinungsvielfalt in sozialen Netzwerken haben.

Zudem kann es durch die Nutzung von Services zur Manipulation der Meinungsbildung kommen. Dies kann einerseits unbeabsichtigt durch bestimmte Charakteristika zugrundliegender Software, wie beispielsweise Recommender Systeme, geschehen. Andererseits können diese Systeme auch bewusst von diversen Akteuren manipulativ eingesetzt werden. Bislang haben die Betreiber sozialer Netzwerke solchen demokratiegefährdenden Aktivitäten nicht hinreichend vorgebeugt. Zugleich fehlt es insbesondere mit Blick auf ihre **hohe Kritikalität** an einem staatlichen Ordnungsrahmen und an einer gesellschaftlichen Kontrolle.



Die DEK sieht perspektivisch bei Medienintermediären mit Torwächterfunktion ein hohes Gefährdungspotential für die Demokratie und dementsprechenden **Regulierungsbedarf**. Die DEK hält es für unerlässlich, dass der Gesetzgeber einen angemessenen Ordnungsrahmen für den Einsatz algorithmischer Systeme durch Medienintermediäre schafft. Zwar obliegt es nach Auffassung der DEK zunächst den Betreibern solcher Plattformen und Dienste selbst, Grundregeln für ein faires Miteinander im Meinungsbildungsprozess zu definieren und durchzusetzen. Dieses „digitale Hausrecht“ hat jedoch Grenzen, insbesondere dort, wo die Integrität des demokratischen Prozesses berührt ist. Abhängig von der Marktmacht und Torwächterfunktion solcher Plattformen und Dienste bestehen im Wege der mittelbaren Drittirkung<sup>13</sup> grundrechtliche Verpflichtungen an die Betreiber. Diese sollte der Gesetzgeber nach Auffassung der DEK konkretisierende Regelungen – insbesondere auch mit Blick auf den Einsatz algorithmischer Systeme durch und in Plattformen und Diensten mit Marktmacht und Torwächterfunktion – stärker als bisher einfachgesetzlich ausformen und präzisieren. Dies ist auch relevant für die von der DEK empfohlene EUVAS (→ oben 3.3).

Regulierungsbedarf besteht auch vor dem Hintergrund der Regulierungsgerechtigkeit im Vergleich zu Rundfunkanbietern. Die DEK empfiehlt der Bundesregierung zu prüfen, wie Gefahren durch besonders meinungsmächtige Anbieter begegnet werden kann. Hierzu kann ein Spektrum von Maßnahmen in Frage kommen, das sich prinzipiell von Steigerung der Transparenz bis hin zu einer Ex-ante-Kontrolle in der Form eines Lizenziertungsverfahrens für demokratierelevante algorithmische Systeme erstreckt.

## 6.2 Vielfalt bei Medienintermediären am Beispiel sozialer Netzwerke

Die Funktionspluralität sozialer Netzwerke sowie die überwiegend hohe Kritikalität der von ihnen genutzten algorithmischen Systeme stellen den von der DEK empfohlenen Ansatz einer risikoadaptierten Regulierung für algorithmische Systeme allerdings vor besondere Herausforderungen. Für besonders zielführend hält die DEK vor diesem Hintergrund positive gesetzliche Vorgaben für soziale Netzwerke, die etwa die **Transparenz und Vielfalt des dortigen Diskurses** verbessern und die **Rechte der Nutzer** stärken.

Jedenfalls dort, wo soziale Netzwerke eine beherrschende Marktmacht haben, fordert die DEK weitergehende Maßnahmen zur **Vielfaltssicherung**, weil ausschließlich abwehrende Maßnahmen nicht ausreichen. In derartigen Netzwerken operierende algorithmische Systeme, die Auswirkungen auf die für die Demokratie konstitutive Freiheit und Vielfalt der Meinungsbildung haben, weisen bereits aufgrund ihrer Reichweite eine besonders hohe Kritikalität auf. Den Gesetzgeber trifft daher nach Auffassung der DEK eine ethische und eine verfassungsrechtliche Pflicht, zum Schutz der Demokratie eine **positive Medienordnung** für Medienintermediäre zu etablieren. Dies kann durch eine Transformation der Medienrechtsordnung geschehen.

Der Gesetzgeber muss geeignete Maßnahmen treffen, um sicherzustellen, dass im Gesamtangebot die plurale Vielfalt der Meinungen abgebildet sowie die **Ausgewogenheit, Neutralität und Tendenzfreiheit in der Informationsgesellschaft** gewährleistet ist.<sup>14</sup> Das gilt für meinungsmächtige Medienintermediäre mit Torwächterfunktion erst recht. Laut Bundesverfassungsgericht bedarf es zur Sicherung pluraler Vielfalt materieller, organisatorischer und Verfahrensregelungen, die an der Aufgabe der Herstellung der Kommunikationsfreiheit orientiert sind und deshalb geeignet sind zu bewirken, was Art. 5 Abs. 1 GG gewährleisten will.

13 BVerfGE 128, 226, 249 (FRAPORT); 148, 267 ff. Rn. 32 ff. (Stadionverbot).

14 Vgl. BVerfGE 136, 9, 28 m.w.N.

Vor diesem Hintergrund stehen die Gesetzgeber in den Bundesländern, bei denen die Zuständigkeit für das Medienrecht liegt, in der Pflicht, die genannten Vorgaben umzusetzen. Dasselbe gilt für den Gesetzgeber einer EU-Verordnung für Algorithmische Systeme (EUVAS) (s.o.). Schon aktuell unterfallen Medienintermediäre als sog. Video-Sharing-Plattformen (VSP) der AVMD-Richtlinie<sup>15</sup>, weil sie nutzergenerierte Inhalte für die Allgemeinheit bereitstellen. Auch der Entwurf des Mediendiens-te-Staatsvertrages nimmt Medienintermediäre in seinen Anwendungsbereich auf. Die DEK begrüßt insoweit erneut die im Entwurf für einen **Medienstaatsvertrag (MStV-E)** vorgesehenen Vorgaben für die Transparenz sozialer Netzwerke als ersten Schritt in diese Richtung.

Bei der Ausgestaltung der Vorgaben haben die **Lan-desgesetzgeber** weitreichende Gestaltungsspielräume. Allerdings müssen sie die Entscheidung über das Regulierungsmodell selber treffen und dürfen sie nicht einer Vereinbarung der Privaten überlassen. Aus Sicht der DEK sollten Pluralitätspflichten für Medienintermediäre jedenfalls die Verpflichtung zum Einsatz solcher algorithmischer Systeme umfassen, die zumindest als zusätzliches Angebot auch einen Zugriff auf eine tendenzfreie, ausgewogene und die plurale Meinungsvielfalt abbildende Zusammenstellung von Beiträgen und Informationen verschaffen.<sup>16</sup>

Auf Basis dieser Überlegungen empfiehlt die DEK der Bundesregierung ferner, zu prüfen, ob es weitere Bereiche gibt, in denen unabhängig von der hier diskutierten demokratirelevanten Situation eine entsprechende Pflicht zur Statuierung von Neutralitätsgeboten und Vielfaltsvorgaben geboten erscheint. In Betracht kommt hier etwa der **Schutz Minderjähriger** vor Beeinflussung durch und über soziale Netzwerke.

### 6.3 Kennzeichnungspflicht für Social Bots

Der demokratische Prozess beruht im Kern auf der freien Meinungs- und Willensbildung menschlicher Akteure. Auf diversen Plattformen werden jedoch Bots, d. h. Software-programme, eingesetzt, welche den **Anschein erwecken, menschliche Nutzer** zu sein. Nach Auffassung der DEK ist es hochproblematisch, wenn solche Bots dazu genutzt werden, individuelle Nutzer bzw. den öffentlichen Diskurs zu manipulieren oder gar bei anstehenden politischen Entscheidungen das Abstimmungsergebnis in eine bestimmte Richtung zu lenken. Die Vortäuschung der Menschlichkeit suggeriert zum einen fälschlicherweise, dass die verbreiteten Äußerungen das Ergebnis autono-mer Reflexion und eigenständiger politischer Meinungs-bildung seien. Zum anderen kann durch Automatisierung die Anzahl und Frequenz von Meinungäußerungen massiv erhöht werden, wodurch auch die Beurteilung fak-tischer Mehrheitsverhältnisse von Meinungen erschwert bzw. unmöglich wird. Nach Ansicht der DEK ist hier ein regulatorisches Eingreifen erforderlich.

Vor diesem Hintergrund empfiehlt die DEK als **trans-parenzsteigernde Maßnahme** eine Kennzeichnungs-pflicht für Social Bots in sozialen Netzwerken. Schon nach allgemeinen Erwägungen empfiehlt die DEK eine solche Kennzeichnungspflicht überall dort, wo eine Verwechslungsgefahr von Social Bots mit mensch-lichen Gesprächspartner besteht (→ oben). Aufgrund des besonderen Gefährdungspotentials für den demokrat-i-schen Prozess hält die DEK darüber hinaus jedenfalls eine Kennzeichnungspflicht für solche Social Bots, die Einfluss auf politische Meinungsbildungsprozesse nehmen, auch unabhängig von einer konkreten Verwechslungsgefahr, für unbedingt geboten.

<sup>15</sup> Richtlinie 2010/13/EU vom 10.3.2019 zur Koordinierung bestimmter Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Bereitstellung audiovisueller Mediendienste (Richtlinie über audiovisuelle Mediendienste).

<sup>16</sup> Dazu Rolf Schwartmann / Maximilian Hermann / Robin Muhlenbeck: MultiMedia und Recht (MMR), 2019 (8), S. 498, 498 ff.



#### 6.4 Maßnahmen gegen „Fake News“

Eine Kennzeichnungspflicht für Social Bots kann der automatisierten Verbreitung sog. Fake News entgegenwirken. Darüber hinaus ist die DEK aber der Auffassung, dass das Konzept von Fake News sich **nicht als Anknüpfungspunkte für eine medienrechtliche Regulierung** eignet. Die Vorstellung eines gesetzlichen Fake News-Tatbestands, der eine objektive, trennscharfe Linie zwischen zugespitzter oder satirischer Meinungsäußerung und absichtlich-falscher Darstellung von Nachrichten zieht, scheitert an der Komplexität menschlicher Kommunikation. Zudem kann eine – typischerweise mit dem Begriff der Fake News assoziierte – Desinformation und Manipulation der öffentlichen Meinungsbildung auch durch eine selektive Darstellung wahrer Tatsachen erfolgen.

Darüber hinaus empfiehlt die DEK insbesondere dem Gesetzgeber den Betreibern sozialer Netzwerke, den Nutzern ein einfach handhabbares **Recht auf Gegendarstellung** einzuräumen, bei der die Richtigstellung einer nachgewiesenen falschen Behauptung (z.B. ein erfundenes Zitat) in die „Timeline“, den „Newsfeed“ o.ä. aller Nutzer eingespeist werden muss, von denen das Netzwerk anhand vorhandener Daten rekonstruieren kann, dass sie die falsche Tatsachenbehauptung angeboten bekommen hatten.

Die DEK betont, dass der Staat keine Anreizstruktur zu einer Kollateralzensur („collateral censorship“) durch soziale Netzwerke schaffen darf. Zum Schutz vor sog. overblocking ist es daher aus Sicht der DEK erforderlich, parallel zu den den Betreibern auferlegten Pflichten den Betroffenen zeitnahe und effiziente verfahrensrechtliche Schutzmechanismen einzuräumen. Hierzu gehört nach Auffassung der DEK insbesondere ein **Recht auf ein wirksames Verfahren, um gelöschte Beiträge wieder einzustellen**, solange diese keinen Gesetzen widersprechen; eine Berufung der Netzwerke auf ihre eigenen Regeln darf als Grund für eine dauerhafte Löschung/Blockade allein nicht ausreichen. Derartige Rechte müssen nach Auffassung der DEK Nutzerinnen und Nutzer gegenüber allen sozialen Netzwerken gelten.

#### 6.5 Transparenzpflichten für News-Aggregatoren

Soweit soziale Netzwerke algorithmische Systeme verwenden, die auch journalistisch-redaktionelle Angebote Dritter aggregieren, selektieren und allgemein zugänglich präsentieren, sollten sie Nutzern und interessierten Dritten in dem Maße Einblick in ihr technisches Verfahren der Nachrichtenauswahl und -priorisierung gewähren müssen, der nachvollziehbar macht, wie eine Empfehlung im Einzelfall zu Stande kommt. Dabei genießt das demokratische Informationsinteresse grundsätzlich Vorrang vor den Geschäftsgeheimnissen der Medienintermediäre. Solche Offenlegungspflichten sollten sich im Interesse eines fairen Meinungsbildungsprozesses und –aus tauschs auch auf die wirtschaftlichen Verflechtungen erstrecken. Auch aus diesem Grund begrüßt die DEK die aktuellen Reformüberlegungen zum Medienstaatsvertrag (MStV-E), der für Medienintermediäre ab einer gewissen Reichweite entsprechende Transparenzpflichten vorsieht.

## Zusammenfassung der wichtigsten Handlungsempfehlungen

### 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.

**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.

**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.

## 7. Der Einsatz algorithmischer Systeme durch staatliche Stellen

### 7.1 Chancen und Risiken beim Einsatz algorithmischer Systeme durch staatliche Stellen

Die Bürger erwarten zu Recht, dass der Staat **die beste verfügbare Technik nutzt**, um seine Aufgaben zu erledigen. Hierzu gehören, je nach Aufgabenbereich, auch algorithmische Systeme. Bereits heute existieren Systeme, die staatliche Stellen von repetitiven Tätigkeiten entlasten können – und die dadurch Verfahren beschleunigen und Kapazitäten für komplexe Fälle freisetzen –, die in bestimmten Konstellationen Einheitlichkeit und Qualität staatlichen Handelns verbessern oder die – etwa in Form von Chatbots oder Sprachassistenten – Bürgern den Zugang zum Recht erleichtern.

Zugleich müssen staatliche Stellen beim Einsatz von algorithmischen Systemen besonders hohe Standards wahren. Denn zum einen sind sie als Träger hoheitlicher Gewalt unmittelbar an die Grundrechte gebunden. Zum anderen kommt staatlichem Handeln generell eine **Modell- und Vorbildcharakter** für die gesamte Gesellschaft zu. Die institutionellen und Wissenskapazitäten, die der Staat zur Gewährleistung hinreichender Kontrolle der von Privaten eingesetzten algorithmischen Systeme aufbauen muss, müssen dementsprechend auch genutzt werden, um das Handeln der eigenen staatlichen Stellen anzuleiten und zu beaufsichtigen. Insbesondere dem von der DEK geforderten Kompetenzzentrums Algorithmische Systeme dürfte in diesem Zusammenhang eine Schlüsselrolle zukommen.

Der Einsatz algorithmischer Systeme durch staatliche Stellen muss **grundsätzlich als besonders sensibel** i.S.d. Kritikalitätspyramide (mindestens Stufe 3) gelten. Daher gehört aus Sicht der DEK eine umfassende Risikofolgenabschätzung zu den zwingenden Voraussetzungen jedes ethisch verantwortbaren Einsatzes algorithmischer Systeme. Darüber hinaus sind – je nach Kritikalität der staatlich genutzten Systeme – gegebenenfalls weitere der oben erörterten Instrumente zum Schutz der Bürger auch für hoheitlich genutzte algorithmische Systeme in Stellung zu bringen. Weitergehende datenschutzrechtliche Anforderungen bleiben davon ebenso wie sonstige verfassungs- und verwaltungsrechtliche Vorgaben für die Ausgestaltung der Systeme unberührt. Hinzu kommt, dass nach Auffassung der DEK in bestimmten Bereichen, in denen der Einsatz algorithmischer Systeme mit übergeordneten verfassungsrechtlichen Gütern kollidiert, die Nutzung algorithmischer Systeme unabhängig von im Einzelfall getroffenen Schutzmaßnahmen ausgeschlossen oder nur unter sehr restiktiven Bedingungen zulässig ist. Dies betrifft insbesondere den Einsatz algorithmischer Systeme für Zwecke der Rechtsetzung und der Rechtsprechung.

### 7.2 Algorithmische Systeme in der Rechtsetzung

Grenzen sind dem Einsatz algorithmischer Systeme im staatlichen Kontext bei der Rechtsetzung gezogen. Die DEK hält den demokratischen Prozess im Sinne einer möglichst freien Meinungs- und Willensbildung menschlicher Akteure für prinzipiell unantastbar. Automationsunterstützung in der Rechtsetzung ist daher **allenfalls für untergeordnete Hilfsaufgaben** (z.B. Aufdeckung begrifflicher Inkonsistenzen) bzw. **sehr weit von der demokratischen Willensbildung entfernte Rechtsakte** (z.B. Kataloge technischer Vorgaben in nachgelagerten Verordnungen) akzeptabel. In beiden Fällen sind höchste Anforderungen an die Qualität und Sicherheit der eingesetzten Systeme zu stellen.

Die DEK spricht sich in diesem Zusammenhang insbesondere auch gegen den Anspruch an neu erlassene Rechtsakte aus, diese müssten bereits im Hinblick auf eine mögliche künftige maschinelle Anwendung konzipiert werden; **die Technik hat auch insoweit dem Recht zu folgen, und nicht umgekehrt das Recht der Technik.** Allenfalls dann, wenn nach herkömmlichen Kriterien zur Bewertung von Gesetzgebung (Konformität mit Grundrechten und anderem höherrangigem Recht, Folgenabschätzung usw.) zwei gleichwertige Versionen denkbar sind, darf das Argument der leichteren Algorithmisierbarkeit einer Version den Ausschlag geben.

### 7.3 Algorithmische Systeme in der Rechtsprechung

Auch in der Rechtsprechung ist die Nutzung algorithmischer Systeme nach Auffassung der DEK **nur in Randbereichen** zulässig. Recht wird im „im Namen des Volkes“ und das heißt jedenfalls im streitigen Verfahren sowie in verwaltungsgerichtlichen und in Strafverfahren stets durch menschliche Richter gesprochen. Der Befriedungseffekt eines Gerichtsverfahrens wird nicht nur durch das Urteil selbst (Ergebnisgerechtigkeit), sondern auch durch die menschliche Anhörung und Abwägung widerstreitender Interessen und insbesondere die strukturelle Abarbeitung der Tatbestands- und Rechtsfolgenseite (Verfahrensgerechtigkeit) – im Unterschied zu einer intransparenten Black-Box-Entscheidung – erreicht.

Aufgrund des oftmals hohen Vertrauens in die vermeintliche „Unfehlbarkeit“ technischer Systeme („Automation Bias“) sowie der geringen Bereitschaft, abweichende Entscheidungen zu treffen, insbesondere wenn dies mit zusätzlicher Argumentations- und Beweislast sowie dem Risiko eines „Fehlurteils“ verbunden ist (sog. Default-Effekte), sind auch rechtlich unverbindliche Entscheidungsvorschläge für Urteile durch algorithmische Systeme aus Betroffenensicht in der Regel **hoch problematisch**.

Hilfreich können algorithmische Systeme dagegen – unter der Voraussetzung strenger Qualitätskontrolle und hoher Sicherheitsmaßstäbe – bei nicht unmittelbar die richterliche Entscheidung betreffenden **Vorbereitungsarbeiten** (z.B. Akten-Management, Dokumentkontrolle) sein.

Denkbar ist schließlich auch der Einsatz von Systemen, die **richterliche Entscheidungen retrospektiv analysieren**, ausschließlich der freiwilligen Nutzung durch Richter offenstehen und durch hohe Sicherheitsmaßnahmen vor einem Zugriff durch Dritte geschützt sind. Solche Systeme könnten z.B. herausarbeiten, ob und welche Entscheidungen durch externe Faktoren beeinflusst wurden, um Richtern künftig zur eigenen Verwendung Wege zur Vermeidung derartiger Verzerrungen zu unterbreiten und somit zu einer besseren und einheitlicheren Rechtsprechungspraxis beizutragen. Auch die Forschung kann ein legitimes Interesse am Zugang zu derartigen Systemen haben, wobei es hier hinreichender Sicherheitsgarantien im Einzelfall bedarf. Der Einsatz von Systemen zum Zweck der Kontrolle des Wegs zur richterlichen Entscheidungsfindung oder zum Abgleich der Spruchtätigkeit von Richtern mit externen Zielvorgaben (z.B. der durchschnittlichen Bearbeitungszeit für einen Fall) ist hingegen mit Blick auf die sachliche richterliche Unabhängigkeit unzulässig.

Im **vorgerichtlichen Bereich** (Beispiel: Geltendmachung von Fluggastrechten) oder auch im Mahnverfahren odgl. ist nach Ansicht der DEK eine vollautomatisierte Behandlung rechtlicher Ansprüche zulässig, sofern dadurch Verfahrensrechte einzelner Beteiligter gewahrt werden. Letzteres ist allerdings nicht gegeben, wenn algorithmische Systeme Korrelationen herstellen, die nicht den festgeschriebenen rechtlichen Vorgaben und Verfahrensschritten folgen. Beim jetzigen Stand der Technik kommen daher in der Regel ausschließlich auf klassischen deterministischen Algorithmen basierende Systeme in Betracht, die z.B. Entscheidungen über das Einhalten formaler (nicht wertungsoffener) Kriterien treffen. Aus systemischer Sicht drohende Kompetenzverluste werden hier durch das Freiwerden von Ressourcen für komplexe Einzelfälle ausgeglichen.



## 7.4 Algorithmische Systeme in der Verwaltung

In der Verwaltung ist tendenziell am ehesten Raum für den Einsatz algorithmischer Systeme. Eine verstärkte **Automatisierung behördlicher Routinefälle**, die sich unter präzise definierte Tatbestands- und Rechtsfolgevoraussetzungen subsumieren lassen, kann dabei im Sinne des Effizienzgebots (§ 10 S. 2 VwVfG) geboten sein, um Verwaltungsverfahren möglichst zweckmäßig und zügig durchzuführen. Insbesondere hier gilt, dass die Entlastung der Verwaltungsmitarbeiter von Routineaufgaben Ressourcen freisetzt. Diese können wiederum für die Bearbeitung nicht-automatisierbarer Verfahren eingesetzt werden.

Potentiale hierfür bestehen insbesondere in der **Leistungsverwaltung**. Dort können und sollten nach Auffassung der DEK algorithmische Systeme dazu genutzt werden, ein proaktives Verfahrensmanagement auszubauen, durch das bei Vorliegen aller erforderlichen Daten auf Seiten der Behörden Leistungen verstärkt antragslos gewährt. Hiervon könnten besonders bildungsferne und hilfebedürftige Menschen profitieren (vgl. die antragslose Familienbeihilfe in Österreich anlässlich der Geburt eines Kindes).

In der **Eingriffsverwaltung** ist der Einsatz algorithmischer Systeme hingegen wegen der besonderen Grundrechtsbetroffenheit vorsichtig zu handhaben. Dies gilt wie bei der gerichtlichen Nutzung nicht nur für algorithmendeterminierte Verwaltungsentscheidungen, sondern bereits dort, wo durch die Nutzung der Systeme der behördliche Entscheidungskorridor verengt wird. Allgemein sind bei der Beurteilung der Zulässigkeit des Einsatzes der Systeme die Tiefe des dadurch erfolgenden Eingriffs und die Reversibilität von Entscheidungen zu berücksichtigen. Grundsätzlich sind für die Gestaltung der Systeme die Technologien zu verwenden, die einer Kontrolle am ehesten zugänglich sind. Regelmäßig wird die Verwaltung daher in sensiblen Feldern allein auf klassischen deterministischen Algorithmen basierende Systeme verwenden dürfen. Aus demselben Grund sollte die Nutzung proprietärer Software vermieden werden.

Bei **Ermessensentscheidungen** der Exekutive und Entscheidungen mit einem Beurteilungsspielraum, die rechtliche Außenwirkung entfalten, hält es die DEK derzeit für geboten, dass Menschen die letzte Entscheidung treffen, sofern die Entscheidung nicht lediglich begünstigende Auswirkungen hat. Denkbar ist es allerdings, durch Bildung von Fallgruppen und weitere Konkretisierung das Ermessen so weit zu reduzieren, dass aus Sicht des algorithmischen Systems letztlich eine gebundene Entscheidung vorliegt. Aus Sicht der DEK bildet § 35a VwVfG die Vielzahl der hier möglichen Fallgestaltungen nicht hinreichend ab, sondern ist zu schematisch. Unter Beachtung der verfassungsrechtlich gebotenen sowie der aus Art. 22 DSGVO ableitbaren Sicherungsmechanismen sollte der Gesetzgeber daher den **Anwendungsbereich des § 35a VwVfG vorsichtig erweitern** bzw. im Fachrecht differenzierte Vorgaben für den teilweisen und vollständig automationsgestützten Erlass von Verwaltungsakten machen. Die Fortentwicklung der Regelungen zur Teil- und Voll-Automatisierung von Verwaltungsverfahren sollte mit den von der DEK empfohlenen horizontalen und sektoralen Regelungen für algorithmische Systeme (→ oben) erfolgen.

## 7.5 Algorithmische Systeme im Sicherheitsrecht

Besonders kritisch wird in der Öffentlichkeit der Einsatz algorithmischer Systeme durch die Sicherheitsbehörden diskutiert. Da administrative Maßnahmen in diesem Bereich besonders tief in Grundrechte eingreifen können, ist der Einsatz algorithmischer Systeme tendenziell **restriktiv** zu handhaben.

Werden algorithmische Systeme zur Vorhersage von Straftaten oder Gefährdungslagen genutzt (sog. **Predictive Policing**), ist zu berücksichtigen, dass auch solche Systeme, die unmittelbar keine personenbezogenen Daten nutzen, grundrechtsrelevante Effekte haben können. Dies ist insbesondere dann der Fall, wenn durch ggf. allzu detaillierte Ortsangaben ein Personenbezug (wieder-)hergestellt werden kann. Ferner kann es durch sog. lagebezogene Risikoprognosen zur übermäßigen Kontrolle bestimmter als sog. Hot Spots identifizierter Nachbarschaften und dadurch zu ethnischen oder sozialen Profilierungen dort ansässiger Bevölkerungsgruppen kommen. Ebenfalls können derartige Maßnahmen Kriminalitätsverlagerungs- und Verdrängungseffekte auslösen. Die DEK empfiehlt daher, die Sicherheitsbehörden für derartige Effekte zu sensibilisieren und in die Vorhersagesysteme Randomisierungen einzubauen, um entsprechende Effekte und sonstige systembedingte Verzerrungen zu reduzieren; zudem muss sichergestellt werden, dass den Sicherheitsbehörden eine menschliche Prüfung weiterer Fälle als der vom System ausgewählten Risikofälle stets möglich bleibt (vgl. § 88 AO). Die Sicherheitsbehörden dürfen zudem nicht allein auf der Basis lagebezogener Prognosen weitergehende ermessensbasierte Eingriffsmaßnahmen anordnen.

Soweit **personenbezogene Risikoprognosen** im Sicherheitsbereich rechtlich zulässig sind, dürfen solche Prognosen nicht vollautomatisiert erstellt werden, sofern sich an die Erstellung der Prognose negative Rechtsfolgen für den Betroffenen knüpfen. Aufgrund des Risikos eines „Automation Bias“ schon bei algorithmenbasierten Entscheidungen ist zudem die Unterstützung menschlicher Entscheidungsträger durch algorithmische Systeme bei derartigen Profilierungen allenfalls in sehr engen Grenzen zulässig.

## 7.6 Transparenzanforderungen beim Einsatz algorithmischer Systeme durch staatliche Akteure

Staatliche Entscheidungen, die unter Nutzung algorithmischer Systeme zu Stande kommen, müssen **transparent und begründbar** bleiben. Dies ist aufgrund der Grundrechtsbindung und der Notwendigkeit einer demokratischen Rückbindung aller hoheitlichen Gewalt im staatlichen Bereich tendenziell noch wichtiger als im privaten Sektor. Für staatliche Stellen gelten daher nicht nur die allgemeinen Transparenzanforderungen (→ oben). Vielmehr müssen sich staatliche Stellen darüber hinaus in besonderem Maße um Offenheit bemühen.

Die DEK weist darauf hin, dass hoheitliche algorithmische Systeme vielfach bereits in den Anwendungsbereich der bestehenden Informationsfreiheits- bzw. Transparenzgesetze fallen. Darüber hinaus begrüßt die DEK das im Rahmen der 36. Konferenz der Informationsfreiheitsbeauftragten in Deutschland verabschiedete Positionspapier zur „Transparenz der Verwaltung beim Einsatz von Algorithmen“, wonach öffentliche Stellen über aussagekräftige, umfassende und allgemein verständliche Informationen bezüglich der eigenen Datenverarbeitungen verfügen müssen und diese, soweit rechtlich möglich, veröffentlichten sollten, einschließlich Informationen (i) zu den Datenkategorien der Ein- und Ausgabedaten des Verfahrens, (ii) zur darin enthaltenen Logik, insbesondere zu den verwendeten Berechnungsformeln einschließlich der Gewichtung der Eingabedaten, zum zugrundeliegenden Fachwissen und zur individuellen Konfiguration durch die Anwendenden sowie (iii) zur Tragweite der darauf basierenden Entscheidungen sowie zu den möglichen Auswirkungen der Verfahren.<sup>17</sup>

17 Positionspapier im Rahmen der 36. Konferenz der Informationsfreiheitsbeauftragten in Deutschland – „Transparenz der Verwaltung beim Einsatz von Algorithmen für gelebten Grundrechtsschutz unabdingbar“, Ulm, 16. Oktober 2018 (abrufbar unter: [https://www.datenschutzzentrum.de/uploads/informationsfreiheit/2018\\_Positionspapier-Transparenz-von-Algorithmen.pdf](https://www.datenschutzzentrum.de/uploads/informationsfreiheit/2018_Positionspapier-Transparenz-von-Algorithmen.pdf)).



Bei der gesetzgeberischen Konkretisierung entsprechender Transparenzpflichten bzw. Informationszugangspflichten gibt die DEK zudem zu bedenken, dass unzureichende Vorgaben zur Transparenz zu Misstrauen in die Systeme führen kann, was sich in erhöhten Anfechtungsraten niederschlagen kann, die den durch den Einsatz algorithmischer Systeme intendierten Effizienzgewinn konterkarieren können. Aus diesem Grund hält es die DEK schließlich allenfalls in wenigen Fällen für vertretbar, den Informationszugang zu hoheitlichen algorithmischen Systemen unter Verweis auf ein Manipulationsrisiko oder auf den Schutz von Geschäftsgeheimnissen pauschal auszuschließen. Im Regelfall ist daher eine Abwägung vorzunehmen.

Informationen über die generelle Funktionsweise des Systems offenzulegen, reicht beim Einsatz algorithmischer Systeme durch Hoheitsträger nicht in jedem Fall aus. Regelmäßig müssen hoheitliche Entscheidungen den Betroffenen gegenüber auch begründet werden, d.h. es sind die „**wesentlichen tatsächlichen und rechtlichen Gründe**“, die die Entscheidung im Einzelfall motiviert haben, anzugeben (vgl. § 39 Abs.1 S.2 VwVfG). Wo eine solche einzelfallbezogene Erläuterung verfassungs- bzw. einfachrechtlich geboten, aber aufgrund der technischen Komplexität des Systems nicht bzw. nicht in einer Art und Weise möglich ist, die im Zuge eines behördlichen Beanstandungsverfahrens oder vor Gericht eine effektive Überprüfung der Tragfähigkeit der Begründung erlaubt, muss der Einsatz algorithmischer Systeme ausscheiden. Im Übrigen ist der Staat aus Sicht der DEK dazu aufgefordert, in der Verwaltung und an den Gerichten hinreichende **Expertise** aufzubauen, die eine entsprechende Kontrolle der systeminternen Entscheidungsprozesse gewährleisten kann.

Die DEK weist darauf hin, dass die Transparenz staatlichen Handelns auch dadurch beeinträchtigt werden kann, dass sich der Staat bei der Erfüllung seiner Tätigkeiten proprietärer Software (sog. Closed Source-Software) von privaten Anbietern bedient. Allgemein erschwert proprietäre Software Änderungen und Anpassungen durch den Benutzer, was ein Abhängigkeitsverhältnis entstehen lässt. Zudem führt die Nutzung proprietärer Software zu einem Mangel an Transparenz und kann damit die gesellschaftliche Akzeptanz der Systeme gefährden. Insbesondere in grundrechtssensiblen Bereichen wie dem Sicherheitsrecht sollte daher nach Möglichkeit auf proprietäre Software verzichtet werden. Stattdessen sollten staatliche Stellen auf **Open-Source-Lösungen** zurückgreifen oder – idealerweise in Form interdisziplinär besetzter Entwicklungsteams – eigene Systeme entwickeln. Wo dies nicht praktikabel ist, empfiehlt die DEK der Bundesregierung, Anpassungen im Vergaberecht zu prüfen, die die gerade beschriebenen negativen Effekte proprietärer Software minimieren. Wo nicht zu befürchten ist, dass durch Transparenz die Effektivität des Systems leidet, also Ausnutzungseffekte ausgeschlossen werden können, sollte die Software-Entwicklung in einem offenen und konsultativen Prozess unter Einbeziehung zivilgesellschaftlicher Akteure erfolgen.

## 7.7 Das Risiko eines automatisierten Totalvollzugs

Die DEK verwehrt sich zwar dagegen, dass es aus ethischer Sicht ein generelles Recht auf Freiheit zur Nichtbefolgung von Normen gebe. Allerdings bestehen gegen einen automatisierten Totalvollzug des Rechts eine Reihe ethischer Bedenken. So können sich Bürger durch eine perfektionierte Vollzugspraxis unter einen Generalverdacht gestellt sehen, unter dem der allgemeine Normbefolgungswille leitet. Ferner besteht beim automatisierten Vollzug die Gefahr, dass die Komplexität der Lebenswirklichkeit nicht hinreichend abgebildet und insbesondere unvorhergesehenen Ausnahmesituationen (Beispiel: Geschwindigkeitsüberschreitung bei Privattransport eines Schwerverletzten ins Krankenhaus) nicht genügend Rechnung getragen wird. Schließlich sind viele Gesetze ursprünglich nicht für einen Totalvollzug erlassen worden. Zu fordern ist daher regelmäßig ein technisches Design, bei dem der Mensch im Einzelfall den technischen Vollzug außer Kraft setzen kann. Zudem stellt sich jede Maßnahme der Rechtsdurchsetzung als eigener staatlicher Eingriff dar und hat sich als solcher am **Verhältnismäßigkeitsprinzip** zu orientieren.



# Zusammenfassung der wichtigsten Handlungsempfehlungen

## 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.

## 8. Haftung für algorithmische Systeme

### 8.1 Bedeutung

Strafrechtliche Verantwortlichkeit, Verwaltungssanktionen oder Haftung auf Schadensersatz sind unverzichtbarer Bestandteil eines ethisch vertretbaren Ordnungsrahmens, auch und gerade für algorithmische Systeme und andere digitale Technologien. Die DEK unterstreicht dabei aus ethischer Sicht insbesondere die Rolle des Schadensersatzrechts, welches sowohl der Kompensation als auch der Prävention von Schäden dient und damit ganz maßgeblich zu einem **grundrechtskonformen Rechtsgüterschutz** beiträgt.

Aus ethischer Sicht sind an ein Haftungssystem, welches neuen digitalen Technologien gerecht werden soll, u.a. die folgenden Anforderungen zu stellen:

- a) Ausreichende **Kompensation** für Geschädigte, insbesondere bei besonders grundrechtsrelevanten Rechtsgütern und soweit Kompensation in einer vergleichbaren Situation bei Einsatz von Menschen oder herkömmlicher Technologie geschuldet wäre;
- b) Setzen der richtigen **Verhaltensanreize**, indem Schäden von denjenigen Akteuren getragen werden, welche die Schäden durch vermeidbares und unerwünschtes Verhalten verursacht haben oder aus deren Sphäre das betreffende Risiko stammt;
- c) **Fairness**, indem diejenigen Akteure für Schäden aufkommen, welche das System etwa in den Verkehr gebracht haben oder welche die Kontrolle über das System ausüben und aus seinem Einsatz den Nutzen ziehen;
- d) **Effizienz**, indem Kosten von denjenigen Akteuren getragen (internalisiert) werden, die diese Kosten mit dem geringsten Aufwand vermeiden oder versichern können.

### 8.2 Schäden durch den Einsatz algorithmischer Systeme

#### 8.2.1 Haftung der „Elektronischen Person“?

Die DEK **rät ausdrücklich davon ab**, Robotern bzw. sog. autonomen Systemen Rechtspersönlichkeit zu verleihen (oft unter dem Stichwort „**E-Person**“ diskutiert) mit dem Ziel, die Systeme selbst haften zu lassen (z.B. ein autonom fahrendes Fahrzeug ohne Halter, das sich als Mobilitätsdienstleistung „selbst betreibt“). Eine solche Maßnahme wäre nicht geeignet, Verantwortlichkeit und Haftung für Schäden denjenigen Akteuren zuzuweisen, welche den Einsatz des Systems zu verantworten haben und letztlich von diesem Einsatz ökonomisch profitieren. Vielmehr könnte die Maßnahme im Gegenteil dazu genutzt werden, sich der Verantwortlichkeit zu entziehen. Durch die Rechtspersönlichkeit von Maschinen als eines neuen Typs juristischer Person ließe sich kein wünschenswertes Ergebnis erzielen, das nicht zwangsläufig auf andere Weise zu erzielen wäre (z.B. mithilfe des Gesellschaftsrechts). Autonom agierende Maschinen gar analog zu natürlichen Personen zu behandeln, wäre aus der Sicht der DEK eine gefährliche Verirrung.

#### 8.2.2 Gehilfenhaftung für „Autonome“ Systeme

Die DEK hält es allerdings für geboten, eine Zurechnung entsprechend den Regelungen über die Haftung für **Gehilfen** (vgl. insbes. § 278 BGB) bei sog. autonomen Systemen vorzunehmen. Ein Akteur, der sich zur Erweiterung seines Aktionsradius eines solchen Systems bedient (z.B. ein Krankenhaus bedient sich eines chirurgischen Roboters), sollte sich im Falle einer Fehlfunktion nicht exkulpieren können, da auch ein Akteur, der sich eines menschlichen Erfüllungsgehilfen (z.B. eines menschlichen Chirurgen) bedient, für das – als Verhalten des Akteurs selbst gedacht – schuldhafte Fehlverhalten dieses Gehilfen haftet. Dies erlangt besondere Bedeutung bei der **Haftung für algorithmische Systeme**, wo anderenfalls leicht Haftungslücken entstehen, wenn kein Sorgfaltspflichtverstoß der Hinterperson bei Einsatz und Überwachung des algorithmischen Systems nachgewiesen werden kann.



### Beispiele 18

*Ein chirurgischer Roboter in einem Krankenhaus verursacht einen zu langen Operationsschnitt mit Komplikationen. Oder: Durch ein algorithmisches System wird die Kreditwürdigkeit eines Bankkunden falsch abgeleitet und dieser kann das einmalig günstige Angebot einer Immobilie nicht annehmen.*

Dabei mag es vereinzelt schwierig sein, ein für Autonome Systeme adäquates Pendant zum „Sorgfaltsmaßstab“ zu ermitteln, v.a. sobald die Fähigkeiten einer Maschine diejenigen eines Menschen übersteigen. In der Mehrzahl der Fälle aber werden Fehlfunktionen von Normalfunktionen zu unterscheiden sein und daher kann dies nicht generell gegen die Haftung des Betreibers angeführt werden. Der Maßstab muss dann durch am Markt verfügbare vergleichbare Systeme bestimmt werden, wobei die Frage, der Einsatz welcher Technologie dem Betreiber zugemutet werden konnte, nach allgemeinen Grundsätzen zu entscheiden ist (z. B. unterscheidet sich insofern die Frage, welche Qualität von chirurgischem Roboter einzusetzen war, nicht von der Frage, welche Qualität von Röntgengerät einzusetzen war).

### 8.2.3 Gefährdungshaftung

Dass die Regeln der klassischen Verschuldenshaftung nicht immer ausreichen, um die rechtlichen Probleme, die bei gefährlichen Produkten auftreten, zu lösen, ist grundsätzlich bekannt. Die Rechtsordnung hat auf diese Herausforderung bislang eine Reihe von Antworten gefunden. Dazu gehören insbesondere:

- **Modifikation der Verschuldenshaftung** (z. B. durch Anpassungen des Sorgfaltsmaßstabs und diverse Beweiserleichterungen bis hin zur Beweislastumkehr);
- verschiedene Tatbestände der **Gefährdungshaftung** (d.h. für Anlagen und Tätigkeiten, die typischerweise Schäden verursachen, aufgrund ihres gesamtgesellschaftlichen Nutzens aber nicht verboten werden sollen); und

- die **Produkthaftung** nach dem ProdHaftG; diese stellt sich dabei als spezielle Form der verschuldensunabhängigen Haftung dar, die sich von der Gefährdungshaftung dadurch unterscheidet, dass sie u. a. einen Fehler des Produkts voraussetzt und sie dadurch der Verschuldenshaftung etwas angenähert wird.

Es muss sichergestellt sein, dass diese Antworten auch bei gefährlichen digitalen Anwendungen zu einer rechts-sicheren Kompensation von Schadensereignissen führen.

Gegenwärtig bestehen bei digitalen Anwendungen **Rechtsunsicherheiten und Haftungslücken**, die vor allem aus der Unvorhersehbarkeit von Schadensereignissen, u. a. beim Inverkehrbringen – und damit gegebenenfalls einem Versagen der klassischen Verschuldenshaftung – resultieren sowie daraus, dass durch das Zusammenwirken verschiedener Akteure und verschiedener Anwendungen in aller Regel kaum nachvollzogen werden kann, wo ein Fehler aufgetreten ist und/oder wo die Fehlerursache gesetzt wurde. Auch der offene und dynamische Charakter digitaler Ökosysteme und die enge funktionale Verknüpfung von Produkten, digitalen Inhalten und digitalen Dienstleistungen stellen eine Herausforderung dar. Diese Rechtsunsicherheiten sind aus Sicht von Unternehmen wie Verbrauchern **Hindernisse für Innovationen und für die Akzeptanz neuer Technologien**. Wenn Schadensereignisse regelmäßig nicht zugeordnet und kompensiert werden können, kann die durch Haftungsbestimmungen intendierte Marktwirkung nicht erzeugt werden. Um einen angemessenen Interessenausgleich herzustellen, muss der Gesetzgeber Transparenz und Verantwortung schaffen. Nur wenn die Verantwortlichkeiten geklärt sind, ist auch eine praxisgerechte Versicherbarkeit von Schäden möglich.

Die DEK kann den komplexen rechtstechnischen Fragen nach der richtigen Verortung einer haftungsrechtlichen Lösung nicht vorgreifen, zumal teilweise erst Chancen auf eine Lösung auf europäischer Ebene ausgelotet werden sollten. Aus ethischer Sicht ist entscheidend, dass **Rechtsklarheit und Rechtssicherheit, insbesondere in Bezug auf die oben beschriebenen Haftungsgrundsätze**, geschaffen wird. Dass neben einer sachgerechten Anpassung der Produkthaftungsrichtlinie (→ dazu [sogleich](#)) auch punktuelle Modifikationen der Verschuldenshaftung und/oder neue Tatbestände der Gefährdungshaftung erforderlich sein können, erscheint nach derzeitigem Stand der Diskussion jedoch sehr wahrscheinlich.

Im Gesetzgebungsprozess wird dabei zunächst zu klären sein, **für welche Produkte, digitalen Inhalte und digitalen Dienstleistungen** welches Haftungsregime sachgerecht und wie dieses konkret auszustalten ist, wobei es wesentlich wiederum auf die Kritikalität (→ oben) des betreffenden Systems ankommen wird, aber auch auf weitere, speziell im Haftungskontext relevante Kriterien. So kann eine Gefährdungshaftung (nach dem Modell etwa der Kfz-Halterhaftung) bei Geräten, deren Betriebsrisiko ähnlich unkontrollierbar ist und zu Schäden an Leib und Leben führen kann, durchaus angemessen sein. Dabei muss immer die Frage nach der Versicherbarkeit bzw. einer allfälligen Pflichtversicherung eine Rolle spielen. Stets wäre zugleich mitzuentcheiden, **für welche Schäden** gehaftet werden soll (z.B. Personen- und Sachschäden, Datenverlust, reine Vermögensschäden, immaterielle Schäden).

Schließlich wird jeweils zu entscheiden sein, wer unter Berücksichtigung der oben beschriebenen Haftungsgrundsätze der richtige **Adressat der Haftung** ist. Dabei zeichnen sich vor allem drei mögliche Haftungsadressaten ab, von denen gegebenenfalls auch jeweils zwei als Gesamtschuldner haften könnten:

- der individuelle **Halter** des Systems (d.h. der Eigentümer oder derjenige, der in einer ähnlichen Position das System für seine eigenen Zwecke einsetzt);
- der **Hersteller** des Systems;
- der **Betreiber** des Systems (d.h. je nachdem, wer das höhere Maß an Kontrolle über den Systembetrieb ausübt, der individuelle Halter als Frontend-Betreiber oder aber ein Backend-Betreiber, der mit dem Hersteller identisch sein kann, aber nicht sein muss).<sup>18</sup>

Eine Bestimmung des Adressaten und der Art der Haftung ist dabei stets abhängig von der konkreten Art des vernetzten oder Autonomen Systems und der Identifikation der konkreten Haftungssphären.

#### 8.2.4 Produktsicherheit und Produkthaftung

Insgesamt ist derzeit ein Paradigmenwechsel vom einmaligen Inverkehrbringen eines Produkts hin zum Inverkehrbringen eines Produkts und zusätzlicher, fortwährender Leistungserbringung für das Produkt zu verzeichnen. Daher kommt der laufenden **Produktbeobachtung** und **Produktpflege** eine gesteigerte Bedeutung zu. IT-Sicherheits- und Datenschutzstandards müssen nicht nur erfüllt sein, wenn ein Produkt das Werktor verlässt, sondern dürfen auch bei späteren Software-Updates nicht verloren gehen. Umgekehrt sollte den Hersteller bei später auftretenden Sicherheitslücken – entsprechend der Regelungen in den Richtlinien zu digitalen Inhalten und digitalen Dienstleistungen sowie zum Warenhandel – im Rahmen der berechtigten Verbrauchererwartungen zur Nutzungsdauer eine Pflicht zu **Sicherheitsupdates** treffen.

<sup>18</sup> Zum Haftungskonzept einer derart differenzierten Betreiberhaftung in digitalen Ökosystemen siehe den Bericht „Liability for Artificial Intelligence and other emerging digital technologies“ der von der Europäischen Kommission eingesetzten Expert Group on Liability and New Technologies (New Technologies Formation), vsl. Oktober 2019 (im Erscheinen), Nr. [11], S. 41 ff.

**Beispiel 19**

*Für eine intelligente Hausanlage werden keine Sicherheitsupdates angeboten, weshalb es nach einem Cyberangriff zu einem Wohnungseinbruch kommt.*

Die aus den 1980er Jahren stammende Produkthaftungsrichtlinie konnte die Charakteristiken vernetzter, hybrider und autonomer Produkte noch nicht einbeziehen. Die DEK empfiehlt der Bundesregierung, bei der **Evaluierung und Überarbeitung der Produkthaftungsrichtlinie** auf europäischer Ebene auf rechtssichere und rechtsklare Regelungen insbesondere für folgende Aspekte zu dringen:

- a) das Unterfallen digitaler Inhalte und digitaler Dienstleistungen, wie etwa auch algorithmische Systeme, unter den Produktbegriff;
- b) die Haftung für Produktfehler, die erst nach dem Inverkehrbringen infolge sich selbst verändernder Software, erfolgter oder pflichtwidrig unterlassener Updates, oder produktspezifischer Daten auftreten;
- c) die Haftung für Verletzungen der Produktbeobachtungspflicht;
- d) die Einbeziehung typischerweise von digitaler Produktsicherheit betroffener Rechtsgüter, insbesondere die Verletzung des informationellen Selbstbestimmungsrechts, im Rahmen von Schadensersatzregelungen;
- e) die Anpassung der Einwendung des Entwicklungsrisikos.

### 8.3 Bedarf nach einer Neubewertung des Haftungsrechts

Digitale Ökosysteme werfen eine Vielzahl weiterer Probleme im Zusammenhang mit Haftung und Verantwortlichkeit auf. So besteht teilweise eine Haftungslücke im geltenden Deliktsrecht bei **Schäden an Daten und digitalen Gütern**, soweit weder ein anerkanntes absolut geschütztes Rechtsgut verletzt ist (z.B. Eigentum am Speichermedium) noch ein existierendes Schutzgesetz verletzt wurde (z.B. Normen des Strafrechts) noch die Voraussetzungen vorsätzlicher sittenwidriger Schädigung vorliegen. Neue digitale Technologien gehen auch vielfach mit der **opportunistischen Nutzung fremder Infrastrukturen** einher (z.B. indem von privaten IoT-Geräten generierte Sensordaten von Dritten systematisch gesammelt und verwertet werden, oder auch durch unmittelbare Nutzung von Rechenkapazität oder Sendefunktionen), was schwierige Haftungsfragen aufwerfen kann. In stärker vertragsrechtlich geprägten Zusammenhängen können immense Schäden – insbesondere zulasten von Verbrauchern – dadurch verursacht werden, dass die **Nutzbarkeit von hochwertigen Gütern** (Immobilien, Maschinen, Kraftfahrzeuge usw.) immer mehr von der langfristigen Erbringung digitaler Dienste abhängig ist (Software-Updates, Nutzerkonten u.a.) und die Erbringung dieser Dienste nicht gesichert ist bzw. sogar gezielt unterbrochen werden kann, um Einzelne unter Druck zu setzen (**Electronic Repossession**).

Auch sind digitale Ökosysteme teilweise durch das Zusammenwirken zahlreicher Komponenten und Betreiber gekennzeichnet, wobei es für den Geschädigten vielfach unverhältnismäßig schwierig ist, nachzuweisen, **welcher von mehreren potenziellen Schädigern** (z.B. Hardware-Lieferant, Lieferanten mehrerer Software-Komponenten, Lieferant von Daten-Feeds oder Netzwerkbetreiber) einen Schaden verursacht hat. Andererseits schaffen digitale Technologien nicht nur neue Intransparenzen in Bezug auf die Schadensverursachung, sondern können umgekehrt auch dazu beitragen, Kausalverläufe in nie da gewesener Weise zu dokumentieren. Es stellt sich daher die Frage, welchen Akteur welche Verpflichtung trifft, durch **Logging von Daten** bereits ex ante zur Aufklärung der Schadensverursachung beizutragen und wem die tatsächlich durch Logging aufgezeichneten Daten im Schadensfall offenzulegen sind.

Die DEK empfiehlt daher der Bundesregierung insgesamt, zu prüfen, inwieweit das geltende Haftungsrecht den **Herausforderungen digitaler Ökosysteme** gewachsen ist oder einer Überarbeitung bedarf. Dabei ist vorrangig eine Lösung auf europäischer Ebene anzustreben. Die DEK warnt in diesem Zusammenhang vor einer Tendenz, den Blick einseitig auf bestimmte technologische Merkmale, insbesondere das Merkmal maschinellen Lernens, zu richten. Während maschinelles Lernen bestimmte zusätzliche Gefahren schafft und bestimmte zusätzliche Zurechnungsprobleme mit sich bringt, sind die meisten Herausforderungen für das Haftungsrecht durch andere Faktoren (z. B. Unkörperlichkeit, Zusammenwirken vieler Komponenten, Vernetzung, Dezentralisierung) bedingt.



# Zusammenfassung der wichtigsten Handlungsempfehlungen

## 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 auszustalten 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.

Teil G

# Für einen europäischen Weg



Die Fülle an Fragen, die sich der Datenethikkommission gestellt haben und deren Diskussion jeweils wieder neue Fragen aufwarf, lässt deutlich werden, dass dieses Gutachten lediglich einen weiteren Grundstein für einen **Zukunftsdiskurs über Ethik, Recht und Technologie** legen kann, der immer weiter und auf breiter Basis geführt werden muss. Dieser Diskurs muss von vornehmlich interdisziplinärer sein und ein breites Spektrum an Wissenschaften ebenso wie eine Vielfalt von Vertretern aus Wirtschaft, Zivilgesellschaft und Politik umfassen. Angesichts des hohen ökonomischen Drucks und der Geschwindigkeit des technischen Wandels müssen die Ergebnisse dieses Diskurses auf unterschiedlichen Ebenen kontinuierlich von allen beteiligten Akteuren umgesetzt werden, damit eine wertefundierte Gestaltung der technologisch geprägten Zukunft gewährleistet werden kann.

In Anbetracht des Umstandes, dass der Transfer von Daten und die Anwendung algorithmischer Systeme vor nationalen Grenzen keinen Halt machen, kann eine vorausschauende Erörterung ethischer und rechtlicher Fragen zu Daten und algorithmischen Systemen nicht allein auf nationaler Ebene erfolgen. Wir brauchen einen **globalen Blick** auf die Probleme und müssen – vice versa – auch bestrebt sein, unsere Erkenntnisse und Herangehensweisen stärker als bisher in die außereuropäische Debatte einzubringen. Die Erfahrung mit der Umsetzung der DSGVO zeigt, dass die ökonomische Macht des europäischen Wirtschaftsraumes und seine Bedeutung als Absatzmarkt für Betreiber und Anbieter algorithmischer Systeme dazu führen können, dass letztere europäische Rahmenbedingungen bei der Entwicklung und Umsetzung ihrer Produkte und Dienstleistungen aus wirtschaftlichen Interessen heraus berücksichtigen. Zudem dienen europäische Rahmenbedingungen zunehmend auch außereuropäischen Regierungen zur Orientierung bei der Gestaltung ihres eigenen Ordnungsrahmens.

Deswegen sollte der erforderliche Diskussionsprozess insbesondere auch Schwerpunktthema internationaler Foren wie EU, OECD, Europarat, Vereinte Nationen, G7 und G20 sein. Vor diesem Hintergrund empfiehlt die DEK der Bundesregierung, sich aktiv in die entsprechenden internationalen Gremien einzubringen. Insbesondere die **deutsche Ratspräsidentschaft** in der zweiten Jahreshälfte 2020 sollte dazu genutzt werden, die in diesem Gutachten vorgeschlagenen Maßnahmen zur Regulierung des Umgangs mit Daten und algorithmischen Systemen auf europäischer Ebene voranzutreiben. Außerdem plädiert die DEK für eine frühzeitige Mitgestaltung des auf G7-Ebene initiierten Prozesses der Einrichtung eines International Panel on Artificial Intelligence (IPAI) sowie für eine kontinuierliche, aktive Teilnahme der Bundesregierung.

Deutschland und Europa sehen sich im globalen Wettlauf um die Entwicklung von Zukunftstechnologien mit Wertesystemen, Gesellschaftsmodellen und Kulturen konfrontiert, die sich von unseren unterscheiden. Dies hat zu einer Debatte geführt, ob Deutschland und Europa sich an das eine oder andere außereuropäische Modell anpassen müssen, um wettbewerbsfähig zu bleiben. Die DEK unterstützt den bislang eingeschlagenen „**europäischen Weg**“ (in der Debatte oft auch als „dritter Weg“ zwischen den Strategien der USA und Chinas bezeichnet), wonach sich europäische Technologien 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 sollten.

Um im Zukunftsdiskurs über das Zusammenspiel von Ethik, Recht und Technologie handlungsfähig zu bleiben, muss die digitale Souveränität Deutschlands und Europas weitestmöglich gewährleistet sein. Digitale Souveränität von Staaten oder Organisationen umfasst das gesamte Feld der Verarbeitung von Daten, das heißt die Kontrolle über die Speicherung, Übertragung und Verwendung ihrer schutzwürdigen Daten inklusive der unabhängigen Entscheidung darüber, wer darauf zugreifen darf. Da grenzüberschreitende Datenflüsse für ein globalisiertes Miteinander von Menschen, Staaten und Unternehmen erforderlich sind und das Internet als Basis für solche Datenflüsse ein globales „Netz der Netze“ ist, macht die verteilte weltweite Struktur, die sehr unterschiedliche Rechts- und Gesellschaftssysteme umfasst, eine vollständige Souveränität unmöglich. Damit betrifft digitale Souveränität ganz zentral Fragen der technischen Infrastruktur einschließlich der Hardware, der Netze, der Steuerungskomponenten, wie Router oder Adress-Server, und der Datenzentren. Gerade in Anbetracht der großen Abhängigkeit von ausländischen Produkten sieht die DEK erheblichen Handlungsbedarf auf deutscher und europäischer Ebene durch **Investitionen in die Entwicklung und Sicherung entsprechender Technologien und Infrastrukturen**, um die digitale Souveränität Deutschlands und Europas zu gewährleisten.

Da in Deutschland und sogar europaweit derzeit die wichtigsten der eingesetzten Basiskomponenten für die Internetinfrastruktur fast ausschließlich von Unternehmen aus anderen Kontinenten bezogen werden können, kann sich der Souveränitätsanspruch derzeit nur auf die Fähigkeit beschränken, die verwendeten Basiskomponenten zunächst kritisch zu analysieren und zu bewerten und dann möglichst sicher zu betreiben, um die Gefahr der missbräuchlichen Nutzung durch fremde Staaten und Organisationen zu minimieren. Perspektivisch aber hält es die DEK für bedeutsam, dass Deutschland und Europa ein **höheres Maß an digitaler Souveränität auch in der technischen Infrastruktur** entwickeln. Forschung und Entwicklung von möglichst sicheren Systemen sollten unterstützt werden. Dies umfasst sowohl neu gestaltete Komponenten, um bisherige Systeme zu ersetzen, als auch Ansätze, um auf Basis vorhandener Komponenten trotz bekannter oder vermuteter Unzulänglichkeiten oder Sicherheitsrisiken zu Gesamtlösungen zu kommen, die dem Schutzbedarf angemessen sind.

Digitale Souveränität eines Staates ist allerdings nicht nur im Verhältnis zu anderen Staaten zu sehen, sondern auch im Verhältnis zu nicht-staatlichen Machtzentren. Mit der Entwicklung der Datenwirtschaft gehen **ökonomische Konzentrationstendenzen** einher, die das **Entstehen neuer Machtungleichgewichte** beobachten lassen. Die Forschungs- und Entwicklungsbedingungen im Bereich algorithmischer Systeme und anderer digitaler Technologien werden zunehmend von einigen wenigen großen Digitalunternehmen bestimmt, die häufig auch noch zu wichtigen Finanzquellen für öffentliche Forschung werden und diese mitprägen. Auch die meinungsbildende Funktion von Intermediären und ihr damit verbundener Einfluss auf den gesellschaftspolitischen Diskurs wuchs in den vergangenen Jahrzehnten – ebenso wie die damit verbundene Missbrauchsgefahr – stetig an. Die DEK hält es auf der Grundlage der ethischen und rechtlichen Grundwerte und -freiheiten sowie mit Blick auf die digitale Souveränität Deutschlands und Europas für dringend geboten, die Verschiebung solcher Machtverhältnisse, die für das Funktionieren eines demokratischen Staates und einer sozialen Marktwirtschaft von zentraler Bedeutung sind, umfassend zu beobachten und in den einschlägigen Bereichen wirkungsvoll zu regulieren.

Wer von anderen übermäßig abhängig ist, wird vom „rule maker“ zum „rule taker“ und setzt seine Bürgerinnen und Bürger letztlich Vorgaben aus, die von Akteuren aus anderen Regionen der Welt formuliert werden. Bemühungen um die **langfristige Sicherung der digitalen Souveränität** sind daher nicht nur ein Gebot politischer Weitsicht, sondern auch Ausdruck ethischer Verantwortung.





# Anhang



# 1. Leitfragen der Bundesregierung an die Datenethikkommission

## Koalitionsvertrag:

„Wir werden zeitnah eine Daten-Ethikkommission einsetzen, die Regierung und Parlament innerhalb eines Jahres einen Entwicklungsrahmen für Datenpolitik, den Umgang mit Algorithmen, künstlicher Intelligenz und digitalen Innovationen vorschlägt. Die Klärung datenethischer Fragen kann Geschwindigkeit in die digitale Entwicklung bringen und auch einen Weg definieren, der gesellschaftliche Konflikte im Bereich der Datenpolitik auflöst.“

## Leitfragen an die Datenethikkommission:

Die Digitalisierung verändert unsere Gesellschaft grundlegend. Neuartige datenbasierte Technologien können zu einem Nutzen für den Alltag des Einzelnen, für Wirtschaft, für Umwelt und Wissenschaft und für die Gesellschaft als Ganzes führen und bergen große Potentiale.

Gleichzeitig werden auch die Risiken der Digitalisierung wahrgenommen. Es stellen sich zahlreiche ethische und rechtliche Fragen, in deren Mittelpunkt die Auswirkungen dieser Entwicklungen und die gewünschte Rolle der neuen Technologien stehen. Wenn der digitale Wandel zum Wohl der gesamten Gesellschaft führen soll, müssen wir uns mit möglichen Folgen der neuen Technologien befassen und ethische Leitplanken definieren.

Eine Herausforderung besteht darin, das Recht für das 21. Jahrhundert so fortzuentwickeln, dass die Menschewürde („ein Mensch darf nicht zum bloßen Objekt werden“) gewahrt bleibt und Grund- und Menschenrechte wie das allgemeine Persönlichkeitsrecht, die Privatsphäre, das Recht auf informationelle Selbstbestimmung, die Diskriminierungsfreiheit, die Wissenschaftsfreiheit, die unternehmerische Freiheit und die Meinungs- und Informationsfreiheit garantiert und zu einem Ausgleich gebracht werden. Dabei bestehen vielfältige Spannungsverhältnisse zwischen Gemeinwohlorientierung, Fortschritt, Innovation und Solidarprinzip.

Diese Kommission soll – unter Berücksichtigung des Diskussions- und Regelungsstandes auf europäischer und internationaler Ebene, nationaler Gestaltungsmöglichkeiten und besonderer Berücksichtigung sensibler Bereiche – ethische Maßstäbe und Leitlinien für den Schutz des Einzelnen, die Wahrung des gesellschaftlichen Zusammenlebens und die Sicherung und Förderung des Wohlstands im Informationszeitalter entwickeln. Die Kommission soll der Bundesregierung auch Empfehlungen oder Regulierungsoptionen vorschlagen, wie die ethischen Leitlinien entwickelt, beachtet, implementiert und beaufsichtigt werden können. Die Vorschläge sollen jeweils auch eine Beschreibung des zugrunde gelegten Begriffsverständnisses und Einschätzungen zu möglichen Folge- und Nebenwirkungen umfassen.

Die Öffentlichkeit soll in geeigneter Weise an der Arbeit der Kommission teilhaben können.

Für ihre Arbeit gibt die Bundesregierung der Datenethikkommission Leitfragen in drei Bereichen zur Hand:

### I. Algorithmenbasierte Prognose- und Entscheidungsprozesse („algorithmic decision making“ = ADM)

Fortgeschrittene Automatisierungssysteme prägen in immer stärkerem Maße das wirtschaftliche und gesellschaftliche Leben und den Alltag des Einzelnen. Datenerfassung und -analyse ermöglichen die Entwicklung neuartiger Deutungsmodelle, die auch dazu genutzt werden, algorithmenbasierte Entscheidungen zu treffen oder vorzubereiten. Algorithmen ermöglichen es beispielsweise, Verhaltensmuster und Unterschiede im Verhalten verschiedener Gruppen zu erkennen. Ob bei der individuellen Preisgestaltung im Onlinehandel, der Einschätzung der Kreditwürdigkeit oder der Bewerberauswahl bei Einstellungsverfahren: Menschen werden in immer mehr Lebensbereichen von technischen Verfahren bewertet. Die Datenauswertung und die Prognosen über individuelles Verhalten können Chancen bieten (z.B. für die Forschung, die Innovationsfähigkeit der Wirtschaft, die Effizienzsteigerung von Datenverarbeitungsprozessen), bergen aber auch Risiken (z.B. für die individuelle Handlungsfreiheit und Selbstbestimmung, Teilhabe und Chancengleichheit einzelner Menschen wie gesellschaftlicher Gruppen). Gesellschaftliche Ungleichheit und Diskriminierung von Individuen oder Personengruppen kann fortgeschrieben werden, wenn in die Programmierung des Algorithmus oder seine Trainingsdaten tendenziöse Vorfestlegungen („biases“) oder Diskriminierungen eingeflossen sind. Diese Risiken bestehen vor allem bei teilhaberelevanten und persönlichkeitsensiblen ADM-Prozessen. Vor diesem Hintergrund stellen sich insbesondere mit Blick auf den Schutz von Verbraucherinnen und Verbrauchern folgende Fragen:

- Welche ethischen Grenzen gibt es für den Einsatz von ADM-Prozessen bzw. sollte es geben?
- Kann es ethisch geboten sein, ADM-Prozesse einzusetzen?
- Gibt es Merkmale, Kriterien oder Datenpunkte, die – beispielsweise aufgrund ihres Alters oder ihrer Herkunft – nicht in ADM-Prozesse einfließen sollten?

- Wie kann ermittelt werden, welche Vorurteile und Verzerrungen in welchen Bereichen ethisch unerwünscht sind? Welche Auswirkungen kann der Einsatz von ADM-Prozessen auf gesellschaftliche Gruppen haben?
- Welche Regulierungsansätze sind denkbar, um Manipulationen, Ungleichbehandlung und Diskriminierung zu verhindern?
- Empfiehlt sich ein abgestufter Regulierungsrahmen abhängig vom Risiko für soziale Teilhabe bzw. dem Diskriminierungspotential?
- Wie kann Verlässlichkeit, Reproduzierbarkeit und Überprüfbarkeit von ADM gewährleistet werden?
- Gibt es Grenzen des Einsatzes von ADM, wenn Einsatz und Kriterien den betroffenen Menschen nicht erklärt werden können?
- Sind Testmethoden möglich, die selbstlernende ADM überprüfbar machen?

### II. Künstliche Intelligenz (KI)

Mit der Entwicklung von KI werden in Industrie und Verwaltung immer mehr Systeme mit einem hohen Grad an Automatisierung eingesetzt, die Methoden der KI verwenden und etwa über die Fähigkeit verfügen, durch den Einsatz von Trainingsdaten zu „lernen“. Darüber hinaus wird an einer Nachbildung der kognitiven Funktionen im menschlichen Gehirn gearbeitet. Die Entwicklungen im Bereich Künstliche Intelligenz werfen die Frage auf, wie die Würde, die Autonomie und die Selbstbestimmung des Einzelnen gewahrt bleiben und gefördert werden kann. In dem Zusammenhang stellen sich unter anderem folgende Fragen:

- Welche ethischen Grundprinzipien müssen bei der Entwicklung, Programmierung und Nutzung von KI eingehalten werden?

- Wo verlaufen ethische Grenzen für den Einsatz von KI und Robotern, insbesondere in besonderen Lebensbereichen wie Pflege und Betreuung und bei besonders schutzbedürftigen Gruppen (Kinder, ältere Menschen, Menschen mit Behinderungen)? Kann es ethisch geboten sein, KI einzusetzen?
- Kann es bei KI „Ethics by Design“ geben? Wenn ja, wie ließe sie sich implementieren und kontrollieren?
- Wie kann sichergestellt werden, dass Maschinen, die auf KI-Basis arbeiten, kontrollierbar sind?
- Wem sind die mit KI generierten Schöpfungen/Erfindungen zuzuordnen? Wer sollte die Verantwortung für fehlerhaft arbeitende Systeme tragen? Wie kann die Verantwortlichkeit der an der Entwicklung und am Einsatz von KISystemen beteiligten Akteure (Programmierer, Datenwissenschaftler, Auftraggeber, usw.) transparent gemacht?
- Was wird darüber hinaus zukünftig nötig sein, um die für unsere Gesellschaft konstitutiven Freiheiten und Grundrechte nachhaltig zu gewährleisten?

### III. Daten

Die Digitalisierung ist gekennzeichnet durch eine Zunahme der Datenmenge (Big Data), durch eine enorme Datenakkumulation bei einzelnen Akteuren, durch die Geschwindigkeit der Datenverarbeitung (Echtzeit), durch Vernetzung (Internet, komplexe Akteursnetzwerke, Internet der Dinge), durch zunehmende Ubiquität und Permanenz von Daten und durch die Weiterentwicklung verschiedener Methoden der Datenanalyse. Dabei steigt mit der Menge der verfügbaren Daten auch die Möglichkeit von immer granulareren Analysen. Durch Daten werden neue Geschäftsmodelle entwickelt und Wertschöpfungsketten sowie Arbeitsprozesse verändert. Daten werden zum Teil als Wirtschaftsgut angesehen, das Wertschöpfung ermöglicht („Datenwirtschaft“).

Sowohl auf nationaler als auch auf europäischer Ebene gibt es geltendes Recht (u. a. Datenschutz-Grundverordnung, Open Data) und zahlreiche gesetzgeberische Initiativen, die den Umgang mit Daten betreffen (u. a. e-Privacy-Verordnung, Free Flow of Data). Sie sollen einerseits Grundrechte wie das Recht auf informationelle Selbstbestimmung wahren und andererseits in diesem Rahmen nützliche und innovative Datenverarbeitungen ermöglichen. Diskutiert werden weitere Vorschläge, ob und wie der Zugang zu Daten, die Nutzung von Daten, der Handel mit Daten und Rechte an Daten erstmals oder besser reguliert werden könnten.

Dabei können sich folgende Fragen zum Umgang mit Daten allgemein, zum Datenzugang und zur Datennutzung stellen:

- Welche ethischen Grenzen der Ökonomisierung von Daten gibt es?
- Wer darf den ökonomischen Nutzen aus Daten ziehen?
- Sollte es eine Pflicht zum Angebot von Bezahlmodellen geben?
- Sind einheitliche Regelungen, die für alle Daten gleichermaßen gelten, empfehlenswert? Oder sollten bereichsspezifische Regelungen (z. B. für Gehirndaten) bevorzugt werden? Was sollte der Anknüpfungspunkt für bereichsspezifische Regelungen sein?
- Welche Folgen haben bestehende Zugriffs- und Ausschließlichkeitsrechte an Daten für Wettbewerb und Innovation und welche Folgen hätten zusätzliche Zugriffs- und Ausschließlichkeitsrechte an Daten?
- Bedarf es staatlicher Angebote als Teil der Daseinsvorsorge, damit die Bürgerinnen und Bürger sich verantwortlich, kompetent und souverän im Internet und in den sozialen Netzwerken bewegen können und den Umgang mit Daten beherrschen? Kann die Bereitstellung von Daten, insbesondere offener Daten, ein Teil der staatlichen Daseinsvorsorge werden?

- Wieviel Transparenz ist notwendig und angemessen, um das Recht auf informationelle Selbstbestimmung zu wahren und Bürgerinnen und Bürgern eine selbstbestimmte Teilhabe am Wirtschaftsleben zu ermöglichen?
- Erfordern besondere Lebenslagen spezielle Schutzkonzepte für einzelne Nutzergruppen?
- Sind die bestehenden Institutionen in sensiblen Bereichen ausreichend, um eine ethisch vertretbare Nutzung von Daten sicherzustellen? Wie kann eine ausreichende Vertretung der jeweiligen Stakeholder nachhaltig sichergestellt werden?
- Welche Auswirkungen können umfassende Datensammlungen auf das Funktionieren der Marktwirtschaft (z.B. Wettbewerbsfähigkeit, Informationsasymmetrie zwischen Anbietern und Verbrauchern, Möglichkeit, innovative Produkte zu entwickeln) und der Demokratie (z.B. Erfassung und Auswertung des Verhaltens in sozialen Netzwerken) haben? Wie kann erforderlichenfalls gegen Datenmacht/Datensilos (insbesondere Intermediäre) vorgegangen werden?
- Sollten Daten oder der Zugang zu ihnen in bestimmten Fällen zum Allgemeingut erklärt werden? In welchen Fällen und unter welchen ethischen Kriterien?
- Die Nutzung von nicht-personenbezogenen Daten kann kollektive Wirkungen haben. So können zum Beispiel Einzelne oder bestimmte Bevölkerungsgruppen schlechter gestellt werden, weil die Datenanalyse ergibt, dass in einem bestimmten Stadtviertel die Zahlungsmoral geringer ist. Welche Regelungsinstrumente wären hierfür notwendig? In welchen Sektoren?
- Ist eine gesetzliche Regelung zur Verbesserung des Zugangs zu Daten möglich, erforderlich und sinnvoll?
- Muss es aus ethischen Gründen Datenverarbeitungsverbote geben, etwa bei bestimmten Datenarten (z.B. politische Einstellung; Gehirndaten) oder bestimmten Verwendungsbereichen (z.B. Profiling für politische Zwecke oder zur Verwendung bei Wahlen)?
- Unter welchen Voraussetzungen kann es eine ethische Pflicht zur Datennutzung geben?
- Wird ein möglicher Gemeinwohlnutzen der Datenverarbeitung von der Rechtsordnung in hinreichender Weise anerkannt? Wenn nein, wie kann dies erreicht werden?
- Ist es möglich und sinnvoll, Experimentierklauseln zur Erprobung neuer Anwendungen oder neuer Regulierungsinstrumente zu schaffen?
- Ist es sinnvoll, in Dateninfrastrukturen zu investieren? Wenn ja, in welche?
- Wie können die grundrechtlich geschützten Interessen des Einzelnen, der Unternehmen, der Wissenschaft und Kunst und das Gemeinwohlinteresse an der Datennutzung in Einklang gebracht werden?

## 2. 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



#### **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



#### **Marit Hansen**

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



#### **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

# 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](mailto:datenethikkommission_gs@bmi.bund.de)  
[datenethikkommission\\_gs@bmjv.bund.de](mailto:datenethikkommission_gs@bmjv.bund.de)

## Internet

[www.datenethikkommission.de](http://www.datenethikkommission.de)

## Gestaltung

Atelier Hauer + Dörfler GmbH, Berlin

## Bildnachweis

S. 53 shutterstock.com;  
S. 234: BMI (Gruppenfoto), Studio Wilke (Christiane Wendehorst), Reiner Zensen (Christiane Woopen), BPA/Kugler (Ulrich Kelber);  
S. 235: Christian Kruppa (Dieter Kempf), vzbv/Gert Baumbach (Klaus Müller), Markus Mielek (Sabine Sachweh), TH Köln/Schmülggen (Rolf Schwartmann), UHH/Nicolai (Judith Simon), Jim Rakete (Wolfgang Wahlster)

## Druck

Brandenburgische Universitätsdruckerei und Verlags-  
gesellschaft Potsdam mbH (bud)

© DEK 2019

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







