abida
ASSESSING BIG DATA

Big Data im Gesundheitsbereich

GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

01IS15016A-F

Dr. Thilo Weichert

ABIDA - ASSESSING BIG DATA

PROJEKTLAUFZEIT 01.03.2015-28.02.2019

Westfälische Wilhelms-Universität Münster,
Institut für Informations-, Telekommunikations- und
Medienrecht (ITM), Zivilrechtliche Abteilung

Karlsruher Institut für Technologie,
Institut für Technikfolgenabschätzung
und Systemanalyse (ITAS)

Leibniz Universität Hannover
Institut für Rechtsinformatik
(IRI)

Technische Universität Dortmund,
Wirtschafts- und Sozialwissenschaftliche
Fakultät (WiSo) Techniksoziologie

Ludwig-Maximilians-Universität München,
Forschungsstelle für Information, Organisation
und Management (IOM)

Wissenschaftszentrum
Berlin für Sozialforschung

ABIDA - Assessing Big Data
Über das Gutachten

Das Gutachten wurde im Rahmen des ABIDA-Projekts mit Mitteln des Bundesministeriums für Bildung und Forschung erstellt. Der Inhalt des Gutachtens gibt ausschließlich die Auffassung des Autors wieder. Diese deckt sich nicht automatisch mit denen des Ministeriums und/oder der einzelnen Projektpartner.

ABIDA lotet gesellschaftliche Chancen und Risiken der Erzeugung, Verknüpfung und Auswertung großer Datenmengen aus und entwirft Handlungsoptionen für Politik, Forschung und Entwicklung.

www.abida.de
© 2018 – Alle Rechte vorbehalten

INHALT

1 Einleitung – Fragestellung, Methode

Das vorliegende Gutachten zu „Big Data im Gesundheitsbereich“ wurde erstellt im Rahmen des vom Bundesministerium für Bildung und Forschung (BMBF) geförderten Projektes „Assessing Big Data“ (ABIDA).

Das vorliegende Gutachten thematisiert schwerpunktmäßig die massenhafte Erfassung, Speicherung und Auswertung von Gesundheitsdaten, wodurch sich zwangsläufig inhaltliche Querbezüge zu den weiteren Gutachten, die im Rahmen von ABIDA erstellt werden, ergeben.

1.1 Thematischer Hintergrund

In der Leistungsbeschreibung zum vorliegenden Gutachten heißt es über den thematischen Hintergrund: „Gesundheitsdaten gehören mit zu den persönlichsten Daten, die es gibt. Zu den Zielen von Big Data im Gesundheitswesen gehört es, neben der Erzeugung von Daten bspw. in der Genomanalyse, zu einem besseren Verständnis der primären Patientendaten zu kommen.“

„Obwohl wir kaum begonnen haben, zu erfassen, was das für unsere Seelen, unsere Gesellschaften, unsere Weltordnung bedeutet, bleibt das globale Netzwerk grundlegend für unsere Alltagspraxis.“[1] Es bestehen gewaltige Hoffnungen, durch die Verknüpfung von Patientendaten mit Erkenntnissen aus vergleichbaren Fällen und Behandlungsverläufen und dem Einsatz von diagnose- und behandlungsunterstützenden „intelligenten“ Systemen die medizinische Versorgung zu verbessern und Kosten zu sparen. Von „Chancen biblischen Ausmaßes“ ist die Rede.[2] Heilungs- und Heilsversprechen liegen oft nah beieinander. Nicht selten handelt es sich dabei um Werbeversprechen und persönliche Meinungen, denen es an der empirischen Evidenz fehlt.

Die Zusammenführung und Auswertung von Gesundheitsdaten beschränkt sich nicht auf den medizinischen Bereich. Durch die Einbeziehung von Daten aus anderen Lebensbereichen, etwa über das Wohn- und Arbeitsumfeld (Ernährungsweise, Schlafdauer und -qualität, Fernsehkonsum, Stress, Bewegung, Urlaub, Überstunden usw.), Angaben in sozialen Netzwerken, das Klima, die Region usw. können nicht nur neue medizinische, sondern auch ökonomische, soziale und politische Erkenntnisse erlangt werden. Aussagen über die Gesundheit einer Person können aus Daten abgeleitet werden, die in anderen Bereichen als dem Gesundheitssektor anfallen. So erlaubt z. B. die Datenanalyse aus sozialen Netzwerken und der Internetnutzung Rückschlüsse und Wahrscheinlichkeitsberechnungen, ob ein Nutzer übergewichtig, depressiv, herzkrank, suchtgefährdet oder Ähnliches ist.

Mit Big Data ist die Hoffnung verbunden, die gesundheitliche Prävention zu stärken. Anstatt z. B. hohen Blutdruck oder Diabetes nach ihrem Auftreten zu behandeln, soll schon

---

1 Greenfield, Radical Technologies, zit. bei Graff, Das große Unbehagen, SZ v. 9.11.2017, 11.

2 Wehmeier/Baumann in Langkafel, S. 147, zitieren The Guardian UK v. 22.2.2014.

das Auftreten solcher Krankheiten durch frühzeitiges Eingreifen verhindert werden. Dieses umfassende Verständnis von Krankheit bzw. Gesundheit spiegelt sich darin wieder, dass individuelle wie gesellschaftliche Interventionen früher und umfassender einsetzen und hieraus neue Märkte entstehen. Big Data spielt dabei eine zentrale Rolle durch die Vorhersage von persönlichen Erkrankungen wie von Epidemien.

Treiber der informationstechnischen und der medizinischen Entwicklung sind die wirtschaftlichen Rahmenbedingungen. Die Gesundheitswirtschaft ist einer der größten Wirtschaftssektoren in modernen Gesellschaften. Mehr als 300 Mrd. € fließen jährlich in das deutsche Gesundheitssystem; damit werden 12% des Bruttoinlandsprodukts erwirtschaftet. Der Sektor wächst stärker als die Gesamtwirtschaft. Einen wesentlichen Beitrag hierzu leistet die Digitalisierung.[3] Nach Schätzungen des McKinsey Global Institutes ergibt sich durch den Einsatz von Big Data allein im US-amerikanischen Gesundheitswesen ein Potenzial für Effizienz- und Qualitätssteigerungen im Wert von ca. 222 Mrd € jährlich und für den gesamten öffentlichen Sektor in Europa in Höhe von 250 Mrd. €.[4] „Stark in der öffentlichen Diskussion steht die Big-Data-basierte Differenzierung der Tarife von Krankenkassen, die auf der Erfassung der Körperdaten, insbesondere dem Bewegungsverhalten, beruhen. Hierzu werden Befürchtungen über eine kontroverse Selektion von Risiken, zum Anpassungsdruck auf Nicht-Nutzer und über eine mögliche Entsolidarisierung im Gesundheitswesen geäußert."[5]

Das Gutachten nimmt eine faktische Bestandsaufnahme vor, stellt den rechtlichen Rahmen dar und zieht hieraus praktische und politische Schlussfolgerungen. Philosophische oder wissenschaftstheoretische Erwägungen können im Rahmen des vorliegenden Gutachtens nur am Rande einfließen.[6] Behandelt werden auch nicht im Detail die technischen[7] sowie die mathematisch-statistischen Aspekte[8], soweit sie nicht gesellschaftliche oder rechtliche Implikationen haben.

1.2 Übersicht

Nach einer Diskussion und Klärung von Begriffen (Kap. 2) werden wichtige Akteure beim Einsatz von Big Data im Gesundheitsbereich sowie deren Intentionen, deren praktisches Vorgehen sowie die Stellung der Betroffenen dargestellt (Kap. 3). Dabei wird auch erörtert, inwieweit mit dem Einsatz dieser Technik ein Bedeutungsgewinn oder -verlust dieser Akteure sowie eine Veränderung des Verhältnisses von diesen untereinander verbunden ist. Zu unterscheiden ist zwischen Datenlieferanten, Intermediären, Anwendern der Big-Data-Technik sowie Nutzern der Analyseergebnisse.

---

3 Bundesministerium für Wirtschaft und Energie, Eckpunktepapier Digitalisierung der Gesundheitswirtschaft, Mai 2017, S. 1.

4 Langkafel in Langkafel S. 12.

5 Leistungsbeschreibung „Vergabe eines Gutachtens zum Thema Big Data im Gesundheitsbereich; 2017_32_BS", S. 9 f.

6 Dazu z. B. von Müller in Langkafel S. 53 ff.

7 Dazu Strategy/pwc S. 56 ff.

8 Dazu überblickmäßig Deutscher Ethikrat S. 40 ff.

Die Akteure verfolgen mit ihren Beiträgen verschiedene Zielsetzungen. Ob, inwieweit und unter welchen Voraussetzungen diese Zwecke erreicht werden und welche Möglichkeiten sich hieraus ergeben, wird thematisch strukturiert dargestellt (Kap. 4). Diesen Chancen stehen spezifische individuelle, institutionelle und gesellschaftliche Risiken gegenüber, die bei der Anwendung berücksichtigt werden müssen und auf die das Recht reagiert bzw. reagieren sollte (Kap. 5).

Die verfassungsrechtlichen Aspekte von Big-Data umfassen den Schutz von Grundrechten wie auch institutionelle Fragestellungen, etwa der allgemeinen Gesundheitsvorsorge oder des Sozialstaats- und des Demokratiegrundsatzes (Kap. 6). Deren Konkretisierung im nationalen sowie im europäischen Recht und evtl. in weiteren Rechtsquellen muss aus straf-, zivil- und öffentlich-rechtlicher Perspektive beleuchtet werden, wobei im Vordergrund der vorliegenden Darstellung das Datenschutz- und das Verbraucherrecht stehen (Kap. 7-9).

Beim Einsatz von Big-Data-Technik bestehen spezifische rechtliche Fragestellungen in unterschiedlichen Anwendungsfeldern. Diese werden systematisch vertieft bearbeitet (Kap. 10).

Abschließend wird der sich aus der Darstellung ergebende Handlungsbedarf für den Gesetzgeber und für weitere Akteure – von den Anwendern, Herstellern, Verbänden, sonstige Institutionen bis hin zur Forschung – zusammengefasst (Kap. 11).

1.3 Methode

Das Gutachten beruht auf der Auswertung wissenschaftlicher Publikationen sowie der Medien, insbesondere der Presse. Das ursprünglich verfolgte Ziel, mit Hilfe von standardisierten Fragebögen von Stakeholdern zusätzliche Informationen einzuholen, erwies sich als zu unflexibel. In offenen Gesprächen mit interessierten und kompetenten Beteiligten wurden die Fragestellungen hinsichtlich der jeweiligen spezifischen Themen erörtert. Durch gezielte Nachfragen und eine vertiefte Erörterung der spezifischen Fragestellungen konnten erheblich bessere Erkenntnisse als über eine standardisierte Befragung erlangt werden. Wurde hierbei auf weiterführende Literatur[9] verwiesen, so wird diese als Quelle ausgewiesen.

2 Begriffe

Im Rahmen einer disziplinübergreifenden Untersuchung bedarf es einiger begrifflichen Klärungen, da viele der verwendeten Begriffe unterschiedlich genutzt und verstanden werden. Da ein zentraler Fokus in der Untersuchung rechtlicher Aspekte und den insofern bestehenden Defiziten liegt, wird auf eine präzise rechtliche Einordnung besonderer Wert gelegt.

[9] Ein medizinisch-technischer Literaturüberblick findet sich bei Strategy/pwc S. 66 ff., 207 ff.

2.1 Gesundheitsdaten

Big Data im Gesundheitsbereich basiert grundsätzlich auf Informationen von Menschen, d. h. von natürlichen Personen. Dabei kommt es zumeist nicht auf die Identität der einzelnen Person an, sondern auf die Individualität des einzelnen „Falls" und dessen generalisierbare Aussagekraft. Der Rohstoff von Big Data sind **personenbezogene Daten** im Sinne des Datenschutzrechts (im Detail s. u. 8.3). Hierzu zählen auch personenbeziehbare Daten, in denen die Identität der einzelnen Person nicht mehr bekannt ist, die aber z. B. über ein Pseudonym einer natürlichen Person zugeordnet werden können (s. u. 8.12.2).

Das Datenschutzrecht stellt generell personenbezogene Daten unter Schutz, ein besonderer rechtlicher Schutz besteht für sensitive Daten, zu denen Gesundheitsdaten und genetische Daten gezählt werden. Diese Daten gehören gemäß der Definition von Art. 9 Abs. 1 DSGVO zu den „**besonderen Kategorien** personenbezogener Daten", deren Verarbeitung nur unter höheren Anforderungen zulässig ist.

In Art. 4 Nr. 15 DSGVO werden Gesundheitsdaten wie folgt definiert: „personenbezogene Daten, die sich auf die **körperliche oder geistige Gesundheit** einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen". Eine weitere Konkretisierung nimmt Erwägungsgrund (ErwGr) 35 S. 1 DSGVO vor. Danach werden in einer weiten Auslegung alle Daten erfasst, „die sich auf den Gesundheitszustand einer betroffenen Person beziehen und aus denen Informationen über den früheren, gegenwärtigen und künftigen körperlichen oder geistigen Gesundheitszustand der betroffenen Person hervorgehen".[10] Angeknüpft wird an den Gesundheitszustand, nicht an eine Krankheit. Auch der Ablauf und der Inhalt einer medizinischen Behandlung einschließlich der eingenommenen Medikamente sowie die Feststellung, dass eine Person genesen oder überhaupt völlig gesund ist, gehören hierzu.[11]

Erfasst wird auch die **Inanspruchnahme von Gesundheitsleistungen**. Dazu gehören Daten, „die im Zuge der Anmeldung für sowie der Erbringung von Gesundheitsdienstleistungen im Sinne der Richtlinie 2011/24/EU" erhoben werden (ErwGr 35 S. 2 DSGVO). Alle Formen der Organisation und Erbringung von Gesundheitsleistungen werden erfasst, unabhängig davon, wie diese organisiert, erbracht oder finanziert werden. Bei der Inanspruchnahme von Leistungen kommt es nicht darauf an, dass eine gesundheitlich helfende Stelle als solche benannt wird. Es kann genügen, dass z. B. die allgemein bekannte Adresse einer Drogenberatungsstelle aufgeführt wird und hierüber eine gesundheitsbezogene Zuordnung möglich wird.[12]

---

10 Klabunde in Ehmann/Selmayr Art. 4 Rn. 43; Greve in Auernhammer Art. 9 Rn. 4.

11 Simitis in Simitis § 3 Rn. 260; Bergmann/Möhrle/Herb § 3 Rn. 171; vgl. Article 29 Working Party, 5.2.2015, Annex – health data in apps and devices, http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf.

12 Kühling/Seidel in Kingreen/Kühling, 37.

Zu personenbezogenen Gesundheitsdaten gezählt werden auch mit Nummern, Symbolen oder Kennzeichen erschlossene, also **pseudonymisierte Daten** bzw. Datensätze, wie sie oft in Krankheitsregistern oder bei medizinischen Forschungsprojekten vorliegen: „Informationen, die von der Prüfung oder Untersuchung eines Körperteils oder einer körpereigenen Substanz, auch aus genetischen Daten und biologischen Proben, abgeleitet wurden, und Informationen etwa über Krankheiten, Behinderungen, Krankheitsrisiken, Vorerkrankungen, klinische Behandlungen oder den physiologischen oder biomedizinischen Zustand der betroffenen Person unabhängig von der Herkunft der Daten, ob sie nun von einem Arzt oder sonstigem Angehörigen eines Gesundheitsberufes, einem Krankenhaus, einem Medizinprodukt oder einem In-Vitro-Diagnostikum stammen“ (ErwGr. 35 S. 2 DSGVO). Es kommt nicht darauf an, wer das Datum auf welche Weise erfasst. Dazu gehören also auch physiologische Daten von Selbstmessungen, Gesundheits-Apps, Smart-Watches, Fitness-Geräten oder Wearables[13], wie sie im Wellness- und Lifestyle-Bereich oder im Arbeitsleben genutzt werden.[14]

Gesundheitsdaten sind wegen ihrer **existenziellen Bedeutung** für die Betroffenen besonders rechtlich geschützt. Dies geht bis auf den Eid des Hippokrates (um 460 bis 370 v. Chr.) des ärztlichen Berufsstandes zurück: „Was ich bei der Behandlung sehe oder höre oder auch außerhalb der Behandlung im Leben der Menschen, werde ich, soweit man es nicht ausplaudern darf, verschweigen und solches als ein Geheimnis betrachten.“ Dieser Schutz ist heute insbesondere mit der ärztlichen Schweigepflicht (Patientengeheimnis) in Berufsordnungen von Heilberufen oder in § 203 Strafgesetzbuch (StGB) normiert (s. u. 6.8). Der damit verbundene Schutzgedanke besteht darin, einem Menschen zu ermöglichen, in einer individuellen Notsituation den Zugang zur Hilfe zu ermöglichen, ohne dadurch Nachteile befürchten zu müssen, weil Daten an Dritte gelangen, die mit dieser Nothilfe nichts zu tun haben.[15]

Gesundheitsdaten sind auch gegeben, wenn auf den Gesundheitszustand **Rückschlüsse** möglich sind,[16] etwa bei Inanspruchnahme von gesundheitsbezogenen Dienstleistungen, bei der Angabe bestimmter Krankheitssymptome, einer behördlichen medizinischen Feststellung (z. B. Anerkennung als Schwerbehinderter)[17] oder der ärztlichen Feststellung einer Arbeitsunfähigkeit.[18] Gesundheitsrelevante Daten fallen in verschiedenen, teilweise einander überschneidenden, teilweise völlig voneinander losgelösten Kontexten an.

---

13 Klose in Stiftung Datenschutz (2017) S. 97 ff.; zum Einsatz im Arbeitsleben Weichert NZA 2017, 567 f.

14 Eßer in Auernhammer Art. 4 Rn. 73; Härting Rn. 539; Jandt DuD 2016, 572.

15 Weichert in Kühling/Buchner Art. 4 Nr. 15 Rn. 4; Schaar in Stiftung Datenschutz (2017) S. 142 f.; ähnlich der Eid des Assaf, ca. 5. Jahrhundert nach Christus: „Verrate nicht das Geheimnis eines Mannes, der dir Vertrauen schenkte.“

16 Gola/Schomerus § 3 Rn. 56a.

17 Gola in Gola Art. 4 Rn. 76

18 EuGH 6.11.2003 – C-101/01, Rn. 49–51 = JZ 2004, 243 f. – Lindqvist; a. A. Schild in Wolff/Brink § 3 Rn. 150.

Big Data ermöglicht eine umfassende Dekontextualisierung und Rekontextualisierung.[19] Werden Daten, die für sich keine Gesundheitsdaten sind, mit Gesundheitsdaten in einen inhaltlichen Zusammenhang gestellt, so werden sie zu Gesundheitsdaten. Es kommt auf den Verwendungszusammenhang der Information im Einzelfall an.[20] Relevant ist, ob direkt oder indirekt die Angabe Informationen über die Gesundheit des Betroffenen vermittelt.[21] Dies ist z. B. der Fall, wenn über Einsatz von Sexspielzeug, etwa eines Vibrators, Daten an ein Unternehmen weitergeleitet werden.[22] Die Angaben eines Schrittzählers von einem sog. Wearable, mit dem keine weiteren Werte erfasst werden, sind keine Gesundheitsdaten, wohl aber, wenn weitere Körper- und Bewegungsdaten erfasst sowie individuelle Zuordnungen vorgenommen werden, um Rückschlüsse auf den Gesundheitszustand zu ziehen.[23]

Eine Grundbedingung für die technische Revolution im Gesundheitsbereich war, dass Gesundheitsdaten digital erhoben und gespeichert werden können. Dies ist durch die Fortschritte im Bereich der Sensorik immer mehr und detaillierter möglich. Dabei hat neben der Erfassung von Orts-, Bewegungs- und Bilddaten die Messung und Registrierung von chemischen und biologischen Prozessen bzw. Zuständen eine zentrale Bedeutung. Das Forschungslabor Google X hat eine digitale Kontaktlinse für Diabetiker entwickelt, die über die Tränenflüssigkeit den Blutzuckerwert eines Menschen misst und die Daten mit einer Funkantenne, die dünner als ein menschliches Haar ist, an ein externes Gerät, z. B. an ein Smartphone übermittelt.[24] Auf der menschlichen Haut lassen sich Sensoren aufbringen, mit denen Körperfunktionen gemessen werden können, die bei Alltagsaktivitäten keinerlei Beeinträchtigungen bewirken.[25] Atemanalysen ermöglichen über sog. Metabolite die Erkundung von Krankheitsursachen, sind aber auch geeignet zur Personenidentifizierung oder zur Kontrolle des Lebensstils.[26] Mit einer Auswertung der von mit einer Videokamera erfassten Gesichtsbilder lässt sich der Puls einer Person messen.[27]

2.1.1 Genetische Daten

Bis zum Wirksamwerden der DSGVO war es streitig, inwieweit genetische Daten in jedem Fall als Gesundheitsdaten anzusehen sind und so einen besonderen rechtlichen Schutz genießen.[28] Genetische Daten stehen in einem engen Zusammenhang mit Gesundheitsdaten. Mit der Anwendbarkeit der DSGVO (Art. 9 Abs. 1) ist deren Sensitivität

---

19 Deutscher Ethikrat S. 11; Ladeur DuD 2016, 360 f.

20 Kontext ist nicht identisch mit Absicht; hierauf stellt Gola in Gola Art. 4 Rn. 76 ab.

21 Simitis in Simitis § 3 Rn. 263; Deutscher Ethikrat S. 96.

22 Sammelklage gegen Vibratoren-App bringt 5 Millionen kanadische Dollar, DANA 2017, 108; Klage gegen datensammelnde Vibrator-App, DANA 2016, 198.

23 Zit. nach Dregelies VuR 2017, 259.

24 Kontaktlinse misst Blutzuckerwert, DANA 2014, 81.

25 Gesundheitssensoren – auf die Haut aufgedruckt, DANA 2013, 76 f.; Sensorpflaster zum Aufkleben, DANA 2012, 40.

26 Atemanalysen – nicht nur zur medizinischen Diagnostik, DANA 2014, 41.

27 Pulsmessen per Webcam, DANA 2013, 130.

28 Dafür Weichert in Däubler u. a., § 3 Rn. 65; Bergmann/Möhrle/Herb § 3 Rn. 172; relativierend Simitis in Simitis, § 3 Rn. 259.

uneingeschränkt anerkannt als eine **besondere Kategorie personenbezogener Daten.** Nach Art. 4 Nr. 13 DSGVO sind genetische Daten „personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden".

Eine **Präzisierung** nimmt ErwGr 34 DSGVO vor: „Genetische Daten sollten als personenbezogene Daten über die ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person definiert werden, die aus der Analyse einer biologischen Probe der betreffenden natürlichen Person, insbes. durch eine Chromosomen-, Desoxyribonukleinsäure (DNS)- oder Ribonukleinsäure (RNS)-Analyse oder der Analyse eines anderen Elements, durch die gleichwertige Informationen erlangt werden können, gewonnen werden." Eine Definition enthält zudem § 3 Nr. 11 GenDG. Danach sind genetische Daten „die durch eine genetische Untersuchung oder die im Rahmen einer genetischen Untersuchung durchgeführte Analyse gewonnenen Daten über genetische Eigenschaften." Eine molekularbiologische Analyse ist also nicht zwingend Voraussetzung für die Annahme; es genügt ein sonstiges Verfahren, mit dem Rückschlüsse auf genetische Merkmale gezogen werden.

Die **Besonderheit** genetischer Daten besteht darin, dass sie von der Eizellenbefruchtung bis lange nach dem Tod weitgehend stabil und unverändert bleiben. Die Betroffenen sind den damit verbundenen Merkmalen „schicksalhaft ausgeliefert". Eine Anonymisierung von genetisch analysierten Proben ist praktisch nicht möglich.[29] Genetische Daten erlauben eine Aussage über bestehende äußerlich erkennbare sowie innere körperliche und seelische Merkmale einer Person. Sie lassen auch Prognosen mit Wahrscheinlichkeitsangaben, z. B. über künftige Erkrankungen, zu. Wegen der Vererblichkeit der Erbinformationen sind nicht nur Aussagen zur untersuchten Person möglich, sondern auch zu näheren direkten biologischen Verwandten (u. a. Eltern, Geschwister, Kinder). Biologische Verwandte müssen dabei nicht zueinander in einem sozialen Verhältnis stehen. Als Datenträger kommen Speichel, Hautschuppen oder Haare in Betracht, die oft unbewusst und unkontrollierbar zurückgelassen werden. Gendaten bedürfen oft für ihre Generierung eines technisch aufwändigen Verfahrens, bei dem Big-Data-Technik zum Einsatz kommt.[30] Angesichts der absehbaren biotechnologischen Entwicklung sehen manche Autoren in der Verteidigung der „Bioprivatheit" eine der wichtigsten anstehenden gesellschaftspolitischen Aufgaben.[31]

---

29 Schaar ZD 2016, 225; Greve in Auernhammer Art. 9 Rn. 2; verkürzt Eßer in Auernhammer Art. 4 Rn. 61 in Bezug auf Forschungszwecke, unter Verweis auf Hardenberg ZD 2014, 116 f.; ähnlich Schreiber in Plath Art. 4 Rn. 45.

30 Art. 29-Datenschutzgruppe WP 91, 4 f.; Weichert DuD 2002, 134; ders. DuD 2017, 540.

31 Sorgner in Stiftung Datenschutz (2017) S. 177 ff.

2.1.2 Biometrische Identifikatoren

Mit dem Wirksamwerden der DSGVO werden gemäß Art. 9 Abs. 1 auch „biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person“ als sensitive Daten eingestuft. Diese Einstufung ist nicht darauf zurückzuführen, dass dabei auch ein Gesundheitsbezug bestehen kann, sondern darauf, dass viele biometrische Merkmale unveränderbar sind und sich (z. B. per Gesichtserkennung, Stimmerkennung) regelmäßig zu einer ungewollt oder gar heimlichen Identifikation sowie für Zuordnungen beliebiger individueller Angaben und Datensätze eignen.[32] Zu einer solchen Identifikation bzw. Authentisierung können Ergebnisse medizinischer Diagnoseinstrumente, etwa Hirnstromanalysen, genutzt werden.[33] Viele Gesundheitsdaten, etwa Bilddaten vom Gehirn, sind für jeden Menschen einzigartig.[34] Selbst bei einem Menschen vorgefundene Bakterien eignen sich zur präzisen personalen Identifizierung.[35] Insbesondere biometrischen Rohdaten erlauben teilweise – ähnlich wie genetische Daten – Aussagen über gesundheitliche bzw. körperliche oder seelische Zustände, wodurch sich die Sensitivität der Daten erhöht. Im Interesse der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO) sind solche für Identifizierungszwecke nicht nötigen Zusatzinformationen zu vermeiden (s. u. 8.12).[36]

2.1.3 Gedanken- und Emotionsdaten

In den Frühzeiten der Digitalisierung erfolgte an der Schnittstelle zwischen Mensch und Maschine (Computer) ein Medienbruch. Mit neuen Techniken wird dieser ganz oder teilweise aufgehoben. Schon weit verbreitet sind Sprachassistenten, wie sie inzwischen von allen großen US-Plattformen für Endnutzer angeboten werden, etwa als Alexa bzw. Echo (Amazon), Google Home bzw. Assistant, Cortana (Microsoft), Siri bzw. PodHome (Apple).[37] Weitere Beispiele gewillkürter Schnittstellenautomation sind der Einsatz implantierter Chips, die Bedienung von Rechnern mit Hilfe von bestimmten Körperbewegungen (z. B. Kopfbewegung) oder – noch in einem frühen Entwicklungsstadium – die Computersteuerung mit Gedanken. Angestrebt wird damit zumeist ein Komfort- und Funktionalitätsgewinn. Eingesetzt wird die Technik aber auch zur Unterstützung von Menschen mit Behinderungen, denen z. B. wegen der Unmöglichkeit der Nutzung ihrer Hände die Verwendung von Tastatur oder Touchpad nicht möglich ist. Anders als z. B. bei der klassischen Tastatureingabe verflüchtigt sich bei derartigen Techniken zumeist die Explizitheit der Eingabe, da mit Sensoren gekoppelte Algorithmen den menschlichen Willen interpretieren müssen, bevor sie diesen umsetzen können. Es ist für die Sensoren zumeist nicht möglich, zu unterscheiden, ob der wahrgenommene Befehl intentional oder unabsichtlich erfolgte.

---

32 Weichert in Kühling/Buchner Art. 4 Nr. 14 Rn. 2; Deutscher Ethikrat S. 56.; Theißen S. 126 ff.
33 Authentifizierung per Hirnstromanalyse, DANA 2017, 59.
34 Deutscher Ethikrat S. 65.
35 Mikroben identifizieren Personen und Umgebungen, DANA 2015, 188.
36 Weichert in Kühling/Buchner Art. 4 Nr. 14 Rn. 9.
37 Deutscher Ethikrat S. 52.

Eine weitere Stufe der Digitalisierung wird mit Sensoren erreicht, die nicht **mehr gewillkürte Handlungen**, sondern mechanische, chemische oder biotechnische Zustände interpretieren. Ein Beispiel hierfür ist der Aufmerksamkeitssensor im Auto, der den Lidschlag des Fahrers misst und interpretiert. Ein medizinisches Beispiel ist die automatisierte Insulinabgabe bei Diabetes-Patienten.[38]

Von besonderer persönlichkeitsrechtlicher Relevanz ist es, wenn nicht objektive, sondern **subjektive persönliche Sachverhalte**, insbesondere Gedanken und Gefühle erfasst werden. Dies ist z. B. über Stimm- oder Gesichtsanalysen möglich.[39] Dabei werden menschliche Gedanken erfasst und für Entscheidungszwecke interpretiert.[40] Anknüpfungspunkt sind nicht mehr Äußerlichkeiten einer Person, sondern deren per Algorithmus interpretierte Wertungen und Entscheidungen. Nicht nur bewusste, sondern auch un- bzw. unterbewusste innere Vorgänge der Personen werden zum Gegenstand digitaler Datenverarbeitung. Gefühle waren bisher personale Sachverhalte, die einer Erfassung und Auswertung nur sehr begrenzt zugänglich waren. Dies hat sich mit der fortgeschrittenen Automation der Mensch-Maschine-Beziehung geändert.[41]

Eine frühe Anwendung der metrischen Erfassung von Emotionsdaten sind die bis heute im Einsatz befindlichen, inzwischen technologisch weiterentwickelten **Lügendetektoren** oder Polygrafen. Mit ihnen werden Hirnströme, Blutdruck, Puls, Atemfrequenz, Schweißbildung, Hautdurchblutung sowie weitere Körperfunktionen gemessen, während ein Proband mit bestimmten Fakten oder Fragen konfrontiert wird. Derartige Tests beruhen auf der Annahme, dass physische oder psychische Bedrohungslagen beim Menschen unwillkürlich komplexe Muster an körperlichen Reaktionen hervorrufen.[42] Eine spezielle solche Detektion wurde in Tschechien bei Asylsuchenden eingesetzt, die angaben, wegen ihrer Homosexualität in ihrem Heimatland verfolgt zu sein. Zur Prüfung der Richtigkeit dieser Angabe wurden Erektionstests durchgeführt, bei denen den Flüchtlingen pornografische Filme und Bilder von nackten Männern, Frauen und Kindern vorgelegt wurden (sog. Phallometrie).[43]

Inzwischen hat sich die Neurowissenschaft weiterentwickelt. Hirnscanner ermöglichen äußerst differenzierte Aussagen über die von Fragen oder faktischen Eindrücken verursachten Gefühle von Probanden. Die Erfassung nicht nur von einzelnen Gedanken und Emotionen, sondern von diesen zugrunde liegenden **Werthaltungen und Einstellungen** bzw. deren Ableitung aus äußerlichen Daten wird in absehbarer Zukunft eine zunehmende Bedeutung erlangen. Die emotions- oder psychoadäquate Ansprache von Menschen birgt

---

38 Weichert DANA 2017, 203; Deutscher Ethikrat S. 78; Müller, App auf Rezept, Der Spiegel 29/2017, 68; vgl. z. B. Do-It-Yourself Pancreas System (DIYPS), diyps.org.

39 Sog. Emotion Analytics; Affektive Informatik im Dienste von Kundenbindung und Sicherheit, DANA 2013, 36; Jüngling, Diese Stimmanalyse entlarvt all unsere Geheimnisse, www.welt.de 6.3.2015.

40 Computer lesen Gedanken, DANA 2012, 40 f.; Computer analysieren Sprechergefühle, DANA 2012, 41.

41 Deutscher Ethikrat S. 139 f.

42 Hipp/Winter, Antworten des Unbewussten, Der Spiegel 44/2017, 26 f.; ausführlich zum frühen Einsatz von Lügendetektoren in den USA Westin, Privacy and Freedom, 1967/1970, S. 145 ff.

43 Erektionstests bei homosexuellen Asylsuchenden, DANA 2011, 24 f.

ein großes Manipulationspotenzial. Wirtschaftliches, soziales und auch das politische Verhalten lässt sich damit beeinflussen. Die Wirkungen müssen sich nicht auf die einzelne Person beschränken, sondern können ganze Gesellschaften betreffen. Dies zeigte sich u. a. anlässlich des US-Präsidentschaftswahlkampfs 2016, wo mit gezielter Propagandaansprache u. a. mit sog. Fake-News eine erkennbare Wählerbeeinflussung erfolgte.[44] Über soziale Netzwerke und Messengerdienste kamen Algorithmen zum Einsatz kamen, die Botschaftsinhalte vermittelten, „die auf Angst und Wut basieren".[45]

Angaben zu Gedanken, Gefühlen oder über neuronale Vorgänge sind spezifisch bisher von unserem Recht noch nicht erfasst. Gesetzlich geschützt sind die Menschen allenfalls vor der diskriminierenden Nutzung solcher Daten in politischen, sexuellen oder gesundheitlichen Kontexten durch die Anwendung von Art. 9 DSGVO oder des AGG. Hinsichtlich ihrer Sensitivität entsprechen sie Gesundheitsdaten und gehen regelmäßig weit darüber hinaus. Sie sind in besonderem Maße schutzbedürftig. Solange insofern keine spezifischen Schutzvorkehrungen bestehen, sind sie als Gesundheitsdaten zu behandeln, zumal sie aus körperlichen Umständen abgeleitet werden. Gesundheit bezieht sich nicht nur auf körperliche, sondern auch auf seelische Verhältnisse.

2.1.4 Metadaten

Bei der Datenverarbeitung generell und insbesondere bei der Verarbeitung von Gesundheitsdaten bekommen sog. Metadaten eine zunehmende Bedeutung. Dabei handelt es sich nicht um Dateninhalte, sondern um diesen zugeordnete Daten, die Auskunft geben über die Umstände der Datenverarbeitung, also insbesondere über Herkunft, Empfänger, Ort, Zeit, Kontext, verarbeitendes System (Hard- od. Software). Metadaten fallen regelmäßig bei der Telekommunikation an, wo sie bisher als Nutzungsdaten in § 15 TMG bzw. als Verkehrs- und Standortdaten in den §§ 96, 98 TKG spezifisch geregelt sind. Im Entwurf einer künftigen europäischen ePrivacy-Verordnung[46] werden Metadaten definiert als die Daten, „die in einem elektronischen Kommunikationsnetz zu Zwecken der Übermittlung, der Verbreitung oder des Austauschs elektronischer Kommunikationsinhalte verarbeitet werden".[47]

Metadaten spielen nicht nur in der Kommunikation eine Rolle, sondern sind auch von hoher Relevanz bei stelleninternen Verarbeitungsprozessen. Mit Hilfe von Metadaten können Zugriffs-, Schreibe- und Leserechte zu einzelnen Datensätzen vergeben,

---

44 Zu Cambridge Analytica Kosinski, Ich habe nur gezeigt, dass es die Bombe gibt, dasmagazin.ch 3.12.2016 (Das Magazin No. 48/2016).

45 So der demokratische US-Abgeordnete Adam Schiff, zitiert nach Kuhn, Hauptsache Chaos, SZ 3.11.2017, 7.

46 Entwurf der EU-Kommission, Verordnung über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation) v. 10.1.2017, Stellungnahme des EU-Parlaments v. 20.10.2017, Bericht über den Vorschlag für eine Verordnung über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation, COM(2017)0010 – 'C8-0009/2017 – 2017/003(COD).

47 Art. 4 Abs. 3 lit. c Entwurf ePrivacy-Verordnung.

Zweckfestlegungen vorgenommen sowie sonstige Verarbeitungsanforderungen definiert werden.

Ursprünglich ging man davon aus, dass Metadaten weniger sensitiv wären als Inhaltsdaten, da mit ihnen nur Umstände, keine originären Inhalte abgebildet werden. Big Data und vernetzte Kommunikation hat diese Sichtweise verändert: Metadaten sind, da sie zumeist strukturiert vorliegen, besonders leicht auswertbar und verraten über die Rahmenbedingungen einer Verarbeitung auch viel über die Kommunikations- oder Verarbeitungsinhalte (z. B. Inanspruchnahme einer Gesundheitsberatung). Metadaten eignen sich besonders zum Tracking (s. u. 2.3), zur Profilbildung (s. u. 2.5) oder zu sonstigen Big-Data-Auswertungen und haben insofern besondere persönlichkeitsrechtliche Relevanz.[48]

2.2 Big Data

Die Begriffe „Big Data" bzw. „Big Data Analytics" sind nicht rechtlich definiert. Wegen ihrer Offenheit und Ungenauigkeit wird mit ihnen ein weiter Anwendungsspielraum eröffnet.[49] Es handelt sich um Sammelbegriffe für digitale Techniken, die in dreierlei Hinsicht „groß" sind, nämlich in Bezug auf *volume* (Umfang, Datenvolumen), *velocity* (Geschwindigkeit, mit der die Datenmengen generiert, transferiert und ausgewertet werden) sowie *variety* (Bandbreite der Datentypen, -formate und -quellen). Es geht um ein „Bündel von neu entwickelten Methoden und Technologien, die die Erfassung, Speicherung und Analyse eines großen und beliebig erweiterbaren Volumens unterschiedlich strukturierter Daten ermöglicht".[50] Die Zusammenführung und Auswertung der Daten erfolgt mittels digitaler statistisch-inferenzieller Verfahren. Ziel von Big Data ist es, Muster zu erkennen und daraus Einsichten zu gewinnen.[51] Erweitert wird die Definition um *value* und *validity*, was für (unternehmerischen) Mehrwert und Datenqualität steht.[52] Unter den Stichworten „validity" bzw. „veracity" werden die Verlässlichkeit und Vollständigkeit von Big-Data-Anwendungen und der dabei verwendeten Daten thematisiert. Mit der Menge der Daten steigt, Relevanz unterstellt, die Aussagekraft der Analyse für einzelne untersuchte Faktoren und die Möglichkeit, zusätzliche, auch schwach wirkende Faktoren und ihre Interaktionen zu berücksichtigen.[53]

Angesichts einer hohen Aussagekraft bzw. „Intelligenz" von Big-Data-Ergebnissen ist auch von Smart Data die Rede.[54] Der Begriff Big Data hat sich vor weniger als 10 Jahren etabliert. Er ist Ausdruck des in dieser Zeit erfolgten informationstechnischen Fortschritts.

---

48 EuGH 21.12.2016 – C-203/15, C-698/15, Rn. 98-100 ,= DVBl 2017, 180 f.; BVerfG 24.1.2012 – 1 BvR 1299/05, Rn. 137 = NJW 2012, 1424; Münch S. 108 f.

49 Langkafel in Langkafel S. 4.

50 Langkafel in Langkafel S. 12, mit Verweis auf den Wissenschaftlichen Dienst des Deutschen Bundestags v. 6.11.2013, Nr. 37/13; Krolop/Souchon in Langkafel S. 181 ff.; Raum in Stiftung Datenschutz (2017) S. 135 f.

51 Deutscher Ethikrat S. 36.

52 Zur rechtlichen Einstufung von Datenqualität Hoeren ZD 2016, 459 ff.

53 Deutscher Ethikrat S. 10; Strategy/pwc S. 54.

54 Krolop/Souchon in Langkafel S. 184; Timm MedR 2016, 689.

Er steht für eine neue Ära digitaler Kommunikation und Datenverarbeitung, mit der ein ökonomischer und gesellschaftlicher Umbruch einhergeht.

Big Data ist eine Antwort auf die Begrenzung der Nutzungsmöglichkeiten von Daten in geschlossenen oder lokalen Systemen. Sie entspringt dem Wunsch und der Begehrlichkeit, weltvolle Daten aus ihren Datensilos zu „befreien" und diese multifunktional verwenden zu können. Durch die globale informationstechnische Vernetzbarkeit von Daten sowie deren fast unbeschränkte Speicher-, Veränder- und Auswertbarkeit gibt es hierbei kaum noch technische Grenzen.

Big Data umfasst die Datenverarbeitungsprozesse des Erfassens und Sammelns (data collection), des Speicherns (storing), des Zusammenführens und Verwaltens (integration and sharing), des Analysierens (analytics) und des Visualisierens bzw. der Nutzung zur Entscheidungsfindung.[55] Der Begriff beschreibt sowohl die Verarbeitungsprozesse wie auch die hierfür nötige informationstechnische Infrastruktur. Big Data ist zunächst ein technischer Begriff, der aber soziale, politische, kulturelle, strukturelle und rechtliche Implikationen aufweist.[56]

Big Data im Gesundheitsbereich hat oft eine medizinische Dimension. Hier liegt ein Schwerpunkt in „Omics-Analysen". Als Omics-Daten werden biotechnische Daten aus Genom, Epigenom, Transkriptom, Proteom und Metabolom bezeichnet. Mit diesen aus Molekularanalysen erlangten Daten erfolgt die Verarbeitung von Daten mit Gigabite-Dimension.[57]

Durch Big-Data-Konvergenzen können neben dem Omics-Bereich Daten aus standardisierten und formatierten Datensätzen, Sensordaten, Daten aus bildgebenden Verfahren, unstrukturierte Textdaten, z. B. aus Arztbriefen, deren Inhalt mit Hilfe von Wortanalysen (Semantics) zu erfassen versucht wird, zusammengeführt und ausgewertet werden.[58] Der Rohstoff der hierfür benötigten Daten liegt inzwischen zumeist vollständig digitalisiert, zumindest in digitalisierbarer Form vor, auch im Medizinbereich; es ist die Rede von „datenzentrierter Medizin".[59]

Hinsichtlich der mit Big Data verfolgten technisch-operativen Ziele gibt es kaum Beschränkungen. Unterschieden wird insofern zwischen „Abfragen und Reporting", „Data Mining", „Datenvisualisierung"[60], „Optimierung"[61] und „Simulation".

---

55 Vgl. die Definition des Begriffs der Datenverarbeitung in Art. 4 Nr. 2 DSGVO.

56 Langkafel in Langkafel S. 14.

57 Schepers/Peuker in Langkafel S. 40; Timm MedR 2016, 688; auch „Omik" genannt, Deutscher Ethikrat S. 12, 56.

58 Eberhardt in Langkafel S- 133; zu den semantischen Methoden im Einzelnen Engelhorn in Langkafel S. 205 ff.

59 Ladeur DuD 2016, 360 f. in Abgrenzung zur „erfahrungs- oder evidenzbasierten Medizin" (EBM).

60 Dazu Langkafel in Langkafel S. 253 ff.

61 Dazu Haferkamp in Stiftung Datenschutz (2017) S. 59 ff.

Eine aus persönlichkeitsrechtlicher Sicht – auch im Gesundheitsbereich – besondere Anwendung von Big Data ist die vorhersagende Analytik (predictive analytics). Der vorhandene Datenbestand wird nicht nur genutzt, um eine spezifische, evtl. aktuelle Situation zu analysieren, sondern um Vorhersagen zu künftigen Entwicklungen zu treffen. Bezieht sich die Prognose auf individuelles Verhalten, so sind damit zumeist auch Erwartungen in Bezug auf bestimmte (z. B. gesundheitsrelevante) Verhaltens- oder Reaktionsweisen verbunden, etwa zum Krankheitsverlauf oder zur Einnahme von Medikamenten. Die Prognosen können sich auch auf ein Gruppenverhalten oder einen künftigen kollektiven Zustand beziehen, etwa wenn der Verlauf einer Grippewelle vorhergesagt wird.[62] Gehört eine Person einer solchen analysierten Gruppe an oder wird sie einer solchen zugeordnet, so können derartige Gruppenprognosen für diese Person individuelle Auswirkungen haben.

Mit dem Einsatz von Big Data sind teilweise Heils- und Heilungsversprechen verbunden, für die es keine reale Grundlage gibt. Mit dem Einsatz können auch Ängste und negative Assoziationen verbunden sein, die ebenso wenig eine reale Grundlage haben müssen.[63] Es bedarf daher einer analytischen kritischen Hinterfragung der jeweils eingesetzten Methoden, die bei einem verantwortungsvollen Einsatz zweifellos zum Nutzen der Menschen eingesetzt werden können. Für eine solche kompetente und verantwortliche Nutzung dieser Technik wurde das Wort „datability“ kreiert. Datability war das Leitthema der Cebit 2014.[64]

2.3 Tracking

Beim Tracking wird das Verhalten einer Person auf der Zeitachse hinsichtlich eines oder mehrerer Merkmale, etwa des Aufenthaltsortes, verfolgt. Ein Fall des Gesundheitstrackings ist der Einsatz von Instrumenten des „Quantified Self“ (s. u. 4.5).[65] Aus – in der Vergangenheit erfassten – Trackingdaten werden individualisierte Profile (s. u. 2.5) zu einzelnen Personen erstellt und Prognosen für die Zukunft abgeleitet. In der Praxis am weitesten verbreitet ist das Internet-Tracking hinsichtlich des Surf-, Nutzungs-, Konsum- und Kommunikationsverhaltens von Nutzern.[66] Im Gesundheitsbereich wird die Tracking-Technologie z. B. eingesetzt, um jederzeit den Aufenthaltsort eines Patienten oder einer gefährdeten Person feststellen zu können. Sie dient auch zur Organisation von Betriebsabläufen in Gesundheitseinrichtungen.[67] Auch das Nachvollziehen des Verlaufs von Krankheitsparametern, z. B. Körpertemperatur, Herzschlag oder Atemaktivität, kann als Tracking bezeichnet werden.

62 Krolop/Souchon in Langkafel S. 185
63 Langkafel in Langkafel S. 8 ff., 35 f.; Selke in Stiftung Datenschutz (2017) S. 152.
64 Langkafel in Langkafel S. 10; Brunner in Langkafel S. 65 f.
65 Haferkamp in Stiftung Datenschutz (2017) S. 60 f.
66 Weichert ZD 2013, 255.
67 Theißen S. 45 ff.

2.4 Scoring

Der Begriff „Scoring“ stammt aus der Finanzwirtschaft; er hat 2009 in Deutschland in § 28b Bundesdatenschutzgesetz (BDSG) eine gesetzliche Regulierung gefunden. Ein Score ist ein „Wahrscheinlichkeitswert für ein bestimmtes zukünftiges Verhalten“ eines Betroffenen. Dieser wird mit Hilfe von Merkmalsdaten berechnet „zum Zweck der Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses“ unter Zugrundelegung eines wissenschaftlichen mathematisch-statistischen Verfahrens. Grundlage des Scorings sind Daten über Personen, über die in der Vergangenheit Erkenntnisse zu einer bestimmten Frage gesammelt wurden. Scoring basiert auf der Erwägung, dass bei Vorliegen bestimmter vergleichbarer Merkmale anderer Personen bei der gescorten Person ein ähnliches Verhalten oder ein ähnlicher Zustand vorausgesagt werden kann.[68] Der zunächst für die Bonitätsbewertung von Kunden etablierte Begriff wird inzwischen in den unterschiedlichsten Zusammenhängen verwendet. Ein Score kann auch ein Zahlenwert sein, der durch die Auswertung von Gesundheitsdaten zustande gekommen ist und wird so selbst zu einem Gesundheitsdatum.

Scoring unterscheidet sich von sonstigen informationstechnischen Bewertungen dadurch, dass keine eindeutigen, vorher definierte Datenzuordnungen vorgenommen werden, sondern vielmehr eine größere Anzahl von Merkmalen verwendet werden, deren Relevanz für die Feststellung der Wahrscheinlichkeit durch bisherige statistische Erfahrung festgelegt wird und variabel ist. Aus einem Score vorgenommene Ableitungen sind keine vorfestgelegten Wenn-dann-Entscheidungen, sondern basieren auf automatisierten Spekulationen. Datenschutzrechtlich ist das Scoring im Zusammenhang mit der Regulierung von automatisierten Entscheidungen von Bedeutung (Art. 15 EG-DSRl, § 6a BDSGaF, Art. 22 DSGVO, §§ 31, 37 BDSGnF), die auf der Grundlage von per Scoring berechneten Werten getroffen werden. Scoring ist ein Vorläufer und zugleich eine bestimmte Ausgestaltung von Big Data.

Das Scoring wurde im Rahmen der Bonitätsprüfung entwickelt und wird seit Jahren insbesondere bei der Kreditvergabe eingesetzt (s. u. 8.9).[69] Auch im Gesundheitsbereich finden solche Verfahren zur Unterstützung bei Entscheidungsprozessen in der Organisation von Behandlungen eine Rolle. Im Militärbereich ist die Triage ein spezifisches (ursprünglich militärisches) Auswahlverfahren, das letztlich auf einem Score begründet ist (s. u. 5.1). Für den medizinischen und den Versicherungs-Bereich hat jüngst das US-Unternehmen „Aspire Health“ ein Verfahren vorgestellt, mit dem aus ärztlichen Diagnosedaten als Score die prognostizierte Lebenserwartung errechnet wird.[70]

---

68 Korczak, Verantwortungsvolle Kreditvergabe, Gutachten im Auftrag des BMVEL, 2005, S. 29; Abel, RDV 2006, 108 f.; Hoeren, RDV 2007, 93.

69 Dazu ausführlich ULD/GP Forschungsgruppe, Scoring nach der Datenschutz-Novelle 2009 und neue Entwicklungen, 2014.

70 Soliman, Der Todesalgorithmus: Computer berechnet Lebenserwartung, daserste.ndr.de 14.12.2017; Welchering, Big-Data-Algorithmen – Wenn Software über Leben und Tod entscheidet, www.zdf.de 20.12.2017.

2.5 Profilbildung – Profiling

Profiling wird erstmals in **Art. 4 Nr. 4 DSGVO** normativ definiert als „jede Art der automatisierten Verarbeitung personenbezogener Daten, 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".

Der aus dem Englischen kommende Begriff lässt sich übersetzen mit Erstellung, Aktualisierung und Verwendung von **Datenprofilen natürlicher Personen**. Zielsetzung des Profiling kann es z. B. sein, Straftaten (durch sog. Profiler) oder Steuerhinterziehung zu ermitteln oder potenzielle Kunden für Werbezwecke gezielt anzusprechen (Direktwerbung, vgl. ErwGr 70 S. 1 DSGVO), ein bestimmtes Verhalten zu prognostizieren (z. B. Kreditrückzahlung, vgl. ErwGr 71 S. 1 DSGVO) oder die Eignung eines Kandidaten oder eines Stellenbewerbers zu bewerten.

Das mit Profiling umschriebene Vorgehen wurde schon früh von der Rechtsprechung des Bundesverfassungsgerichts (BVerfG) thematisiert, als es 1969 aus dem allgemeinen Persönlichkeitsrecht ein **Verbot der Erstellung totaler Persönlichkeitsbilder** ableitete: Es sei mit der Menschenwürde nicht vereinbar, „wenn der Staat das Recht für sich in Anspruch nehmen könnte, den Menschen zwangsweise in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren".[71] Für die freie Entfaltung der Persönlichkeit bedürfe es eines verbleibenden „Innenraums", in dem der Mensch „sich selbst besitzt" und „in den er sich zurückziehen kann, zu dem die Umwelt keinen Zutritt hat, in dem man in Ruhe gelassen wird und ein Recht auf Einsamkeit genießt". Bei der Integration automatisierter Informationssysteme entsteht demnach die Gefahr, dass Personendaten zu einem „teilweisen oder weitgehend vollständigen Persönlichkeitsprofil zusammengefügt" werden, „ohne dass der Betroffene dessen Richtigkeit und Verwendung zureichend kontrollieren kann".[72] Auch im privaten Bereich gilt das Verbot der zwangsweisen und heimlichen Erfassung, die auf die „Offenlegung wesentlicher Teile des Persönlichkeitsbildes gerichtet ist".[73] Nicht erst das Erstellen von Profilen, sondern auch die systematische Datensammlung zu einem Menschen, z. B. durch systematische Observation, wurde früh gerichtlich untersagt.[74]

Die praktische Bedeutung von Profiling hat mit der Entwicklung des **Big Data** zugenommen. Die Auswertung großer Datenmengen zu einer Person ermöglicht präzise und aussagekräftige Bewertungen und Prognosen, die zur Grundlage von ein Individuum betreffenden Entscheidungen genommen werden können. Dieser Zusammenhang wird

---

71 BVerfG 16.7.1969, 1 BvL 19/63, Mikrozensus, NJW 1969, 1707 = BVerfGE 27, 1 ff.
72 BVerfG 16.7.1969, 1 BvL 19/63, BVerfGE 27, 6.
73 BGH 3.5.1986, III ZR 233/84, NJW 1988, 3078; bzgl. Beschäftigten Däubler Rn. 428 ff.
74 Vgl. BVerwG 21.3.1986 – 7 C 73/84, NJW 1986, 2332.

künftig von Art. 22 DSGVO erfasst (s. u. 8.9).[75] Profiling erfolgt z. B., wenn ein Online-Dienstanbieter die Internetaktivitäten seiner Nutzer nachvollzieht und so ggf. „ein Profil des Betroffenen erstellt (…), das insbesondere die Grundlage für sie betreffende Entscheidungen bildet oder anhand dessen ihre persönlichen Vorlieben, Verhaltensweisen oder Gepflogenheiten analysiert oder vorausgesagt werden sollen“ (ErwGr 24 S. 2 DSGVO). Das Profiling zu einem Menschen wird technisch erleichtert durch „Online-Kennungen wie IP-Adressen und Cookie-Kennungen, die sein Gerät oder Software-Anwendungen und -Tools oder Protokolle liefern, oder sonstige Kennungen wie Funkfrequenzkennzeichnungen, (…) die Spuren hinterlassen, die insbesondere in Kombination mit eindeutigen Kennungen und anderen beim Server eingehenden Informationen dazu benutzt werden können, um Profile der natürlichen Personen zu erstellen und sie zu identifizieren“ (ErwGr 30 S. 2 DSGVO). Das Zusammenführen von einem Betroffenen zuzuordnenden Daten aus „smarten“ Geräten und Anwendungen (Kfz, Wearables, Smart Watches, Haushaltsgeräte) ist eine Grundlage für das Profiling.

Für das Profiling wesentlich ist das zielgerichtete Verknüpfen personenbezogener Daten, die logisch zueinander in Beziehung gesetzt werden, so dass dabei ein Bild oder Teilabbild entsteht unter qualifizierter Auswahl und Kombination der Daten aus verschiedenen Lebensbereichen oder Nutzungsvorgängen. Art und Umfang der Daten sowie Verwendungsweisen sind zwar nicht begriffsbestimmend für das Profiling, können aber das Gefahrenpotential für die Persönlichkeitsrechte der Betroffenen erhöhen.[76]

Persönlichkeitsprofile lassen sich entlang einer zeitlichen Entwicklung (Langzeitprofile, s. o. Tracking 2.3) oder als sektorenübergreifende Blitzaufnahme (Querschnittsprofile) erstellen. Langzeitprofile geben Antworten auf Fragen nach individuellen Einstellungen, Verhaltensweisen oder Eigenschaften, z. B. Krankheitsgeschichten. Querschnittsprofile fassen Informationen aus verschiedenen Lebensbereichen zusammen (z. B. über Familie, Gesundheit, Vermögen, Religion, Freizeit). Durch das Verbot von Langzeitprofilen soll verhindert werden, dass die Vergangenheit prägend für die Zukunft eines Menschen wird. Das Verbot von Querschnittsprofilen sichert das Ausfüllen unterschiedlicher sozialer Rollen. Es ist äußerst schwierig, eine objektive Grenze festzulegen, bei deren Überschreiten ein absolutes Verbot von Persönlichkeitsprofilen wirksam wird. Der Gefahr von Persönlichkeitsprofilen versuchte der Gesetzgeber – bisher mit beschränktem Erfolg – durch die Regelungen zu automatisierten Entscheidungen und zum Scoring Herr zu werden.[77]

2.6 Personalisierung – Personalizing

Personalisierung bezeichnet die nominelle Zuordnung von Merkmalen, insbesondere von per Big Data erstellten Analyseergebnissen, zu einer natürlichen Person und die Anpassung

---

75 Weichert in Reiffenstein/Blaschek S. 242 f.; kritisch Artikel-29-Arbeitsgruppe, zit. in ULD/GP Forschungsgruppe S. 161 f.; Schröder/Taeger, Scoring im Focus: Ökonomische Bedeutung und rechtliche Rahmenbedingungen im internationalen Vergleich, 2014, S. 138 ff.

76 Kühnl, Persönlichkeitsschutz 2.0, 2016, S. 20 f.; Theißen S. 84 ff.

77 ULD/GP Forschungsgruppe S. 172.

von Programmen, Diensten oder Informationen an deren persönliche Eigenschaften, Vorlieben, Bedürfnisse oder Fähigkeiten. Personalisierungen können individuell oder zu Personen mit einem oder mit mehreren gemeinsamen Merkmalen (gruppenbezogen) erfolgen. Sie basieren auf der merkmalsbezogenen Unterscheidbarkeit der Menschen durch Identifikatoren und Merkmalsmuster. Diese Merkmalsmuster basieren oft auf Profilen (s. o. 2.5).

Die Personalisierung kann in der **individuellen Anpassung** von Produktangeboten und Vertragsgestaltungen im Rahmen einer Kundenbeziehung (Customizing) bestehen, insbesondere in Form von informationstechnischen Angeboten im Online-Geschäft. Personalisierungen sind bei der Preisgestaltung bei Online-Angeboten, auch im Bereich der Gesundheit, weit verbreitet, wobei die vermutete, per Big Data bewertete Zahlungsbereitschaft ausschlaggebend ist.[78] Bei der Feststellung dieser Zahlungsbereitschaft ist der individuelle Bedarf an einem Produkt ein wesentlicher Faktor, der bei Gesundheitsleistungen vom Gesundheitszustand abhängig gemacht werden kann, wenn hierzu Daten verfügbar sind. Personalisierungen können aber auch in jedem anderen sozialen, politischen, beruflichen oder konsumbezogenen Zusammenhang vorgenommen werden.

Bei der **personalisierten Medizin** werden die Medikation oder sonstige Therapien an die individuelle medizinische oder genetische Disposition angepasst.[79] Durch spezifische Analysen z. B. des menschlichen Genoms wird die Empfänglichkeit für eine Behandlung untersucht und dadurch deren Wirkung verbessert. Bei der Krebsbehandlung hat sich gezeigt, dass Tumore auf einer Erbgutanalyse basierend wegen ihrer Unterschiedlichkeit individuell besonders wirksam behandelt werden können.[80] Je nach aufgefundenen Genmarkern kann die Wirkung von Arzneimitteln oder sonstigen Behandlungsmethoden stark voneinander abweichen. Das Prinzip „One drug fits all" ist oft unzutreffend. Nach einer tief gehenden individuellen Anamnese wird das Medikament oder die Therapie individuell gestaltet, wobei Big Data zum Einsatz kommen kann.[81]

Personalisierte bzw. individualisierte Medizin beschränkt sich nicht auf somatische Bio-Marker. Denkbar sind auch **Psycho- oder Soziomarker**, mit denen eine präzise zugeschnittene Therapie im Sinne einer „stratifizierten Medizin" gefunden und angewendet werden kann.[82]

---

78 Hoffmann, Schwer zu fassen, SZ 4.1.2018, 18; die Firma prudsys AG erhielt 2017 für ein entsprechendes Sofwareangebot den BigBrotherAward 2017 in der Kategorie Verbraucherschutz, bigbrotherawards.de/2017/verbraucherschutz-prudsys.

79 Rasmussen, Das vermessene Ich, Böll Thema 3/2012, 30 f.; Weichert ZD 2013, 255; Strategy/pwc S. 86 f.

80 Deutsches Krebsforschungszentrum, zit. bei Langkafel in Langkafel S. 27; Becker, Heilen mit Big Data, SZ 15.11.2016, 34.

81 Mahler, Jedem sein eigenes Medikament, Der Spiegel 28/2017, 80 f.

82 Langkafel in Langkafel S. 31 ff.

2.7 Prothetik

Prothetik ist die Entwicklung, die Herstellung und der Einsatz von nicht körpereigenen Werkstücken im oder am Körper. Eine zentrale Funktion von Prothesen ist der künstliche Ersatz für verlorene Organe oder Körperteile, wie eines Armes oder Beines.[83] 1958 wurde der erste Herzschrittmacher erfolgreich bei einem Patienten in Stockholm eingesetzt.[84] 2004 wurde VeriChip von der US-Gesundheitsbehörde FDA als Medizinprodukt zugelassen, ein reiskorngroßes RFID-Implantat zur Identifikation von Patienten.[85] Derartige Chips werden im Körper, z. B. zwischen den Fingern oder im Oberarm, implantiert und ermöglichen eine elektronische Identifizierung oder Authentisierung, wie sie im Gesundheitsbereich nützlich sein kann. Von Forschenden der University of California in San Francisco wurde ein kleines Gerät entwickelt, das im Körper implantiert wie eine stationäre künstliche Niere in der Lage ist, das Blut zu reinigen.[86] Es muss nicht um den Ersatz von menschlichen Körperfunktionen gehen, auch deren Erweiterungen oder Entlastungen (Orthetik) fallen unter den Oberbegriff. Analoge Prothesen können nur in sehr grober Weise Hilfe leisten. Mit digitalen Prothesen sind differenziertere Hilfen möglich. Voraussetzung ist in den allermeisten Fällen eine Mensch-Maschine-Schnittstelle, bei der medizinische und informationstechnische Funktionalitäten verknüpft werden.

2.8 Robotik

Während bei der Prothetik die (informationstechnisch gestützte) Hilfe direkt am oder im Köper ansetzt, agieren bei der Robotik eigenständige informationstechnische Systeme. Roboter im Gesundheitsbereich mit möglichem Big-Data-Bezug sind Operationsroboter, bei denen (evtl. auf Distanz und mit Sensoren ausgerüstet) der Operationsvorgang von einem Arzt geleitet wird. Roboter übernehmen zunächst routinemäßige, zunehmend aber auch komplexere Aufgaben. Dabei werden sie regelmäßig von Sensoren und einer komplexen Datenverarbeitung unterstützt. Es gibt Kleinstroboter, selbst im Mikro- und Nanobereich, die sich in einer festgelegten Art fortbewegen können und im Gesundheitsbereich zum Einsatz kommen. Das Stuttgarter Max-Planck-Institut hat jüngst einen 3,7 zu 1,5 Millimeter kleinen Silikon-Roboter präsentiert, der sich durch Magneten gesteuert im Körper eines Menschen auf unterschiedliche Weise fortbewegen kann und der mit Sensoren oder Wirkmedikamenten zur lokalen Anwendung ausgestattet werden kann.[87]

Roboter finden zunehmend im Pflegebereich Einsatz. Sie sind in der Lage, vielfältige vordefinierte Aufgaben eigenständig zu erfüllen, etwa das Umbetten und Waschen von Personen. Care-O-bot ist ein „intelligenter Pflegewagen“, der Ärzte oder Pfleger begleitet

---

83 Honey, Prothesen wie aus einem Star-Wars-Film, Kieler Nachrichten Wochenendjournal 14./15.10.2017, 6.

84 Theißen S. 1

85 Theißen S. 17 ff. mit vielen weiteren Beispielen von informations- und kommunikationstechnischer (IKT-) Implantaten.

86 Mobile Blutwäsche, Der Spiegel 42/2017, 104.

87 Schwenkenbecher, Krabbeln, klettern, schwimmen, SZ 25.1.2018, 14.

und für diese Assistenzfunktionen erfüllt.[88] Mario ist ein von der Universität Passau entwickelter Pflegeroboter, der auch zur Unterstützung von Dementen eingesetzt werden kann.[89] Paro ähnelt äußerlich einer jungen Robbe und dient als Kuschelroboter zur Betreuung insbesondere von Demenzkranken. Hobbit kombiniert Kommunikations-, Unterhaltungs-, Sicherheits- und Assistenzfunktionen und kann selbständig Aktivitäten auslösen, z. B. einen Notruf absetzen.[90] In Japan ist der Einsatz von Pflegerobotern wegen des hohen Pflegebedarfs v. a. älterer Menschen stark ausgeprägt.[91] Der Deutsche Ethikrat hat sich mit dem Einsatz von Pflegerobotern beschäftigt.[92] Pflegeroboter dokumentieren digital nicht nur ihre eigenen Tätigkeiten, sondern auch die Eingabedaten sowie die über Sensoren und Kommunikation erlangten Informationen von den betreuten wie von bedienenden oder dritten Personen.[93]

2.9 Künstliche Intelligenz

Künstliche Intelligenz (KI, englisch „artficial intelligence", AI) beschreibt informationstechnische Systeme, die versuchen menschliches „intelligentes" Verhalten nachzubilden und eigenständig Probleme zu lösen, indem automatisiert Lernprozesse (basierend auf Rückmeldungen aus der Umwelt, evtl. in Reaktion auf das vorangegangene Vorgehen) in eine Entscheidungsfindung integriert werden. Der populär und in der Wissenschaft verwendete Begriff hat bisher keinen Eingang in rechtliche Regulierungen gefunden.

Expertensysteme, mit denen digitale Informationen für die medizinische Behandlung bereitgestellt werden und mit denen z. B. die ärztliche Diagnose erleichtert oder abgesichert werden, gibt es schon seit 1976. Diese Systeme waren aber nicht lernfähig, sondern funktionierten nach dem Wenn-dann-Prinzip. Wissensbasierte Systeme der KI sind Expertensysteme, die in der Lage sind, auf Fragen eines Anwenders auf Grundlage formalisierten Fachwissens und von Erfahrungen und daraus gezogener logischer Schlüsse Antworten zu liefern, z. B. zur Diagnose von Krankheiten oder der Suche und Beseitigung von Fehlern in technischen Systemen. Es handelt sich um lernende Expertensysteme, die ihre Ergebnisse auf Grundlage von laufend hinzugesammelten Erfahrungsdaten zu verbessern suchen. Solche Verfahren des sog. „deep learning" gibt es seit den 80er Jahren.[94] Während zunächst die beschränkte Rechenkapazität noch Schranken setzte, brachte 2012 der Einsatz von Grafikkarten den Durchbruch. Heute sind neuronale Netze

88 Graf, Assistenzroboter zur Pflegeunterstützung, Vortrag 21.6.2017, http://www.ethikrat.org/dateien/pdf/jt-21-06-2017-graf.pdf.; Münch S. 45 f.
89 Leitgeb, Robo-Pfleger Mario, SZ 24.11.2017, 28.
90 Münch S. 47 f.
91 Becker, Maschinen für mehr Menschlichkeit, SZ 5.9.2017, 23.
92 Deutscher Ethikrat, Wie wird die Zukunft mit intelligenten Maschinen? PM 22.6.2017, https://www.presseportal.de/pm/42978/3666200.
93 Ausführlich zu Gesundheitsrobotern Münch S. 29 ff.
94 Deutscher Ethikrat S. 50 f.

im Einsatz.[95] Inzwischen ist es Entwicklern gelungen, KI-Technologie in einem Smartphone unterzubringen.[96]

Die selbstlernenden Systeme helfen Medizinern in Sekundenschnelle bei der Diagnose und der Wahl der Therapieform. 2015 kaufte IBM zwei Clouddienste aus dem Gesundheitssektor und ermöglichte damit den Zugang zu Millionen von Krankenakten, mit deren Daten, Texten und Bildern das KI-System Watson gefüttert wurde, und mit dem neue medizinische Erkenntnisse erlangt werden sollen.[97] Der Watson Oncology Advisor gibt Handlungsempfehlungen für Krebsbehandlungen; unter dem Namen Watson Discovery Advisor wird nach Verknüpfungen und medizinischen Zusammenhängen unter Auswertung von großen Mengen an Forschungsergebnissen insbesondere durch die Pharmaindustrie gesucht.[98] Das KI-Startup Sentient AI behauptet, dank KI die Blutvergiftung eines Patienten mit 91% Sicherheit eine halbe Stunde vor dem Auftreten der ersten Symptome bestimmen zu können.[99]

Generell und besonders im Gesundheitsbereich wird über die ethische Vertretbarkeit des Einsatzes von KI intensiv diskutiert. Es besteht aber weitgehend Einigkeit, dass der Einsatz solcher Systeme dort nicht nur sinnvoll, sondern geboten ist, wo KI eine Aufgabe plausibel begründbar besser erledigt als der Mensch. Dies wird z. B. für die Auswertung von bildgebenden Verfahren angenommen, bei denen auf das digitale Erfahrungswissen von Massenuntersuchungen zurückgegriffen wird, etwa bei der Diagnose von Hautkrebs anhand von Fotos, von Brustkrebs anhand von Röntgenaufnahmen oder bei der Diagnose der Retinopathie, die oft mit Diabetes einhergeht, durch Analyse der Bilder der Netzhaut. Entsprechendes gilt für die Überwachung von EKG-Werten von Herzpatienten auf Rhythmusstörungen.[100] Bei komplexen, digital schwer erfassbaren, sich noch im experimentellen Stadium befindlichen Verfahren erweist sich der KI-Einsatz als problematisch.[101] Dies gilt in besonderem Maße für Prozesse, bei denen Empathie gefordert ist; dies ist im Gesundheitsbereich oft der Fall.

Das Instrument der KI kann sowohl zum Guten wie auch gezielt für Böses genutzt werden. So zeigt sich, dass mit Hilfe von KI Hackingangriffe erkannt und abgewehrt werden können. Hacker können das Instrument der KI aber auch nutzen, um ihre Angriffsmethoden weiterzuentwickeln.[102] Derartige Angriffe erfolgen zunehmend auch im Gesundheitsbereich (s. u. 5.1).

---

95 Timm MedR 2016, 689 f.

96 Martin-Jung, Das Intelligente Handy, SZ 17.10.2017, 26.

97 Braun, Dr. KI, zur Visite bitte! SZ 14.09.2017, 18.

98 BITKOM, Kognitive Maschinen – Meilenstein in der Wissensarbeit, Leitfaden, 2015, S. 77, 81 f.

99 Bouée, Eine Chance für Europa, SZ 13.11.2017, 18.

100 Deutscher Ethikrat S. 48 f., 51.; Dworschak, Dumm wie ein Sieb, Der Spiegel 2/2018, 105, Martin-Jung, Gesunder Verstand, SZ 19.1.2018, 39, jeweils mit Hinweisen auf die Begrenztheit von KI.

101 Martin-Jung, Die Maschine und ich, SZ 18./19.11.2017, 25.

102 Frenkel, Hacker´s ´Ideal Testing Ground´, The NewYork Times International selected for SZ 7.7.2017, 1.

Die Ergebnisse, die KI hervorbringt, werden maßgeblich von den einfließenden Trainingsdaten beeinflusst. Sind diese Daten mit einem Vorurteil behaftet, so wird auch das KI-Ergebnis regelmäßig dieses Vorurteil bedienen, was bei Übernahme dieser Ergebnisse zur Diskriminierung führt. Computersystemen und auch KI fehlt die menschliche Fähigkeit, Rückschlüsse zu ziehen. Der Mensch hat eine Vorstellung von der Welt, die einem Computer auch über KI nicht vermittelt werden kann. Emmanuel Mogenet, der Forschungsleiter von Google in Europa, wird wie folgt zur KI zitiert: „Ich kann nicht behaupten, dass wir genau wüssten, wie Generalisierung wirklich funktioniert."[103]

3 Verarbeiter von Gesundheitsdaten

Datenquellen mit Gesundheitskontext sind vielfältig.[104] Im Folgenden werden die Stellen bzw. Funktionen benannt, die typischerweise Gesundheitsdaten generieren, speichern und nutzen und die deshalb als Datenlieferanten, als Anwender oder als Nutzer von Big Data im Gesundheitsbereich in Frage kommen.[105] Grundsätzlich ist der Einsatz von Big Data bei allen genannten Gruppen denkbar. Es bestehen aber technische Grenzen hierfür; es fehlt oft noch an Datenquellen, Software, Vernetzung und Know-how. Dies wird sich mit dem weiteren technischen Fortschritt ändern.

In seiner Stellungnahme „Big Data und Gesundheit – Datensouveränität als informationelle Freiheitsgestaltung" von November 2017 differenziert der Deutsche Ethikrat zwischen fünf Akteursgruppen mit unterschiedlichen Funktionen und zumindest teilweise gegenläufigen Interessen: 1. biomedizinische Forschung, 2. Gesundheitsversorgung, 3. Versicherer und Arbeitgeber, 4. kommerzielle Verwertung durch global agierende IT- und Internetfirmen und 5. die Betroffenen selbst.[106] Der Technikeinsatz bei den jeweiligen Stellen ist äußerst unterschiedlich ausgeprägt.

Hinsichtlich der von den jeweiligen Stellen verfolgten primären Zwecke können die folgenden Handlungsfelder unterschieden werden, wobei eine Stelle regelmäßig mehrere Zwecke zugleich verfolgt: 1. Behandlung und Pflege, 2 Gesundheitserziehung und -information, 3. finanzielle Abwicklung und Ressourcenoptimierung, 4. Öffentliches Gesundheitswesen und Monitoring, 5. Prävention, 6. Kommunikation, 7. Kontrolle durch Aufsicht (regulators), 8. Produkt(weiter)entwicklung, 9. Prognose und Organisationsentwicklung, 10. Forschung.[107]

Hinsichtlich der Analysefragestellungen kann zwischen zwei Dimensionen unterschieden werden:

---

103 Martin-Jung, Gorillas und Badewannen, SZ 22.11.2017, 24.
104 Systematischer Überblick bei Strategy/pwc S. 62 ff.
105 Zu den Erwartungen generell Deutscher Ethikrat S. 143 ff.
106 Deutscher Ethikrat S. 11, 68 f; Strategy/pwc S. 55 ff.
107 Ähnlich Langkafel in Langkafel S. 16 ff.

- Bei einer horizontalen Betrachtung steht das Individuum mit seinem gesundheitsrelevanten Verhalten, seiner Befindlichkeit und der Behandlungskette im Vordergrund.

- Die vertikale Betrachtung hat die individuumsübergreifende Gesamtbetrachtung eines konkreten Phänomens im Blick.

Für beide Dimensionen ist die zeitliche Bezugnahme (Was war? Was ist? Was wird sein?) von hoher analytischer Relevanz.[108]

3.1 Medizinische Leistungserbringer: Ärzte, Krankenhäuser, Apotheken u. a.

Die Heilberufe, bei denen zumeist kranke Menschen eine mehr oder weniger intensive Untersuchung und eine Behandlung erfahren und deren Ergebnisse in Krankenakten dokumentiert werden, sind wohl immer noch die Stellen, die heute die meisten und qualifiziertesten Gesundheitsdaten erfassen, speichern und verarbeiten. Die im direkten Patientenkontakt ambulant oder stationär erhobenen Daten werden in Arzt- oder Krankenhausinformationssystemen digital gespeichert. Sie werden von Apotheken, Laboren, Heil- und Pflegediensten bis hin zu Hospizeinrichtungen[109] unterstützt, die ebenfalls zu Dokumentationen verpflichtet sind.

Bei ambulanten Arztpraxen hat sich eine umfassende Digitalisierung unter Einschluss der Patientendokumentation erst relativ spät durchgesetzt. Die elektronische Abrechnung wurde in Deutschland dagegen mit der Krankenversichertenkarte schon im Jahr 1995 eingeführt. Bei Hausärzten erfolgte der Umbruch später als bei Facharztpraxen. Inzwischen verfügt jede Praxis über ein Arztinformationssystem (AIS) und zumeist über weitere digitale Fachanwendungen. Die Beschaffung und den Betrieb des AIS refinanzieren ambulante Ärzte teilweise durch die Weitergabe von (teilanonymisierten) Verordnungsdaten an für deren Aufbereitung spezialisierte Firmen (s. u. 4.8).[110] Die Ärzte greifen auf externe oder im System integrierte Expertensysteme zurück, deren Inhalte zumeist auf Big-Data-Analysen beruhen.

Während eigenes Big Data im ambulanten Bereich selbst noch die Ausnahme ist, haben solche Verfahren in den Krankenhäusern inzwischen Eingang gefunden und setzen sich immer weiter durch.[111] Wegen des hohen Kostendrucks im Krankenhausbereich spielen Anwendungen zur Qualitäts- und Wirtschaftlichkeitskontrolle eine große Rolle (s. u. 4.3, 4.4). Mit Hilfe der Ergebnisse sollen Schwachstellen erkannt und behoben werden, Freiräume besser genutzt und Logistikketten optimiert werden.[112] Im Bereich der Behandlung stehen zunächst eindimensionale Auswertungen im Vordergrund, etwa die

108 Ähnlich Langkafel in Langkafel S. 18 ff.
109 Von Reumont, Ambulante Hospizvereine und Datenschutz, DANA 2010, 112 ff.
110 Kamps in Langkafel S. 76.
111 Langkafel in Langkafel S. 24 f.
112 Laslo in Langkafel S. 193 ff.

massenhafte Analyse von Bilddaten, z. B. aus der Radiologie.[113] Eine weit verbreitete Big-Data-Anwendung ist die Risikobewertung bei Medikamenteninteraktion bzw. die Feststellung von Verträglichkeiten durch einen automatisierten Medikamentencheck (s. u. 10.2).[114] Zunehmend finden komplexe Systeme Anwendung, bei denen strukturierte und unstrukturierte Daten aus unterschiedlichen Quellen und mit unterschiedlichen Fragestellungen ausgewertet werden. So will die US-amerikanische Klinikkette Mayo ihr Ziel, im Jahr 2020 mehr als 200 Mio. Patienten jährlich zu behandeln, dadurch verwirklichen, dass sie ihr Internetangebot der Fernbehandlung ausbaut und hierbei automatisierte Datenerhebung und -auswertung nutzt.[115] An der Cornell-Universität in Ithaca/USA wurde in die Kleidung eingenähte Sensorik entwickelt, die laufend Atemfrequenz, Puls oder Blutdruck der Patienten überwacht, die die Ergebnisse per RFID-Chip über Antennen in den Zimmern von Krankenhäusern und Pflegeheimen an die Behandlungsdokumentation und im Notfall an die Stationsleitung sendet.[116]

Die Digitalisierung des medizinischen Behandlungsgeschehens ist dort am weitesten fortgeschritten, wo sie einen direkten Nutzen für den Behandler bringt oder der Erfüllung gesetzlicher Anforderungen dient, etwa bei der Abrechnung oder der Wirtschaftlichkeits- und Qualitätskontrolle. Defizite bestehen im Hinblick auf die Bereitstellung für die Betroffenen und Dritte und auf Nutzungsmöglichkeiten im Interesse des Gemeinwohls. Dessen ungeachtet kann die zeit- und ortsunabhängige Bereitstellung von Patientendaten zu einem wichtigen Kriterium eines effizienten modernen Gesundheitswesens werden.[117]

Die Angehörigen der Heilberufe sind im Interesse der Nachvollziehbarkeit des Behandlungsgeschehens und des Krankheitsverlaufs zur Dokumentation verpflichtet (z. B. § 10 MBOÄ). Diese erfolgt in der Patientenakte, die zunehmend in elektronischer bzw. digitalisierter Form geführt wird (eAkte, elektronische Patientenakte – EPA, vgl. § 291a Abs. 3 S. 1 Nr. 4 SGB V). Dabei wird je nach Verantwortlichkeit, Zugriffsmöglichkeit und Referenz zwischen verschiedenen Typen unterschieden: Die institutionelle EPA führt alle Informationen zu einem Patienten zusammen, die in der aktenführenden Institution (z. B. Krankenhaus, ambulante Arztpraxis) selbst erhoben oder dorthin übermittelt wurden. Enthalten sind sowohl abrechnungsrelevante wie auch umfassend sämtliche behandlungsrelevanten Informationen (Diagnosen, Prozeduren, Verweildauern,

113 Lepies, Künstliche Intelligenz in der Medizin: „Wir wollen Ärzte nicht arbeitslos machen“, www.heise.de 7.9.2017; Deutscher Ethikrat S. 70.

114 Ludwig, Computer sagt Nein, SZ 11.12.2017, 23; Deutscher Ethikrat S. 70; die Gesundheitsschädlichkeit des Medikaments „vioxx“ soll erst durch Computeranalyse von 17.000 Krankenakten ermöglicht worden sein, vgl. Ladeur DuD 2016, 363 Fn. 32.

115 Müller, App auf Rezept, Der Spiegel 29/2017, 69.

116 Digitalkittel, SZ 28.11.017, 18.

117 Pfeiffer, Gesundheitskarte und Telemedizin – Beispiele für die Digitalisierung, ZBW – Leibnitz-Informationszentrum Wirtschaft, Wirtschaftsdienst 2017 (10) 697.

Laborwerte, Medikationen, Pflegedokumentation, bildgebende Verfahren, Befunde). Die elektronische Fallakte beschränkt sich dagegen auf einen Behandlungsvorgang (Fall).[118]

Bei der einrichtungsübergreifenden Patientenakte erfolgt eine umfassende Dokumentation des gesamten Behandlungsgeschehens zu einer Person bei unterschiedlichen medizinischen Leistungserbringern bzw. Gesundheitsdiensteanbietern (z. B. Ärzten, Physiotherapeuten, Apothekern). Sie wird entweder bei einer zentralen Stelle oder einem der Leistungserbringer auf Einwilligungsbasis des Patienten geführt und steht grds. für alle einbezogenen Anbieter bereit und unterstützt deren integrierte Versorgung.[119] Die Techniker Krankenkasse hat in Kooperation mit großen Krankenhäusern und IBM eine solche elektronische Patientenakte entwickelt, auf die Patienten über eine App auch mit ihren Smartphones zugreifen können.[120] Vergleichbare Pläne verfolgt der AOK-Bundesverband, der über eine digitale Akte die verschiedenen Leistungserbringer miteinander vernetzen will.[121]

Im Projekt epSOS (European Patients Smart Open Services), das offiziell 2014 abgeschlossen wurde, wird das Ziel verfolgt, die nationalen eHealth-Systeme in Europa kompatibel bzw. interoperabel zu machen, indem Notfalldatensets, elektronische Patientendossiers und elektronische Rezepte gemäß gemeinsamen Standards institutions- und länderübergreifend digital verarbeitbar gemacht werden. Damit werden Big-Data-Auswertungen einfacher durchführbar (sog. data cleansing).[122] Daneben gibt es weitere Nomenklaturen bzw. Standards, z. B. ICD (International Code of Diseases), SNOMED CT (Systematische Nomenklatur der Medizin). Derartige Standards zielen aber i. d. R. nicht vorrangig auf Kommunikation und Big-Data-Auswertungen, sondern verfolgen andere Zielsetzungen, z. B. die standardisierte Kostenabrechnung.[123] HL7 (Health Level Seven) ist ein internationaler Datenstandard, der mit Spezifikationen für die Darstellung von Daten die Kommunikation zwischen Gesundheitsinstitutionen erleichtern soll. Gemeinnützige Organisationen wie das Clinical Data Interchange Standards Consortium (CDISC) setzen auf Standards für den Datenaustausch im Bereich klinischer Studien.[124]

Neben von Institutionen geführten Patientenakten gibt es solche, die vom Patienten selbst verwaltet werden (vgl. § 291a Abs. 3 S. 1 Nr. 5 SGB V), während die Einspeisung von den medizinischen Einrichtungen vorgenommen wird. Solche Patientenakten werden zumeist

118 Bergh/Brandner/Kutscha/Heinze/Schreiweis in Stiftung Datenschutz (2017) S. 13 ff.; Lux/Breil, Digitalisierung im Gesundheitswesen: bessere Versorgungsqualität trotz Kosteneinsparung, ZBW – Leibnitz-Informationszentrum Wirtschaft, Wirtschaftsdienst 2017 (10) 688.

119 Haas, Elektronische Patientenakten, 2017, https://www.bertelsmann-stiftung.de/de/publikationen/publikation/did/elektronische-patientenakten/.

120 Becker, Digitale Akte, SZ 17.8.2017, 17.

121 AOK will digitales Netz für Versicherte ausbauen, www.heise.de 10.10.2017.

122 Raum in Stiftung Datenschutz (2017) S. 127; Ladeur DuD 2016, 361.

123 Raum in Stiftung Datenschutz (2017) S. 136.

124 Deutscher Ethikrat S. 64 f.; Strategy/pwc S. 133 ff.

um von Patienten initiierte (z. B. von Wearables stammende) oder selbst vorgenommene Eintragungen (z. B. Tagebuch) ergänzt (s. u. 3.18).[125]

Die technische Entwicklung ermöglicht es, dass der direkte Heilbehandler-Patient-Kontakt durch digitale Kommunikation ergänzt und teilweise ersetzt wird. Wearables und andere Sensorgeräte, die im Alltag vom Patienten mitgeführt werden, ermöglichen es den Heilberufen, orts- und zeitunabhängig Untersuchungsdaten zu beschaffen. Das Arzt-Patienten-Gespräch wird durch Telehealth-Anwendungen über ferne Distanzen ermöglicht, bei dem durch Sensoren oder bildgebende Verfahren qualitativ mit einem Direktkontakt vergleichbare Ergebnisse erreicht werden können.[126] Es gibt sog. „epidermal electronics", auf die Haut aufgebrachte Pflaster oder Tattoos, mit denen z. B. in Echtzeit ein Wundheilprozess nach chirurgischen Eingriffen überwacht wird.[127] Mit Hilfe von über Smartphones erfassten Bildern lassen sich auf die Distanz Hauterkrankungen diagnostizieren, wobei unterstützende mit KI trainierte Bilderkennung zum Einsatz kommen kann. Der Einsatz solcher medizinischer Kommunikationsformen bewirkt eine starke Zunahme an behandlungsrelevanten Daten, die teilweise schon standardisiert digital vorliegen und die sich so für automatisierte Auswertungen geradezu aufdrängen.

3.2 Informationstechnische Dienstleister

Das Personal von medizinischen Leistungserbringern verfügt i. d. R. nur über begrenzte informationstechnische (IT-) Kompetenzen. Wegen der Notwendigkeit des Einsatzes von Informationstechnik bei der Erbringung medizinischer Leistungen müssen zumeist die Dienste externer spezialisierter Anbieter in Anspruch genommen werden. Inzwischen gibt es für die verschiedensten Heilberufsgruppen IT-Produkte, die an die jeweiligen Erfordernisse und Rahmenbedingungen angepasst sind und die ohne vertiefte technische und rechtliche Durchdringung zum Einsatz gebracht werden können. Die Einrichtung und insbesondere die Pflege (Administration, Aktualisierung, Wartung) dieser Produkte bringen es mit sich, dass operative (personenbezogene) Daten der medizinischen Leistungserbringer bei den informationstechnischen Dienstleistern verarbeitet werden, ja manchmal verarbeitet werden müssen. Das über Jahre hinweg ungelöste Problem, wie dieser Umstand in Deutschland mit der beruflichen Schweigepflicht in Einklang gebracht werden kann, wurde zum Ende der 18. Legislaturperiode durch eine Einbeziehung der IT-Dienstleister in die ärztliche oder sonstige berufliche Schweigepflicht im Grundsatz gelöst.[128]

---

125 Bergh/Brandner/Kutscha/Heinze/Schreiweis in Stiftung Datenschutz (2017) S. 16 ff.; kritisch zur Aufnahme von Daten aus Gesundheits-Apps Montgomery, PM Bundesärztekammer 7.6.2016.

126 Wälterlin, Fern-Diagnosen, SZ 17.10.2017, 18; Überblick über die Telemedizin bei Strategy/pwc S. 100 ff.

127 Gesundheitssensoren – auf die Haut aufgedruckt, DANA 2013, 76 f.; Sensorpflaster zum Aufkleben, DANA 2012, 40.

128 Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen v. 30.10.2017, BGBl. I S. 3618; dazu Dierlamm/Ihwas BB 2017, 1097 ff.; Hartung/Steinweg, DB 2017, 2081 ff.; Ruppert K&R 2017, 609 ff.; Wronka RDV 2017, 129.

Die IT-Dienstleister haben über die personenbezogenen Daten aus den Gesundheitsberufen in der Regel keine rechtliche Verfügungsbefugnis, da diese Daten im Auftrag der medizinischen Leistungserbringer verarbeitet werden (§ 11 BDSG, Art. 28 DSGVO). Sie sind deshalb für sie auch für Big Data nicht direkt zugänglich. Die IT-Anbieter dürfen die Daten nur im Rahmen des jeweiligen Auftrags und nach Weisung der medizinischen Leistungserbringer verarbeiten. Dies hindert aber Anbieter z. B. von Arzt- (AIS), Apotheken- oder Krankenhausinformationssystemen (KIS) in der Praxis nicht, die Daten weitergehenden Auswertungen zuzuführen, nachdem diese angeblich wirksam anonymisiert worden sind (s. u. 4.8). Über die konkrete Praxis der Anonymisierung liegen allgemein verfügbar bei fast sämtlichen Verfahren keine belast- und prüfbaren Informationen vor.

3.2.1 Stationärer Bereich

Im Bereich der Krankenhäuser sind die bestehenden Marktkonzentrationen bei den IT-Anbietern für die Auswertbarkeit der verfügbaren Daten förderlich. Sieben Anbieter teilen sich den Markt der Krankenhausinformationssysteme (KIS) weitgehend auf. Marktführer ist Agfa Healthcare mit seinem KIS Orbis, dem Bildarchivierungs- und Kommunikationssystem (PACS) Impax und den Dokumentenmanagementsystemen HydMedia und Agfa Managed Services. Cerner hat 2015 die Gesundheits-IT von Siemens gekauft und wurde so mit der Präsenz in über 500 Krankenhäusern zum zweitgrößten KIS-Anbieter in Deutschland. Die CompuGroup als führender Hersteller von Praxissoftware (s. u. 3.2.2) betätigt sich seit 2008 als KIS-Anbieter und hat durch Aufkäufe anderer Anbieter mit seinem CGM Clinical große Marktmacht erlangt. I-Solutions Health weist ca. 770 Installationen vorwiegend im deutschen Raum auf und präsentiert sich als konzernunabhängiges mittelständiges Unternehmen. Die inhabergeführte Meierhofer AG hat ca. 250 Einrichtungen in Deutschland, Österreich und der Schweiz als Kunden. Nexus war laut eigenen Angaben 2016 in Deutschland 232 Mal und weltweit 462 Mal vertreten. Die seit 2010 im Gesundheitsmarkt aktive Deutsche Telekom ist Marktführerin im Bereich SAP in Krankenhäusern und mit seinem KIS iMedOne in über 200 Kliniken vertreten.[129]

3.2.2 Ambulanter Bereich

Bei den Arztinformationssystemen (AIS) gibt es zwar eine Vielzahl (ca. 150) von Anbietern, doch besitzen die Compu Group Medical Deutschland AG (CGM) mit 31.9% und den vier Softwareangeboten Medistar, Turbomed, Albis, Compumed M1 den größten Marktanteil. Dem folgt die medatixx GmbH&Co KG aus der Merkle-Gruppe mit fünf Angeboten (u. a. x.isynet, x.concept, x.comfort) und einem Marktanteil von ca. 17%. Die beiden Unternehmen sind mit sieben unter den 10 meistverwendeten Anwendungen marktdominierend. Es folgen Psysprax (8%), Hasomed (7%) sowie Agfa Healthcare und Frey mit jeweils 3%.[130]

---

129 Die Top 7 KIS-Anbieter 2017, www.kna-online.de 7.4.2017.

130 Kassenärztliche Bundesvereinigung, Installationsstatistik – Systeme, Stand 31.12.2016, http://www.kbv.de/media/sp/Gesamt_Systeme_Installationen.pdf.

Der Marktführer CompuGroup ist mit Lauer-Fischer auch im Apothekenbereich aktiv. Die Ärzte, die Produkte der CGM einsetzen, erhalten wirtschaftliche Vergünstigungen dafür, dass die angeblich anonymisierten, tatsächlich pseudonymen Datensätze mit Angaben zu Diagnosen und Arzneimitteln an IMS Health (IQVIA) weitergeben werden (s. u. 4.8). Möglich ist auch, dass von der CGM Daten aus den Arztrechnern zu spezifischen medizinischen Fragestellungen über Einzelabfragen abgezogen werden.

Medatixx mit Sitz in Eltville gehört ebenso wie z. B. die Phoenix-Tochter ADG zum Merckle-Konzern (ratiopharm). In 22.300 Praxen finden sich deren Softwarelösungen. Diese wurden und werden weiterhin sehr günstig der Ärzteschaft angeboten. Dies mag früher auf spezifische Arzneimittelempfehlungen zurückzuführen gewesen sein und gilt heute weiterhin wegen der Weiternutzungsmöglichkeiten der erlangten Daten für pharmazeutische Auswertungszwecke. Zwischen Medatixx und IBM besteht eine strategische Partnerschaft, worüber die aus den AIS erlangten Daten bei Watson einfließen und zur KI-Optimierung genutzt werden. Medatixx setzt vermehrt auch auf Health-Apps. So gibt das Unternehmen die Patientenservice-App X.Patient heraus, die durch eine Verbindung mit der Praxis-Software die Kommunikation zwischen Arzt und Patient vereinfachen soll, etwa zur Übermittlung von Gesundheitsdaten an die Praxis oder zur Anforderung von Folgerezepten. Weitere App-Angebote sind die Diabetiker-App MySugar oder Preventicus Heartbeat, über die mittels Kamera der Puls gemessen und an den Arzt übermittelt werden kann.[131]

3.2.3 Apotheken

Zur informationstechnischen Unterstützung der GKV-Abrechnung von Apotheken gibt es in § 300 Abs. 2 SGB V eine Spezialregelung. Diese erlaubt die Einschaltung von Rechenzentren durch die Apotheken und zweckbezogene Datenübermittlungen an ausdrücklich genannte Stellen. Die Apothekenrechenzentren dürfen gemäß Satz 2 dieser Regelung anonymisierte Abrechnungsdaten auch „für andere Zwecke“ verarbeiten und nutzen. Hintergrund dieser Regelung war, dass die Apothekenrechenzentren die strukturiert erlangten Daten gerne für eigene kommerzielle Zwecke nutzen wollten. Derartige Rechenzentren gibt es in Berlin (Rechenzentrum Berliner Apotheken Neuhagen), Bremen (NARZ/AVN)[132], Darmstadt (arz), Datteln (ALG), Haan (ARZ), München (VSA),[133] Schwerin (SARZ)[134] und Starnberg (Digitales Rezept Zentrum).[135]

Alle Apothekenrechenzentren bieten den ihnen angeschlossenen Apotheken als IT-Dienstleistung nicht nur die Rezeptabrechnung an, sondern eine Vielzahl weiterer Services einschließlich Datenanalysen. Historisch bedingt und durch die Verknüpfung mit den Apothekerverbänden haben die Rechenzentren räumliche Schwerpunkte, bieten ihre Dienste aber grundsätzlich bundesweit an. Die zur Noventi-Group gehörende VSA in

131 Schneider, Medatixx: Apps von der ADG-Schwester, apotheke-adhoc.de 1.12.2017.
132 Norddeutsches Apothekenrechenzentrum – NARZ.
133 VSA GmbH, www.vsa.de.
134 Schweriner Apotheken Rechenzentrum GmbH, www.sarz.de.
135 http://www.digitales-rezept-zentrum.de.

München ist Marktführerin bei den Apothekenrechenzentren. Sie rechnet nach eigenen Angaben jährlich über 150 Mio. Rezepte mit einem Volumen von mehr als 12 Mrd. € ab.[136] Das seit 2017 auch zur Noventi-Group gehörende SARZ Schwerin hat Außenstellen in Berlin und Erfurt. Es bietet die FiveRX-Schnittstelle sowie die Apothekensoftware ApoOnline V4 an, mit der arzt-, arzneimittel- und kassenbezogene Auswertungen möglich sind. Zur Noventi-Group gehört weiterhin das ALG Datteln. Das arz in Darmstadt hat den räumlichen Schwerpunkt Hessen, Rheinland-Pfalz, Thüringen und Saarland. Mit 2.500 Apotheken als Kunden rechnet es jährlich ca. 60 Mio. Rezepte mit einem Wert von ca. 4,2 Mrd. € ab.[137] Das ARZ in Haan gibt einen Rezeptumsatz von ca. 7,5 Mrd. € aus ca. 85 Mio. Verschreibungen an. Das Digitale Rezept Zentrum in Starnberg ist ein Tochterunternehmen der Pharmatechnik GmbH. Das Norddeutsche Apothekenrechenzentrum (NARZ/AVN) in Bremen hat seinen Schwerpunkt in Norddeutschland und mit jährlich ca. 96 Mio. Rezepten eine Apothekenumsatz von ca. 7,5 Mio. €.[138]

Über viele Jahre hinweg erfolgte eine Nutzung der von Apotheken gelieferten Daten, ohne eine, wie gesetzlich gefordert, hinreichende Anonymisierung.[139] Nach Medienberichten und intensiven datenschutzaufsichtlichen Prüfungen wurde die Praxis umgestellt, wobei aber einige Apothekenrechenzentren, u. a. die bayerische VSA GmBH – geduldet von ihrer Datenschutzaufsicht – weiterhin mit einem sog. Patientenanonym pseudonymisierte Einzeldatensätze kommerziell vermarkten. Hierbei handelt es sich nicht um die vom Gesetz geforderte Anonymisierung (s. u. 8.12.1). Dessen ungeachtet erfolgt – soweit ersichtlich – diese unzulässige Datennutzung bis heute, insbesondere durch Weitergabe an medizinische Marktforschungsunternehmen (s. u. 4.8). Dies schließt umfangreiche Big-Data-Anwendungen mit ein, für die, legitimiert durch die „Anonymisierung", keine datenschutzrechtlichen Beschränkungen mehr bestehen sollen.[140] Das einzige Rechenzentrum, das überprüfbar eine gesetzesmäßige Anonymisierung vor einer Weitergabe seiner Daten vornimmt, ist das NARZ in Bremen.[141]

Auf der Basis von § 300 SGB V übermitteln die Apothekenrechenzentren Einzeldatensätze zu Verordnungsabrechnungen über Avoxa als einen zweiten Anonymisierungsdienst, der die Daten zugleich poolt, an das Deutsche Apothekenprüfungsinstitut e. V. (DAPI) in Berlin. Mitglieder des DAPI sind die Landesapothekenkammern und -verbände sowie einzelne Apotheken. Die Aufgabe von DAPI besteht darin, die im DAPI-Rechenzentrum in Aachen

136 http://www.noventi.de/marken-in-aktion/vsa-gmbh/.

137 http://www.arz-darmstadt.de/unternehmen/unternehmensportrait/.

138 https://www.narz-avn.de/de/ueber-uns/historie/.

139 37. Jahresbericht (2015), Die Landesbeauftragte für Datenschutz Freie Hansestadt Bremen, Kap. 6.5 (S. 33).

140 BayLDA 5. Tätigkeitsbericht 2011/2012 Kap. 14.4 (S. 74); ULD; ausführlich den Konflikt darstellend Kauß in Plöse/Fritsche/Kuhn/Lüders, „Worüber reden wir eigentlich?" Festgabe für Rosemarie Will, 2016, S. 591 ff.; vgl. Kühling/Klar NJW 2013, 3601 ff.; Weichert DuD 2013, 130; Kircher in Kingreen/Kühling S., 246 f.; die Rspr. weigerte sich bei dem Konflikt, sich mit der zentralen Frage der Anonymisierung auseinanderzusetzen, vgl. Weichert DuD 2015, 323 ff., 397 ff.

141 Klein, NARZ und IMS Health schließen Vergleich, www.deutsche-apotheker-zeitung.de 7.1.2014.

gespeicherten Daten auszuwerten und zu analysieren. Folgende Daten werden u. a. an DAPI weitergegeben: Geburtsjahr des Patienten, Krankenkasse, Versichertenstatus (z. B. Mitglied, Familienversicherter, Rentner), KV-Region des verschreibenden Arztes (entspricht etwa Bundesland), Datum der Verordnung, Abgabedatum in der Apotheke, „Pharmazentralnummer" (PZN), mit Angaben zu Größe, Verabreichungsform, Zusammensetzung, Preise und spezielle Verordnungsumstände (Arbeitsunfall, Notdienst). DAPI ist ein Forschungszentrum für Pharmakoepidemiologie und -vigilanz im European Network of Centres for Pharmacoepidemiology and Pharmacovigilance (ENCePP). Das Projekt ENCePP der Europäischen Arzneimittel-Agentur (European Medicines Agency - EMA) in London verfolgt das Ziel, die Erforschung des Arzneimittelgebrauchs nach der Zulassung zu verbessern (s. u. 10.2).[142]

3.3 Kommunikations-Infrastruktur

Erhobene Daten müssen, um gespeichert, ausgewertet oder sonst wie genutzt werden zu können, zumeist transportiert werden. Hierfür bedarf es bei digitalen Daten einer Netzinfrastruktur. Es gibt unterschiedliche im Gesundheitsbereich zum Einsatz kommende Telekommunikationssysteme. Kommunikationswege sind das klassische Telefonnetz (Telefax, Telefonie), das inzwischen weitgehend internetbasiert ist, sowie direkt das Word Wide Web. Das Internet hat sich inzwischen als die allgemeine Kommunikations-Infrastruktur durchgesetzt, die auch im Gesundheitskontext genutzt wird. Daneben bestehen organisationsinterne wie -übergreifende spezifische Netze, wie z. B. regionale Ärztenetze[143], von den Kassenärztlichen Vereinigungen organisierte Strukturen (KV-Safe-Net)[144] und eigene oder virtuelle Netze zwischen ausgewählten Behandlungs- oder z. B. Forschungseinrichtungen (z. B. Deutsches Forschungsnetz DFN).[145]

Als umfassendes Netzwerk zum Austausch von sensitiven Gesundheitsdaten wird derzeit die Telematik-Infrastruktur mit der elektronischen Gesundheitskarte (eGK) der gesetzlichen Krankenversicherungen (GKV) durch die „Gesellschaft für Telematikanwendungen der Gesundheitskarte" (gematik) aufgebaut. Die eGK wurde erst zum 1.1.2015 verbindlich eingeführt; der Gesetzgeber hatte mit dem GKV-Modernisierungsgesetz[146] eigentlich einen Beginn schon zum 1.1.2006 vorgesehen. Als Anwendungen sind in dieser Infrastruktur vorgesehen: 1. Notfallversorgung, 2. elektronischer Arztbrief, 3. Arzneimittelsicherheitsprüfung, 4. elektronische Patientenakte, 5. Patientendatenbereitstellung, 6. Leistungskonto für Versicherte, 7. Organ- und Gewebespendenerklärung, 8. Hinweis auf Vorsorgevollmachten und Patientenverfügungen (§ 291a Abs. 3 SGB V). Da die Netzstruktur und die Anwendungen immer noch nicht

142 dapi.de/das-dapi/das-dapi-stellt-sich-vor/, abgerufen am 9.1.2018.
143 Pimperl/Dittmann/Fischer/Schulte/Wendel/Wetzel/Hildebrandt in Langkafel S. 63 ff.
144 Strategy/pws S. 129.
145 Überblick über medizinische Netzwerke bei Strategy/pwc S. 129 f.
146 G. v. 14.11.2003, BGBl. I S. 2190; zu den Datenschutzvorkehrungen Schaar in Stiftung Datenschutz (2017) S. 145 ff.

eingerichtet waren, wurde Ende 2015 das sog. E-Health-Gesetz[147] verabschiedet, das Nutzungsanreize und -pflichten regelt.[148] Der zentrale Teil der Infrastruktur, der sog. Backbone, wurde zwischen Dezember 2016 und Juli 2017 mit der Anwendung des Versichertendatenmanagements in Nordrhein-Westfalen und Schleswig-Holstein getestet, in der Folge wurde der bundesweite Rollout von der gematik beschlossen.[149] Dieser blieb aber dadurch behindert, dass das Zwischenstück zwischen IT der Heilberufe und dem Gesundheitsnetz – der Konnektor – nur verzögert ausgeliefert wird.[150]

Nachdem sich immer wieder Verzögerungen bei der Einführung der Telematik-Infrastruktur (TI) ergaben, haben sich die im Verband der Privaten Krankenversicherungen[151] (PKV) zusammengeschlossenen Unternehmen verständigt, eine eigene Netzlösung zu verwirklichen, die mit einem effizienteren Ressourceneinsatz weitgehend die Funktionalitäten der TI verwirklichen soll.

Im Rahmen der Kommunikation werden oft Kommunikationsinhalte mit Gesundheitsbezug zwischengespeichert. Neben diesen Inhaltsdaten fallen weiterhin bei jedem Kommunikationsvorgang Nutzungs- bzw. Metadaten an, die Auskunft geben über die Identität und (evtl. Lokalisierung) der Kommunikationspartner, die in Anspruch genommenen Dienste, die Kommunikationszeiten (Anfang, Ende, Dauer) sowie den Datenumfang (s. o. 2.1.4). Damit in engem Zusammenhang stehen sog. Bestandsdaten, die Auskunft gegeben über die Identität und die technische Erreichbarkeit der Kommunikationspartner. Sämtliche dieser Daten sind bei der Inanspruchnahme von Gesundheitsdienstleistungen sowie zumindest bei Inhaltsdaten beim Austausch zwischen Leistungserbringern als (sensitive) Gesundheitsdaten einzustufen. Sie werden aus Sicherheitsgründen sowie auf Grund rechtlicher Regelungen (Telekommunikations-Vorratsdatenspeicherung) zwischengespeichert und stehen hiermit potenziell für Big Data im Sinne einer Zweitverwertung zur Verfügung. Dass derartige – rechtlich nicht zugelassene – Zweitverwertungen durch die Netzanbieter erfolgen, ist nicht bekannt.

Wohl ist bekannt, dass die Infrastruktur der öffentlichen Netze durch Geheimdienste dazu genutzt wird, Informationen für deren Zwecke abzufangen, zu speichern und auszuwerten. Davon sind unterschiedslos alle über das Internet vermittelten Kommunikationen betroffen, also auch der Austausch von Gesundheitsdaten. Die Geheimdienste, also z. B. die US-amerikanische National Security Agency (NSA), der britische Dienst Government Communications Headquarters (GCHQ) oder der bundesdeutsche

147 G. v. 21.12.2015, BGBl. I S. 2408.

148 Buchner MedR 2016, 662 ff.; Strategy/pwc S. 108.

149 Pfeiffer, Gesundheitskarte und Telemedizin – Beispiele für die Digitalisierung, ZBW – Leibnitz-Informationszentrum Wirtschaft, Wirtschaftsdienst 2017 (10) 697 f.; Borchers, Elektronische Gesundheitskarte: Information zum Start der Online-Anbindung, www.heise.de 10.10.2017.

150 Rosenbach/Schmergal, Einer wird gewinnen, Der Spiegel 43/2017, 74 ff.; fundamentalkritisch zur TI-Infastruktur Bauer, Die Totaldigitalisierung des Systems der Krankenversorgung, Gesundheit braucht Politik 2/2017, 10 ff.

151 Schlingensiepen, App für Privatpatienten, SZ 23.6.2017, 18.

Bundesnachrichtendienst (BND), werten die erlangten Daten mit Big Data aus.[152] Bisher nicht bekannt wurde, ob und inwieweit dabei gesundheitsbezogene Fragestellungen eine Rolle spielen.

3.4 Insbesondere Cloud Computing

Cloud Computing beschreibt die **Bereitstellung von informationstechnischer Infrastruktur** durch einen externen Anbieter über das Internet. Bei den Diensten kann es sich um die Bereitstellung von Speicherplatz, von Rechenleistung, von Anwendungssoftware, um einen kombinierten oder einen umfassenden Dienst handeln. Der Vorteil von Cloud Computing besteht darin, dass die Bereitstellung und Pflege der Dienstleistung vom Dienstleister erfolgt und alle Nutzer der Cloud hiervon profitieren. Dadurch lassen sich Ressourcen und Kosten einsparen und zugleich effektiver nutzen. Ein weiterer Vorteil besteht darin, dass durch die Erreichbarkeit über das Internet Clouddienste ortsunabhängig nutzbar sind. Je nach Angebot wird beim „as a service" unterschieden zwischen „storage" (Datenspeicherung), „infrastructure" (Rechenleistung) „software" (Programme), „platform" (Betriebssysteme mit Anwendungen) oder „analytics" (Auswertung). Es gibt Cloudangebote, die den Einsatz von KI im Bereich Gesundheit ermöglichen, wobei teilweise auch unstrukturierte Daten und Dokumente ausgewertet werden können. Solche Angebote machen IBM mit Watson, SAP mit seinem Angebot Leonardo oder Salesforce mit Einstein. Auch SAS plant, in der Cloud KI-Angebote bereit zu stellen.[153]

Beim Cloud Computing erfolgt ein Outsourcing von IT-Dienstleistungen. Datenschutzrechtlich handelt es sich hierbei regelmäßig um **Auftrags(daten)verarbeitung** (§ 11 BDSGaF, Art. 28 DSGVO), wenn die Verarbeitung zumindest formell inhaltlich vom Anwender bestimmt und gesteuert wird. Konsequenz der Auslagerung von Verarbeitungsaufgaben ist, dass die Kontrolle des Verantwortlichen in dem Maße eingeschränkt wird, in dem er Dritte hiermit betraut.

3.5 Versicherungen und Abrechnungsstellen

Gesundheitsleistungen verursachen Kosten; deren Erbringung ist nicht nur eine Befriedigung individueller Behandlungs- und Konsumbedürfnisse, sondern auch eine **Gemeinschaftsaufgabe** zur Sicherstellung der allgemeinen Gesundheit in einer Gesellschaft. Wegen der unterschiedlichen gesundheitlichen Belastung in der Gesellschaft und den teilweise äußerst hohen, von den Betroffenen nicht aufzubringenden Kosten, haben sich in Deutschland früh solidarische Finanzierungssysteme etabliert, bei denen die Kosten nicht (ausschließlich) von den Konsumenten/Patienten getragen werden, sondern ganz oder teilweise von der Gemeinschaft. In Deutschland besteht zum einen eine staatlich bzw. hoheitlich organisierte Versorgung über die gesetzliche Krankenversicherung (GKV, geregelt im SGB V) mit den Krankenkassen. Daneben bestehen private

---

152 Weichert DANA 2013, 109 ff.; ders. in Geiselberger/Moorstedt, Big Data – Das neue Versprechen der Allwissenheit, 2013, 131 ff. jeweils mit Bezug auf die Snowden-Enthüllungen.

153 Strehlitz, Der Treibstoff der Zukunft, SZ 26.10.2017, 28; Müller, Antworten aus der Cloud, SZ 26.10.2017, 27.

Krankenversicherungen (PKV). Ergänzend bestehen parallele solidarische Finanzierungsmodelle für die Pflege auf gesetzlicher (SGB XI) und privatvertraglicher Grundlage.

Zur Abwicklung der solidarischen Kostenübernahme ist es erforderlich, dass die Gesundheitsdaten nicht nur zwischen dem Betroffenen und dem Leistungserbringer ausgetauscht, sondern dass finanzielle Intermediäre einbezogen werden, welche die Kosten für die Gesundheitsleistungen übernehmen und welche zugleich eine Finanzkontrolle durchführen. Wegen ihrer intermediären Stellung nehmen sie zumeist weitere Aufgaben wahr, etwa Beratungsleistungen oder die Organisation der Erbringung der Gesundheitsleistungen, etwa über Disease-Management-Programme (vgl. §§ 137 f, 137g SGB V) oder über Maßnahmen der integrierten Versorgung (vgl. §§ 140a SGB V). Hierbei fallen regelmäßig weitere Gesundheitsdaten an.

Versicherungen erfüllen zugleich eine ökonomisch motivierte gesellschaftliche Frühwarnfunktion. Sie prognostizieren Risiken für die Zukunft auf Basis von Daten aus der Vergangenheit und machen so auf gesundheitliche Entwicklungen aufmerksam. Im iterativen Prozess der Risikobewertung werden im Interesse des besseren und vertieften Verständnisses viele Daten erfasst und analysiert. Zugleich organisieren sie den Risikoausgleich zwischen verschiedenen Kollektiven (Risikostrukturausgleich, Rückversicherung).[154] Big Data kann hierbei eine wichtige Rolle spielen, etwa zur Erkennung von Compliance-Problemen, z. B. von Betrugsversuchen, zur Erhöhung der Produktivität oder zur Entwicklung neuer Produkte. Tatsächlich war die Versicherungswirtschaft mit 21% der Unternehmen gemeinsam mit Autoherstellern schon Anfang 2016 die Branche, bei der Big Data schon am intensivsten genutzt wurde.[155] Big Data wird von Versicherungen nicht nur in den Sektoren Finanzen, Steuerung und Risikobewertung eingesetzt, sondern auch im Marketing und im Vertrieb.[156] Die Hauptanwendungsfälle liegen im primären Bereich der Versorgung in der Prädiktion von Risiken und dem Versorgungs- und Fallmanagement (über 60%). Im sekundären Bereich der Marktanalyse (Kundenbindung, Kündigungsprognose, Vertriebssteuerung, Tarifkalkulation) sind GKV-Kassen beim Big-Data-Einsatz in der Regel weiter fortgeschritten als private Versicherungen.[157] Analysiert werden insbesondere strukturierte Daten aus anwendungsnahen Quellen, weniger unstrukturierte Daten und solche aus externen Quellen. Während Daten zunächst insbesondere spartenspezifisch ausgewertet wurden, haben sich Datenstruktur und Datenzugang dahingehend geändert, dass Daten auch aus verschiedenen Leistungsbereichen zusammengeführt und analysiert werden.[158]

---

154 Maas/Milanova, Zwischen Verheissung und Bedrohung – Big Data in der Versicherungswirtschaft, Die Volkswirtschaft 5-2014,

155 Autobauer und Versicherer Vorreiter beim Big Data Einsatz, www.bitkom.org 17.2.2016.

156 Fraunhofer IMW S. 2, 9 ff.

157 Fraunhofer IMW S. 9.

158 Fraunhofer IMW S. 16 ff.

Von Versicherungen im gesetzlichen wie im privaten Bereich werden rechtliche Hürden bzw. Unklarheiten als ein zentrales Hindernis für den Einsatz von Big Data angesehen. Es wird vorgetragen, dass insbesondere Datenschutzbedenken einer umfassenden Nutzung von Big Data entgegenstünden.[159]

3.5.1 Gesetzliche Kranken- und Pflegekassen

In den Kranken- und Pflegekassen der gesetzlichen Krankenversicherung (§ 284 SGB V, § 94 SGB XI) wird Big Data in vieler Hinsicht praktiziert. Die Analyse eigener Datenbanken durch Krankenkassen hinsichtlich seltener Krankheiten oder besonderer Symptome zur Früherkennung oder Verhütung von Krankheiten wird von den §§ 20g, 63 SGB V (Modellvorhaben) geregelt. Gem. § 63 Abs. 3a SGB V bedarf es, wenig technikadäquat, nach vorheriger schriftlicher Information einer schriftlichen Einwilligung des Versicherten (s. u. 8.8.1). Die allgemeine Aufgabe von Krankenkassen in § 20 Abs. 1 S. 1 SGB V, wonach diese zur Erhaltung der Gesundheit ihrer Mitglieder verpflichtet sind, rechtfertigt keine spezifischen personenbezogenen Verarbeitungsmaßnahmen.[160]

Der vom Bundesversicherungsamt (BVA) durchgeführte Finanzausgleich zwischen den Krankenkassen zur Nivellierung der unterschiedlichen Gesundheitsrisiken der dort versicherten Personen (Risikostrukturausgleich, §§ 265 ff. SGB V, sog. Morbi-RSA)[161] erfolgt in einem Big-Data-Verfahren, wozu die Krankenkassen ihre Abrechnungsdaten liefern.[162] Um möglichst hohe Ausgleichszahlungen zu erlangen, veranlassen Krankenkassen die abrechnenden Ärzte teilweise, als besonders gravierend bewertete Diagnosen chronischer Krankheiten anzugeben, auch wenn dies nicht (voll) von den Realität abgedeckt ist.[163]

Der Einsatz von Big Data gehört bei Krankenkassen inzwischen zum Standard, wobei größere Krankenkassen eine umfassendere Strategie und Praxis haben als kleinere.[164] In großem Umfang eingesetzt wird die auf dem SAP-Produkt HANA basierende Branchenlösung oscare, in dem CRM-, ERP- und weitere Systeme für Analysen, Berichte und Statistiken zusammengeführt werden. Der Einsatz dient der Berechnung des Morbi-RSA[165], von amtlichen Statistiken und dem Controlling. Ergebnisse dienen der Prävention,

---

159 Fromme, Deutsche Versicherer zögern bei künstlicher Intelligenz, SZ 29.8.2017, 20; Fraunhofer IMW S. 13.

160 Problematisierend im Hinblick auf das Recht auf Nichtwissen Heckmann/Paschke in Stiftung Datenschutz (2017) S. 79 f.

161 BVA, So funktioniert der neue Risikostrukturausgleich im Gesundheitsfonds, 16.9.2008, http://www.bundesversicherungsamt.de/fileadmin/redaktion/Risikostrukturausgleich/Wie_funktioniert_Morbi_RSA.pdf.

162 Fraunhofer IMW S. 15.

163 Buschmann/Latsch/Schmergal/Schmitt, Patient krank, Kasse gesund, Der Spiegel 50/2017, 86 f.

164 Fraunhofer IMW S. 7 f.

165 Risikostrukturausgleich, §§ 265 ff. SGB V.

der „Fehlverhaltensbekämpfung“, dem Service, dem Marketing und dem Vertrieb wie auch der Prozessautomatisierung.[166]

Öffentliche (und auch private, s. u. 3.5.2) Krankenversicherungen greifen nicht nur auf die teilweise sehr komplexen eigenen Datenbestände zurück, sondern beziehen auch die Mitglieder bzw. Versicherten mit ein. Dies kann sowohl in spezifischen Betreuungsprogrammen, z. B. bei der Diabetes-Versorgung, erfolgen, wie auch generell bei der Gesundheitsvorsorge, bei der die Menschen nicht nur zu einem gesunden Lebensstil, sondern auch zur Anlieferung von persönlichen Daten angehalten und hierfür „belohnt“ werden (s. u. 10.5). Der hierbei unter den Stichworten Unterstützung und Beratung erfolgende Austausch steht immer wieder im Verdacht, nicht die Optimierung der Behandlung, sondern die Reduzierung der Behandlungs- und damit der Kassenkosten zum Ziel zu haben.[167]

Die Kostenträger nutzen hierbei den Trend des datenbasierten Selbstmonitoring der Quantified-Self-Bewegung, bei der mit Hilfe von Wearables Körperfunktionen gemessen und ausgewertet werden (s. u. 4.5).[168] Seit 2015 beteiligt sich die AOK Nordost alle zwei Jahre mit bis zu 50% und maximal 50 € an den Kosten von sog. Quantified-Self-Hardware. Zugleich führt sie auf der Basis des § 63 Abs. 1, 2 SGB V als Modellvorhaben ein Prämien-Vorteilsprogramm „FitMit AOK“ durch, ein „digitales Bonusheft“, mit dem körperliche Aktivitäten (min. 10.000 Schritte/Tag, min. 30 Min. Puls über 110/Minute, min. Kalorienverbrauch von 150 kcal/30 Minuten) mit Statuspunkten belohnt werden, die für gesundheits- und bewegungsbezogene Prämien (z. B. Gymnastikband, Sportbekleidung, Bluetooth-kompatible Körperwaage) eingelöst werden können. Die Prämienpunkte werden an die AOK weitergeleitet, nicht aber die Fitnessdaten, die von einem Institut wissenschaftlich ausgewertet werden.[169] Durch das Präventionsgesetz[170] wurden mit § 65a SGB V sog. Bonusprogramme für Gesundheitsbewusste von einer Kann- zu einer Soll-Regelung verstärkt. Krankenkassen sind danach gehalten, ihren Versicherten Bonusprogramme für definiertes gesundheitsbewusstes Verhalten anbieten. Neben der Teilnahme an „empfohlenen Früherkennungsuntersuchungen“ werden „qualitätsgesicherte Maßnahmen der Primärprävention“ bonifiziert. Das Bundesversicherungsamt (BVA) hat die Umsetzung davon abhängig gemacht, dass keine sensitiven Daten an die Krankenkassen übermittelt werden.[171]

Krankenkassen dürfen, je nachdem, welche Aufgabe sie erledigen, Daten von Dritten beschaffen. Regelmäßig ist dies aber nur subsidiär zulässig; Vorrang hat die Datenerhebung

166 Brunner in Langkafel S. 69 f.
167 BfDI 25. TB 2013-2014 Kap. 13.7 (S. 197 ff.).
168 Wehmeier/Baumann in Langkafel S. 145.
169 Klose in Stiftung Datenschutz (2017) S. 100 ff.; zu den Diskussionen im Vorfeld „Quantified Self“ jetzt auch bei Krankenkassen, DANA 2014, 115 f.
170 G. zur Stärkung der Gesundheitsförderung und der Prävention v. 17.7.2015, BGBl. I S. 1368.
171 Bundesverwaltungsamt, Jahresbericht 2015, S. 18 f.; Überblick über die Angebote bei Strategy/pwc S. 103 f.

beim Betroffenen (§ 67a Abs. 2 SGB X). Die Datenerhebungen verfolgen regelmäßig das Ziel der Kosteneinsparung. Hierbei belassen es viele Krankenkassen nicht bei den gesetzlich vorgesehenen Wegen der Datenerhebung. So greifen sie z. B. teilweise, trotz des Widerspruchs von Datenschutzbehörden, auf die Unterstützung von Auskunfteien zurück.[172]

3.5.2 Private Versicherungswirtschaft

Die Erfassung von Gesundheitsdaten im Rahmen des Abschlusses von **privaten Versicherungen** ist in verschiedenen Versicherungssparten langjährige Praxis. Dies ist bei der Kranken- und der Lebensversicherung, einschließlich der Berufsunfähigkeitsversicherung, sowie bei der Unfallversicherung zwangsläufig. Zum Zweck der **Risikobewertung** und zur diagnosebasierten Berechnung von Risikozuschlägen beim Abschluss von Kranken- und Lebensversicherungen schalten die Versicherungsunternehmen regelmäßig Dienstleister ein. Auf dem deutschen Markt sind dies insbesondere die Risk-Consulting Prof. Dr. Weyer, Köln, sowie die Münchner Rück (Munich Re) mit Sitz in München.

Auch in gesundheitsferneren Sparten ist die Erfassung von Gesundheitsdaten der Versicherungsnehmer nicht ausgeschlossen. Während bei der GKV die verarbeiteten Daten gesetzlich relativ präzise benannt sind, werden die Arten der Daten und der Verarbeitung bei der privaten Krankenversicherung (PKV) durch die **Vertragsgestaltung** bestimmt, die weitgehend vom Versicherungsunternehmen vorgegeben wird; der Konkretisierungsgrad bzgl. der Vorgaben und Festlegungen ist regelmäßig niedriger.

Während in der GKV Betrug vorrangig von Leistungserbringern praktiziert wird, wird in der PKV vermutet, dass **betrügerische Aktionen** eher von den Versicherten ausgehen. Um diese zu erkennen, setzen Unternehmen zunehmend Analysewerkzeuge ein, bei denen Erstattungsanträge mit Betrugsmustern verglichen und auf Auffälligkeiten hin überprüft werden.[173]

Die Erhebung von Gesundheitsdaten während des laufenden Versicherungsverhältnisses mit flexiblen Tarifen ist relativ neu. Insbesondere bei **Online- oder Direktversicherungen** wird diese Vorgehensweise gewählt, um die Versicherungsnehmer besser im Hinblick auf ihre Lebensform, das damit verbundene Versicherungsrisiko, aber auch hinsichtlich der Zahlungsfähigkeit oder der Wechselbereitschaft kennenzulernen und einschätzen zu können. 2004 entfielen von allen Versicherungsabschlüssen 2% auf den Online-Vertrieb. 2014 waren es 16%. 2004 informierten sich 13% vor einem Vertragsabschluss im Internet, 2014 waren es 37%. Beim Online-Vertrieb spielen Internet-Vergleichsportale eine wichtige Vermittlerfunktion, in Deutschland insbesondere Verivox und Check24.[174] 2016 kündigte Holtzbrinck an, die erste vollautomatisierte Krankenversicherung nach dem US-Vorbild

172 Deutsche BKK gibt Daten an Schufa, DANA 2014, 171.

173 Schlingensiepen, Datenanalyse soll Betrüger erkennen, SZ 30.08.2017, 18; allgemein Deutscher Ethikrat S. 71, 152 ff.

174 Fromme, Nervige Werbung, SZ 21.12.2015, 22.

„Oscar“ auf den deutschen Markt zu bringen.[175] Juni 2017 ging mit Ottonova die erste digitale private Krankenversicherung an den Markt.[176]

Das Online-Geschäft lief bei privaten Versicherungen lange Zeit eher schleppend. Dies hat sich geändert. Sog. InsurTechs also technologiegetriebene Unternehmen im Versicherungsbereich entwickeln sich sprunghaft. Dabei finden oft Kooperationen zwischen Start-ups und Großkonzernen statt. Bei vielen Unternehmen bestand das Problem, dass die etablierten Anbieter lange an Großrechnertechnologien festgehalten haben.[177]

Eine Weiterentwicklung der auch von gesetzlichen Krankenkassen angebotenen Bonussysteme besteht darin, dass den Versicherten durch den Nachweis von „gesunden Verhaltensweisen“ per Wearable nicht nur bestimmte Vergünstigungen zugestanden werden, sondern dass nach dem Grundsatz „Pay-as-you-live“ vom Versicherungsnehmer gelieferte Gesundheitsdaten die Tarifierung der Versicherung mitbestimmen. Pionier ist insofern für Deutschland der italienische private Versicherer Generali mit seinem sog. Vitality-Programm. Das Unternehmen wirbt damit, dass die Prämie für die Berufsunfähigkeits- oder die Risikolebensversicherung im Idealfall um 16% sinken kann.[178]

Die AXA hat mit Samsung eine Kooperation vereinbart.[179] Auch die Allianz denkt über Telematik-Anwendungen nach.[180] Die Schweizer Krankenversicherung CSS zahlt umgerechnet 40 Cent Belohnung für jeden Tag, an dem der Versicherte per App nachweist, mindestens 10.000 Schritte gegangen zu sein.[181] Es ist umstritten, inwieweit mit einem solchen Vorgehen das versicherungsrechtliche Solidarprinzip untergraben wird (s. u. 10.5).[182]

Private Versicherungen sind nicht nur an klassischen Vertragsdaten interessiert. Sie setzen Big-Data-Technologie auch ein, um Daten aus dem Internet für unternehmerische Zwecke auszuwerten und zu nutzen. Verschiedene Zielrichtungen werden dabei verfolgt: Zum einen geht es um die Aufklärung möglicher Betrugsfälle. So können Eintragungen in sog. sozialen Netzwerken Hinweise darauf geben, dass eine abgerechnete Krankheit oder ein

175 Holtzbrinck plant vollautomatisierte Krankenversicherung nach US-Vorbild, DANA 2016, 94 f.

176 Fromme, Ottonova erhält Millionen, SZ 17.3.2017, 20; www.ottonova.de.

177 Fromme, Digitale Kampfansage, SZ 20.03.2017, 20; Krieger/Hagen, Gute Aussichten für Versicherungs-Start-ups, SZ 15.03.2016, 25; Fromme, Von den Jungen lernen, SZ 19.6.2017, 20; Gröger, Ab in die Garage, SZ 5.9.2016, 22.

178 Generali konkretisiert deutsches Bonus-Projekt, DANA 2015, 86; Wanner, Versicherungskunden mögen Überwachung, SZ 25.11.2016, 22; Wanner/Fromme, Läuft bei Generali, SZ 21.06.2016, 19; Marx, Joggen für den Versicherungsbonus, Kieler Nachrichten 06.09.2017, 6; zur Vorgeschichte und frühen Kritik „Freiwillige“ Gesundheitsdaten bald bei Versicherer Generali? DANA 2015, 32 f.; Deutscher Ethikrat S. 154.

179 AXA erfasst Fitness- und Fahrdaten, DANA 2015, 39.

180 Baureithel, Total gesund, der Freitag 12.3.2015, 03.

181 Selke, Digitale Alchemisten, SZ 1./2.7.2017, 5.

182 Raum in Stiftung Datenschutz (2017) S. 132; Fraktion Bündnis 90/Die Grünen BT-Drs. 18/9058; vgl. aber BReg. BT-Drs. 18/9243 S. 6.

Unfall mit schweren Folgen gar nicht stattgefunden hat. Die Auswertung von Netzdaten dient teilweise generell dem besseren „Kennenlernen" der Kunden, der Personalisierung von Angeboten, der Kundenbindung und -kommunikation oder einer zügigeren Schadensabwicklung. Für die Kommunikation werden teilweise Webdienste genutzt. Es gibt Fälle, bei denen Versicherungsmitarbeiter ermuntert werden, sich z. B. mit Facebook-Nutzern zu befreunden. In Frankreich oder in den USA sind solche Praktiken weit verbreitet. Deutsche Unternehmen sind insofern eher zurückhaltend.[183]

Eine spezifische Form des Einsatzes von Big Data wird von der Versicherungskammer Bayern (VKB) praktiziert. Die VKB arbeitet mit IBM zusammen, die deren auf KI-Basis arbeitenden Computer Watson bei der Bearbeitung der Kundenkommunikation einsetzt. Dabei werden die Kundenschreiben bzw. E-Mails nach Schlagworten sortiert, inhaltlich analysiert und nach verschiedenen Kategorien, z. B. Unmut des Kunden, eingestuft. Die Beantwortung der Schreiben erfolgt noch manuell.[184]

Die Allianz, Europas größter Versicherer, plant eine gemeinnützige Stiftung, welche die von ihr teuer entwickelte Software Allianz Betriebssystem (ABS) kostenfrei auf globaler Ebene zur Verfügung stellen soll. Vorbild für dieses Vorgehen ist die Cloud Foundry, eine offene Software, die von einer US-Stiftung verwaltet wird und Softwarelösungen aus der Datencloud anbietet (vgl. 3.4). Durch die Vielzahl der nutzenden Partner können für Entwicklung und Betrieb Kosten in der Branche gespart werden. Diese gibt allein in Deutschland derzeit mehr als 4 Mrd. € pro Jahr für Informationstechnik (IT) aus.[185] Wird das Angebot von anderen Versicherungsunternehmen angenommen, so führt dies nicht nur zu Synergie- und Einspareffekten, sondern auch dazu, dass die standardisierten Prozesse eine versicherungs- und länderübergreifende Zusammenführung von (mehr oder weniger anonymisierten) Daten ermöglicht wird.

Für sämtliche Sparten außer der privaten Krankenversicherung (PKV) wird im Auftrag des Gesamtverbands der Deutschen Versicherungswirtschaft (GDV) bei der informa Insurance Risk and Fraud Prevention GmbH ein Hinweis- und Informationssystem (HIS) als Warnsystem geführt, mit dem Anträge auf Abschluss von Versicherungen sowie auf Schadensregulierung abgeklärt werden. Zweckrichtung ist es, über die Datenanlieferung zur und Beauskunftung durch diese Auskunftei Versicherungsbetrug und -missbrauch zu verhindern und zu bekämpfen. Im Bereich der Lebensversicherung, der Berufsunfähigkeitsversicherung sowie der Unfallversicherung werden hierbei auch gesundheitsrelevante Daten aus unterschiedlichen Unternehmen erhoben und ausgetauscht. Die Einmeldung und Beauskunftung erfolgt nicht auf der Grundlage einer

183 Krieger/Gröger Vorsicht, Versicherer schaut zu, SZ 23.05.2016, 17.

184 Fromme, Ärger an Watson, SZ 9.12.2015, 17; Digitaler Kundenversteher, SZ 11.05.2016, 19; VKB nutzt „künstliche Intelligenz" zur Sachbearbeitung, DANA 2016, 94.

185 Fromme, Die Allianz gibt eigene Software frei, SZ 20.12.2017, 20.

Big-Data-Auswertung durch das HIS, sondern gemäß vorgegebenen Verdachtskriterien.[186] Ein entsprechendes Warnsystem war auch für die PKV geplant.[187]

Bei der **Schadenabwicklung** mit privaten Versicherungsunternehmen nehmen Krankenhäuser teilweise Makler in Anspruch wie z. B. die ECCLESIA mildenberg Hospital, die bei sich sämtliche Patientendaten speichern, ohne dass bisher hinreichend sichergestellt wird, dass diese Daten nicht von den Maklern für andere Zwecke weiterverwendet werden.[188]

Im Gesundheitswesen generell, insbesondere im privatwirtschaftlichen Sektor, hat ein Kampf **um die Daten** begonnen. Dieser Kampf um die Verfügungsmacht und die ökonomische Nutzungsmöglichkeit von Daten findet derzeit noch vorrangig im Hinblick auf Internetdaten statt; ein neues Feld sind Kfz-Daten. Doch auch der Zugang zu Gesundheitsdaten gewinnt zunehmend Marktrelevanz. Hierbei konkurrieren die Versicherungen mit den Online-Portalen, die zunehmend eigene Versicherungs- und gesundheitliche Beratungs- und Betreuungsangebote machen.[189] Applikationsanbieter unterstützten je nach Anwendung die eine oder die andere Seite.

3.5.3 Sonstige

Neben den klassischen Abrechnungswegen über private und öffentliche Krankenversicherungen haben sich inzwischen weitere eingeschaltete Abläufe und dafür nötige Institutionen mit Gesundheitsdatenverarbeitung etabliert, so etwa im Bereich der hausärztlichen Versorgung die **Hausarztverbände** (§ 73b SGB V). Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) stellte als Datenschutzaufsichtsbehörde fest, dass deren Vorhaben, die Abrechnungsdaten der Hausärzte über einem intransparenten „gekapselten Kern" der Arztsoftware abzuziehen, rechtswidrig ist.[190] Statt die unzulässige Praxis zu unterlassen, wurde in § 295a Abs. 1 SGB V im Jahr 2011 eine Gesetzesänderung vorgenommen, wonach die Hausarztverbände zu Verantwortlichen erklärt wurden, was diesen den Weg frei machte, die weitere Datenverarbeitung eigenmächtig festzulegen.[191] Die Hausärzteverbände der Länder haben sich im Deutschen Hausärzteverband zusammengeschlossen. Die informationstechnischen Dienstleistungen werden durch dessen Hausärztliche Vertragsgemeinschaft Aktiengesellschaft (HÄVG), ein Privatunternehmen mit Sitz in Köln, erbracht.[192] Dieses führt nicht nur den Datenaustausch mit den Krankenkassen durch, sondern stellt, so die vorliegenden Erkenntnisse, die angeblich anonymisierten, tatsächlich aber nur

186 Eichler/Kamp in Wolff/Brink Syst. K Rn. 33 ff., insbes. Rn. 40; ULD, Tätigkeitsbericht 2013, Kap. 5.1.1. (S. 73 f.).
187 ULD, Tätigkeitsbericht 2015, Kap. 5.1.1. (S. 73 f.).
188 Aus datenschutzrechtlicher Sicht kritisch hierzu Weichert VuR 2017, 138 ff.
189 Hagen, Die Bälle aus der Luft holen, SZ 28.01.2016, 18.
190 ULD, 33. Tätigkeitsbericht(TB) 2011, Kap. 4.5.3 (S. 50 ff.).
191 ULD, 34. TB 2013, 2013, Kap. 4.6.1 (S. 61).
192 https://www.hausaerzteverband.de/cms/HAEVG.4.0.html, abgerufen am 9.1.2018.

pseudonymisierten Einzeldatensätze der IMS-Health (IQVIA) für die weitere Aufbereitung, Big-Data-Auswertung und Vermarktung zur Verfügung.

3.6 Stellen zur Qualitätssicherung und Wirtschaftlichkeitskontrollen

Ein relevantes Einsatzgebiet von Big Data ist das Controlling sowohl hinsichtlich der medizinischen Qualität als auch im Hinblick auf die Wirtschaftlichkeit und finanzielle Korrektheit (s. u. 4.3, 4.4). Derartige Maßnahmen werden im GKV-Bereich durch die Kassen(zahn)ärztlichen Vereinigungen (§§ 77 ff. SGB V) sowie durch den Medizinischen Dienst der Krankenkassen (MDK) vorgenommen. Dort findet Big Data bisher keine Anwendung. Vielmehr beschränken sich die genutzten Programme auf Plausibilitätsprüfungen, die händisch auf Basis der Abrechnungserfahrungen programmiert werden.

Gemäß § 2 Abs. 1 S. 3 SGB V haben Qualität und Wirksamkeit der Leistungen „dem allgemein anerkannten Stand der medizinischen Erkenntnisse zu entsprechen und den medizinischen Fortschritt zu berücksichtigen". Damit wird auf den jeweiligen Stand der Wissenschaft Bezug genommen, der zunehmend durch Big Data bestimmt wird. Wird Big Data im Bereich der Qualitätssicherung eingesetzt, so müssen dabei wissenschaftliche Standards eingehalten werden.[193]

In den §§ 139a-139c SGB V ist die Einrichtung eines Instituts für Qualität und Wirtschaftlichkeit im Gesundheitswesen (IQWiG) durch den Gemeinsamen Bundesausschuss (G-BA) vorgesehen. Das Institut erstellt Auswertungen und Gutachten zu Fragen der Qualität und Wirtschaftlichkeit im Bereich der GKV. Dazu gehören die evidenzbasierte Bewertung des aktuellen medizinischen Wissensstandes zu diagnostischen und therapeutischen Verfahren oder die Bewertung von evidenzbasierten Leitlinien sowie Empfehlungen zu Disease-Management-Programmen (§ 139a Abs. 3 SGB V). Aufträge erhält das IQWiG ausschließlich vom Bundesgesundheitsministerium (BMG) und vom G-BA. Der sogenannte Generalauftrag des G-BA ermöglicht es dem Institut, eigenständig Themen aufzugreifen und wissenschaftlich zu bearbeiten. Vom Jahr 2016 an hat der Gesetzgeber ein öffentliches Vorschlagsverfahren für die Bewertung von Untersuchungs- und Behandlungsverfahren, sogenannte HTA-Berichte (Health Technology Assessment) auf das IQWiG gemäß § 139b Abs. 5 SGB V übertragen. Das IQWIG stellt auf seiner Seite gesundheitsinformation.de verlässliche Informationen in verständlicher Weise zur Verfügung.[194]

Im Auftrag des G-BA ist außerdem das Institut für Qualitätssicherung und Transparenz im Gesundheitswesen (IQTiG) bei Maßnahmen zur Qualitätssicherung und zur Darstellung der Versorgungsqualität tätig (§ 137a SGB V).[195] Ein Schwerpunkt liegt in der Entwicklung und Durchführung von Verfahren der einrichtungs- und sektorenübergreifenden

193 Deutscher Ethikrat S. 102
194 Strategy/pwc S. 144.
195 https://iqtig.org.

Qualitätssicherung, der Entwicklung von Kriterien zur Bewertung von Zertifikaten und Qualitätssiegeln sowie die Veröffentlichung der Ergebnisse in allgemein verständlicher Form.

Qualitätssicherung ist auch ein Thema von unabhängigen **Forschungseinrichtungen**. Einen prominenten Platz nimmt hierbei das „Institut für angewandte Qualitätsförderung und Forschung im Gesundheitswesen GmbH“ (kurz: aQua-Institut) ein, das bis Ende 2015 den G-BA bei der Umsetzung der GKV-Qualitätssicherung unterstützte.[196]

Aus den Angaben von Symptomen, Krankheiten und ärztlichen Behandlungen werden Qualitätsstandards abgeleitet, die zur Erarbeitung von Leitlinien beitragen.[197] **Medizinische Leitlinien** sind systematisch entwickelte Feststellungen, die Ärzte, Zahnärzte, Angehörige anderer Gesundheitsberufe und Patienten bei ihren Entscheidungen über die angemessene Gesundheitsversorgung unter spezifischen klinischen Umständen unterstützen sollen. Sie sind nicht bindend und müssen an den Einzelfall angepasst werden. In Deutschland werden medizinische Leitlinien evidenzbasiert in erster Linie von der Arbeitsgemeinschaft der Wissenschaftlichen Medizinischen Fachgesellschaften (AWMF), von der ärztlichen Selbstverwaltung, also von der Bundes(zahn)ärztekammer (BÄK, BZÄK) und der Kassen(zahn)ärztliche Bundesvereinigung (KBV, KZBV) oder von Berufsverbänden entwickelt und verbreitet. Informationen über und Zugang zu internationalen Leitlinien-Projekten und -Agenturen bietet das Guidelines International Network mit der weltweit umfangreichsten Leitlinien-Datenbank.

Ein Controlling erfolgt als Teilaufgabe inzwischen in vielen **Einrichtungen intern**, etwa in Krankenhäusern, bei sonstigen Leistungserbringern, bei den Krankenkassen und privaten Krankensicherungen sowie auch in Forschungseinrichtungen. KIS- und AIS-Systeme enthalten regelmäßig Controlling-Funktionalitäten (s. o. 3.2). § 135a SGB V verpflichtet Leistungserbringer auf das Ziel der Qualitätssicherung. Die Ergebnisse des Controllings dienen der Qualitätskontrolle und -verbesserung sowie der Missbrauchskontrolle und -prävention und damit letztlich der Ressourcen- und Angebotsoptimierung. Die Ergebnisse fließen in betriebsinterne Planungen ein, aber auch in die Festlegung von Behandlungsstandards oder in die Berechnung von Kostenerstattungsgrößen (DRGs, s. u. 3.8, 3.11).[198]

Auch bei den **Wirtschaftlichkeitskontrollen** kann zwischen internen und einrichtungsübergreifenden Anwendungen unterschieden werden. Analysiert werden DRG-Zahlen, Case Mix, Kosten für Personal, Material und Medikamente. Es geht um die Auslastung von Geräten, Betten und Operationssälen, um die vorausschauende Wartung der Geräte, um die Erarbeitung von Qualitätskennziffern, unter Einbeziehung von Raten zu Komplikation, Re-Hospitalisierung oder Sterblichkeit, die mit den Kosten in Relation gesetzt

196 www.aqua-institut.de.
197 Kamps in Langkafel S. 78.
198 Langkafel in Langkafel S. 23 f.

werden.[199] Bei Wirtschaftlichkeitskontrollen kommt das Ziel der Kosteneinsparung regelmäßig mit dem Ziel einer optimalen Behandlung in Konflikt. Wird bei dieser Kontrolle Big Data eingesetzt, so ist darauf zu achten, dass die Algorithmen (z. B. durch Leitlinien) definierte Behandlungsstandards nicht unterschreiten.[200]

Zu den Kontroll- und Qualitätssicherungsinstitutionen im Rahmen der gesetzlichen Krankenversicherung (GKV) gehören auch die Medizinischen Dienste der Krankenkassen (MDK, §§ 275 ff. SGB V).[201]

3.7 Abrechnungsdienstleister: privatärztliche und gewerbliche Verrechnungsstellen

Während im GKV-Bereich die Rolle von Abrechnungsdienstleistern für die ambulante Versorgung weitgehend von den Kassen(zahn)ärztlichen Vereinigungen übernommen wird, gibt es für den stationären Bereich sowie für die Datenweitergabe zur Abrechnung mit den Patienten oder der Krankenversicherung (§ 192 Abs. 3 Nr. 5 VVG) im Rahmen der privatärztlichen Versorgung keine gesetzliche Legitimation. Diese Abrechnungsaufgabe übernehmen für den privatärztlichen Bereich weitgehend die gewerblichen und die privatärztlichen Verrechnungsstellen (PVS). Da es für die Offenbarung von Patientengeheimnissen insofern keine andere Rechtfertigung gibt, bedarf es hierfür jeweils einer Schweigepflichtentbindung des betroffenen Patienten.[202] Um dennoch eine gewisse Abschottung sicherzustellen, sieht § 203 Abs. 1 Nr. 6 StGB für privatärztliche, nicht für gewerbliche, Verrechnungsstellen eine strafbewehrte Schweigepflicht vor. Wegen der Mandantenbezogenheit der jeweiligen Aufträge sind hier ohne eine ausreichende vorangegangene Anonymisierung Big-Data-Analysen nicht zulässig.

Die Abrechnung von stationären GKV-Leistungen unter Einbeziehung Dritter erfolgt teilweise auch unter Einbeziehung Dritter auf der Grundlage von Einwilligungen/Schweigepflichtentbindungen der Betroffenen. Nach einem – teilweise heftig kritisierten – Urteil des BSG vom 10.12.2008 war diese Praxis vorläufig in Frage gestellt.[203] Der Gesetzgeber reagierte auf diese Kritik und erlaubte in § 295a SGB V wie im selektivvertraglichen Bereich die Einschaltung auf Einwilligungsbasis.[204] Da die Einwilligung keine übergreifende Auswertung vorsieht, kommt auch in diesem Bereich jenseits einer vollständigen Anonymisierung keine Anwendung von Big Data in Betracht.

---

199 Wehmeier/Baumann in Langkafel S. 143 ff.; Zimmermann-Rittereiser/Schaper in Langkafel S. 156 f.

200 Deutscher Ethikrat S. 102.

201 Kircher in Kingreen/Kühling S. 171 f.

202 Schirmer in Roßnagel Kap. 7.12 Rn. 73 (S. 1377 f.); Kircher in Kingreen/Kühling S. 230 ff. mit Verweis auf die Rspr. des BGH seit BGH 10.7.1991 – VIII ZR 296/90, NJW 1991, 2955.

203 BSG 10.12.2008 – B 6 KA 37/07 R -, NJW 2009, 3743 = MedR 2009, 685 = BSGE 102, 134; kritisch dazu Kircher in Kingreen/Kühling S. 237 ff.; Schneider S. 111.

204 Kritisch Kircher in Kingreen/Kühling S. 242 ff.

3.8 DIMDI

Eine zentrale Funktion für das öffentliche Gesundheitsdatenmanagement in Deutschland übernimmt das „Deutsche Institut für Medizinische Dokumentation und Information" (DIMDI). Das DIMDI mit Sitz in Köln ist eine nachgeordnete Behörde des Bundesministeriums für Gesundheit (BMG). Eine seiner Aufgaben ist es, der fachlich interessierten Öffentlichkeit aktuelle Informationen aus dem gesamten Gebiet der Medizin einfach und schnell zugänglich zu machen. Zudem gibt es die deutschen Versionen medizinischer Klassifikationen heraus und führt nationale Register u. a. zu Klinischen Studien und legalen Arzneimittel-Versandhändlern.[205]

Das DIMDI ist das deutsche Kooperationszentrum für das System Internationaler Klassifikationen (Collaboration Centre for the Family of International Classifications) der Weltgesundheitsorganisation (World Health Organization) und verwaltet die „International Codes of Diseaeses" (ICD, ICF und die ICD-O für Tumorerkrankungen). Die vom DIMDI herausgegebenen Klassifikationen ICD-10-GM und OPS bilden eine wichtige Grundlage für das pauschalierende Entgeltsystem G-DRG (German Diagnosis Related Groups), das vom Institut für das Entgeltsystem im Krankenhaus (InEK) bereitgestellt und in der stationären Versorgung eingesetzt wird.

Das DIMDI stellt auf seiner Website ein Versandhandels-Register zur Verfügung. Damit können Verbraucher prüfen, welche Versandapotheken oder sonstigen Händler über eine behördliche Versanderlaubnis für Deutschland verfügen. Im seit Juli 2017 beim DIMDI geführten Deutschen Register Klinischer Studien (DRKS) werden in Deutschland laufende und abgeschlossene patientenorientierte klinische Studien registriert.[206] Ab 2018 betreibt DIMDI ein neues Samenspenderregister, in dem gemäß dem Samenspenderregistergesetz[207] Informationen zu Samenspendern und Empfängerinnen von Samenspenden dokumentiert werden. Kinder können ab dem 16. Lebensjahr Auskunft zu ihrer Abstammung über das Register erhalten.

Das DIMDI betreibt zudem spezielle Informationssysteme für Arzneimittel (§ 34 AMG), Medizinprodukte (§ 33 MPG) und Health Technology Assessment (HTA, Gesetz über ein Informationssystem zur Bewertung medizintechnischer Verfahren) sowie für Forschungszwecke ein Informationssystem mit Versorgungsdaten der gesetzlichen Krankenversicherung (§§ 303a – 303e SGB V).

Mit diesem Informationssystem Versorgungsdaten (Datentransparenz), das im Februar 2014 den Pilotbetrieb aufgenommen und im April 2015 die Ausbaustufe 2 erreicht hat, können nutzungsberechtigte Stellen (§ 303e Abs. 1 SGB V) beim DIMDI als Datenaufbereitungsstelle (§ 303d SGB V) die Auswertung von GKV-Versorgungsdaten beantragen. Diese können insbesondere für Analysen des Versorgungsgeschehens im

---

205 Strategy/pwc S. 143 f.

206 § 1 Abs. 1 Nr. 1e, Abs. 3 DIMDI-Arzneimittelverordnung; https://www.drks.de/drks_web/; DRKS: Studienregister jetzt beim DIMDI, www.dimdi.de 30.06.2017.

207 BGBl. 2017 I S. 2513 ff.

Rahmen der Versorgungsforschung und für Steuerungsaufgaben in der gesetzlichen Krankenversicherung genutzt werden. Die in der Datentransparenzverordnung (DaTraV)[208] aufgeführten-Daten beinhalten u. a. Angaben über ambulante und stationäre Diagnosen sowie zur ambulanten Arzneimittelversorgung der gesetzlich Versicherten. Der jahresübergreifende Datenbestand stammt vom Bundesversicherungsamt (BVA), das die Daten von den Krankenkassen für den morbiditätsorientierten Risikostrukturausgleich (Morbi-RSA, s. o. 3.5.1) erhalten hat. Es wird sichergestellt, dass einzelne Versicherte nicht identifizierbar sind. Hierfür werden die Versicherungsnummern durch andere Pseudonyme ersetzt (§ 303c Abs. 2 SGB V). Die gespeicherten Daten sollen künftig vereinfacht generell der Forschung zur Verfügung gestellt werden. Bisher erfolgte wegen des aufwändigen Verfahrens nur eine eingeschränkte Forschungsnutzung. Eine Zuordnung von Leistungserbringern ist bei der Datentransparenz bisher nicht vorgesehen.[209] Die „Datentransparenz" ist ein Beispiel dafür, wie umfangreiche Datensätze in regulierter Form datenschutzkonform zur Auswertung gebracht werden können.[210]

3.9 Öffentlicher Bereich generell

Gesundheitsdaten liegen in großem Umfang im Bereich der öffentlichen Verwaltung vor: bei Gemeinden, Gesundheitsämtern sowie den Behörden, die direkt oder indirekt mit der Gesundheitsversorgung oder der Aufsicht und Kontrolle betraut sind. Dazu gehören sowohl Stellen, die originär solche Daten erheben, z. B. Gesundheitsämter, Sozialleistungsträger, öffentliche Stellen als Arbeitgeber, wie auch solche, die abgeleitete Aufgaben und Befugnisse haben, etwa Ministerien, Kammern im Heilberufebereich, die Kassen(zahn)ärztlichen Vereinigungen, Datenschutz-, Lebensmittel-, Gesundheits- oder Gewerbeaufsichtsbehörden. Big-Data-Anwendungen sind aus diesen Bereichen bisher nicht bekannt.

3.10 Gesundheitsbehörden

Der öffentliche Gesundheitsdienst ist in Deutschland weitgehend landesgesetzlich geregelt und obliegt danach weitestgehend den Kreisen bzw. Kommunen. Seine Funktion besteht darin, vor Ort eine bedarfsgerechte, wirtschaftliche, wirksame und qualifizierte Gesundheitsversorgung der Bevölkerung sicherzustellen. Dies umfasst Beobachtungs-, Überwachungs- und Präventivmaßnahmen sowie die Wahrnehmung der amtsärztlichen Tätigkeit und der damit verbundenen Gesundheitsberichterstattung. In diesem Zusammenhang fallen personenbezogene Gesundheitsdaten an.

Konkret geht es u. a. um folgende Aufgaben: Beratung und Betreuung von Personen in sozialen und gesundheitlichen Problemlagen, Untersuchung und Gesundheitsförderung von Kindern und Jugendlichen, u. a. in Kindertagesstätten und Schulen, Vorsorgeangebote mit ärztlichen Untersuchungen und Impfungen, Infektionsschutz, Hygieneüberwachung von Einrichtungen, Geschlechtskrankenfürsorge, Prostituiertenbetreuung, Aufsicht und

208 DaTraV v. 10.9.2012, BGBl. I S. 1895 ff.
209 Ludwig, Big Data von der Krankenkasse, SZ 9.11.2017, 19.
210 Zur Gesetzgebungsgeschichte ausführlich Weichert, DANA 4/1999, 21-24.

Überwachung der Berufe des Gesundheitswesens, Prüfungswesen für nichtärztliche Heilberufe, Gesundheitshilfe, Gutachtenerstellung und sozialpsychiatrischer Dienst. Die anzuwendenden Gesetze sind weitgehend landesrechtliche Regelungen, so etwa Gesundheitsdienstgesetze, Psychisch-Kranken-Gesetze[211], Heilberufegesetze, Krankenhausgesetze[212], teilweise aber auch Bundesgesetze, so das Infektionsschutzgesetz, das Betäubungsmittelgesetz, die Apothekerbetriebsordnung, das Schwangerschaftskonfliktgesetz oder die Röntgenverordnung.[213]

Den kommunalen Gesundheitsämtern fachlich übergeordnet sind die Landesgesundheitsämter der Bundesländer.[214] Sie nehmen die Aufgaben des öffentlichen Gesundheitsdienstes auf Landesebene wahr und sind zugleich die Schnittstelle zwischen den kommunalen Gesundheitsämtern zur Landespolitik und zu den Landesministerien. Zudem nehmen sie Aufgaben im Bereich der Arbeitsmedizin sowie im Ausbildungs- und Prüfungsbereich von Gesundheitsberufen wahr.

Die hoheitlichen Gesundheitsämter haben nicht die rechtlichen, informationstechnischen und personellen Ressourcen zur eigenen Anwendung von Big Data. Doch fallen bei deren Tätigkeit Daten an, die für Big-Data-Analysen von hoher Relevanz sein können.

Auf der Ebene der Bundesländer existiert ein "Katalog der Gesundheitsberichterstattung der Länder", der durch die Gesundheitsministerkonferenz der Länder (GMK) verabschiedet wird.[215] In diesem Katalog sind etwa 300 Indikatoren zu verschiedenen gesundheitsrelevanten Themen erfasst, die eine vergleichbare Datenbasis ermöglichen sollen. Da nicht alle Daten gleichermaßen in den Bundesländern verfügbar sind, wurde innerhalb des Indikatorensatzes eine Auswahl an sog. Kernindikatoren getroffen, die in allen Bundesländern einheitlich zur Verfügung stehen sollen. Die Daten für die Gesundheitsberichterstattung werden von den Landesgesundheitsämtern und insbesondere den kommunalen Gesundheitsämtern angeliefert. Die Daten fließen in die übergreifende amtliche Statistik ein (s. u. 3.11).

3.11 Amtliche Statistik

Um Regierungen, Parlamente, Verwaltungen, aber auch die Wirtschaft und die Öffentlichkeit über Entwicklungen im gesellschaftlichen Leben zu informieren, sammeln Statistikämter systematisch Informationen über praktisch alle relevanten Lebensbereiche, bereiten diese auf und stellen sie bereit. Die amtlichen Statistiken des Statistischen Bundesamtes und der Landesämter für Statistik sind eine vielseitige Informationsquelle für die Vorbereitung von Entscheidungen, Maßnahmen und Planungen mit einer hohen Aussagekraft. Von Interesse sind nicht personenbezogene, sondern aggregierte, also nach bestimmten Merkmalen zusammengefasste Daten über eine Vielzahl von Personen und

211 Schneider S. 69 ff.
212 Ausführlich Schneider S. 123 ff.
213 Zilkens, Datenschutz in der Kommunalverwaltung, 3. Aufl. 2011, Rn. 189 ff. (S. 193 ff.).
214 Übersicht abzurufen unter www.socialnet.de/branchenbuch/2282.php.
215 www.gbe-bund.de/pdf/Indikatorensatz_der_Laender_2003.pdf.

über Lebenssachverhalte, die regelmäßig aus personenbezogenen Angaben gewonnen werden. Es gehört zum Wesen der Statistik, dass die Daten nach ihrer statistischen Aufbereitung für die verschiedensten, nicht von vornherein bestimmbaren Aufgaben verwendet werden.[216]

Statistische Grunddaten werden aus dem Verwaltungsvollzug sowie aus statistischen Erhebungen gewonnen. Bei den Erhebungen bei privaten Stellen wird unterschieden zwischen Primärerhebungen und Sekundärstatistiken. Bei Primärerhebungen werden die Daten bei den jeweiligen Informationsträgern direkt für statistische Zwecke erhoben. Dazu gehören auch die Volkszählungen sowie die stichprobenartigen Mikrozensus-Erhebungen[217], die sich auch an Individualhaushalte richten. Bei einer Sekundärstatistik sind die Daten zunächst für einen anderen Zweck erhoben worden und werden nun für statistische Zwecke einer Zweitverwertung zugeführt.

Zentrale Rechtsgrundlagen für Statistiken in Deutschland sind auf Bundesebene das Gesetz über die Statistik für Bundeszwecke (BStatG)[218] sowie auf Ebene der Bundesländer die Landesstatistikgesetze.[219] In den allgemeinen Erhebungen zur Volkszählung und zum Mikrozensus werden u. a. gesundheitsrelevante Daten erhoben. Daneben gibt es eine Vielzahl spezifischer gesundheitsbezogener Statistiken. Die Online-Datenbank der Gesundheitsberichterstattung (GBE) des Bundes führt Gesundheitsdaten und Gesundheitsinformationen aus über 100 verschiedenen Quellen an zentraler Stelle zusammen. Seit 1991 werden auf bundeseinheitlicher Grundlage Krankenhausstatistiken erstellt.[220] Zur Unterstützung der Daten der nach § 11a BStatG berichtspflichtigen Unternehmen hat die Deutsche Krankenhausgesellschaft e. V. (DKG) ein XML-Daten-Modul zur Verfügung gestellt. Seit 2005 ergänzt die fallpauschalenbezogene Krankenhausstatistik (DRG-Statistik) die Diagnosestatistik der Krankenhauspatienten. Eine Statistik der schwerbehinderten Menschen soll alle zwei Jahre sozialpolitische Planungen erleichtern (bisher § 131 SGB IX[221]). Eine Pflegestatistik erfasst Daten zum Angebot und zur Nachfrage nach pflegerischer Versorgung (§ 109 Abs. 1 SGB XI). Die Schwangerschaftsabbruchstatistik geht auf das Gesetz zur Vermeidung und Bewältigung von Schwangerschaftskonflikten zurück.[222] Die Todesursachenstatistik findet ihre Rechtsgrundlage im Gesetz über die Statistik der Bevölkerungsbewegung und die Fortschreibung des Bevölkerungsstandes.[223] Daten zu Gesundheitsausgaben werden auf

---

216 BVerfG 15.12.1983 – 1 BvR 209/83 u. a., NJW 1984, 423.

217 Z. B. Mikrozensusgesetz vom 7.12.2016, BGBl. I S. 2826.

218 BStatG v. 22.1.1987, neugefasst durch Bek. v. 20.10.2016, BGBl. I S. 2394, zuletzt geändert durch G. v. 30.10.2017, BGBl. I S. 3618.

219 Überblick bei de.wikipedia.org/wiki/Statistisches_Landesamt.

220 Krankenhausstatistik-Verordnung v. 10.4.1990, BGBl. I S. 730, zuletzt geänd. durch G. v. 17.3.2009, BGBl. I S. 534.

221 Zuletzt geändert durch Art. 2 Bundesteilhabegesetz (BTHG) v. 23.12.2016, BGBl. I 3234 (Übergangsrecht zum Jahr 2017), vgl. jetzt §§ 143 ff. SGB IX.

222 G. v. 27.7.1992, BGBl. I S. 1398, zuletzt geänd. durch G. v. 20.10.2015, BGBl. I S. 1722.

223 G. v. 20.4.2013, BGBl. I S. 826.

nationaler und internationaler Ebene in vergleichbarer Form seit 1992 erfasst.[224] Inzwischen gehen viele amtliche Statistiken auf eine europarechtliche Grundlage zurück.[225] Dies gilt z. B. auch für die Beschaffung der Daten zu den Beschäftigten im Gesundheitswesen.[226]

3.12 Forschung

In der Forschung soll die Auswertung großer Mengen gesundheitsrelevanter Daten zu einem besseren Verständnis wissenschaftlich relevanter Zusammenhänge und Prozesse führen. Medizinische Forschung verspricht technischen Fortschritt, einen immer reichhaltigeren Erkenntnisgewinn zur Verbesserung der Vorsorge und Vorbeugung sowie auf neue diagnostische und therapeutische Möglichkeiten.[227] Besonders im Bereich der Bio-, speziell der Gentechnik, tun sich gänzlich neue Zugänge zu Erkrankungs- und Therapiemechanismen auf. (s. u. 4.7)[228]

Gesundheitsforschung erfolgt nur zu einem kleinen Teil ausschließlich innerhalb einer abgeschlossenen Institution. Erkenntnisgewinne sind oft davon abhängig, dass ein Austausch auf nationaler, europäischer und internationaler Ebene stattfindet und gemeinsame Analysen und Auswertungen vorgenommen werden. Um auf große Datenbestände zurückgreifen zu können, haben sich nationale und übernationale Forschungsnetzwerke und Forschungsregister entwickelt, wobei nicht nur auf eigene Forschungserhebungen zurückgegriffen wird. Vielfach basiert die Forschung auf Daten aus dem Behandlungs-, dem Pflege-, dem privaten oder gar dem Konsumbereich.[229]

Ein auf Big Data basierender Forschungsansatz sind Kohortenstudien. Ein Beispiel hierfür ist das 2014 gestartete Projekt der „Nationalen Kohorte“, bei dem Erbgut und Gesundheit von 200.000 Teilnehmern über Jahrzehnte hinweg untersucht werden sollen, um neue Erkenntnisse über die Genese und den Verlauf von Volkskrankheiten wie Diabetes, Herz-Kreislauf-Erkrankungen, Krebs, Demenz- und Infektionskrankheiten zu gewinnen.[230]

Neue Erkenntnisse erhofft man sich von der Digitalisierung medizinischer Behandlungsakten und deren massenhafter Auswertung für wissenschaftliche Zwecke. In Krebsregister fließen seit vielen Jahren schon Behandlungsdaten in große Datenbestände ein und werden der Forschung zur Verfügung gestellt. Seit Juli 2017 fördert das Bundesministerium für Bildung und Forschung (BMBF) umfänglich die Medizininformatik-

224 Verordnung EG Nr. 1338/2008 zu Gemeinschaftsstatistiken über öffentliche Gesundheit und über Gesundheitsschutz am Arbeitsplatz i. V. m. Verordnung EU Nr. 2015/359 v. 4.3.2015.

225 Poppenhäger in Roßnagel Kap. 8.10 Rn. 40 ff. (S. 1639 ff.).

226 Verordnung EG Nr. 1338/2008 zu Gemeinschaftsstatistiken über öffentliche Gesundheit und über Gesundheitsschutz am Arbeitsplatz; zum Vorstehenden insgesamt Statistisches Bundesamt, Statistisches Jahrbuch 2017, S. 150 ff.

227 Von Kalle/Ücker/Eils/Winkler/Schickhardt in Stiftung Datenschutz (2017) S. 85.

228 Rienhoff, EHEALTHCom 02_03/16, 26; beispielhafte Projekte bei Strategy/pwc S. 77 ff.

229 Deutscher Ethikrat S. 61.

230 Schepers/Peuker in Langkafel S. 41 ff.; Von Kalle/Ücker/Eils/Winkler/Schickhardt in Stiftung Datenschutz (2017) S. 89 f.; Deutscher Ethikrat S. 64.

Initiative, in der zunächst 17 deutsche Universitätskliniken gemeinsam mit externen Partnern so genannte „Datenintegrationszentren“ (DIZ) zum standortübergreifenden Managen und Teilen medizinischer Daten aufbauen.[231] Letztlich zielen derartige Forschungsprojekte insbesondere darauf ab, die Behandlungsmethoden zu verbessern.[232] Die Auswertung von klinischen Behandlungsdaten für Forschungszwecke beschränkt sich also nicht auf die Dokumentation von Krebserkrankungen[233], sondern erfolgt über unterschiedlichste interne sowie institutionsübergreifende Forschungsprojekte, wobei auf Einwilligungen sowie auf unterschiedlichste gesetzliche Grundlagen zurückgegriffen wird und zurückgegriffen werden muss (s. u. 10.8).

Im European Genome-phenome Archive (EGA) werden Rohdaten für genetische Forschungsprojekte gespeichert, die auf Anfrage Konsortiumsmitgliedern und Patienten zugänglich gemacht werden. Die Sammlung umfasst ca. 3.500 Datensätze aus über 1.500 Studien. Neben einem frei zugänglichen Bereich gibt es auch einen Bereich mit beschränktem Zugang, der derzeit über 400 Datenzugriffsausschüsse geregelt wird.[234]

Um die Umsetzung medizinischer Forschungserkenntnisse in der Praxis zu gewährleisten, wurde 1998 das Cochrane-Zentrum in Freiburg gegründet, dessen Funktion es ist, angesichts des Dschungels von Studien im Gesundheitsbereich unabhängige wissenschaftliche Bewertungen zum Erfolg von Behandlungsmethoden vorzunehmen und zugänglich zu machen. Die in vielen Staaten vertretenen Cochrane-Zentren haben Kriterien für evidenzbasierte Medizin (EbM) erarbeitet, die weltweit zum Einsatz kommen. Die Wirksamkeitsüberprüfungen haben zudem das Potenzial, die Kosten der Behandlung dadurch zu verringern, dass die Wirksamkeit und die Kosten z. B. von Arzneimitteln zueinander in ein Verhältnis gesetzt werden (s. u. 10.2). Die bisher nur kurzfristige Sicherstellung der Finanzierung des Cochrane-Zentrums in Freiburg wurde durch eine auf 10 Jahre angelegte Unterstützung aus Steuermitteln verstetigt.[235]

3.13 Pharma- und Medizinprodukteunternehmen

Die Pharmaindustrie betreibt Forschung und Entwicklung (F+E, Research and Development, R+D). In diesem Kontext werden eigene Biodatenbanken geführt bzw. es finden Kooperationen mit Forschungs- und Behandlungseinrichtungen statt.[236] Die systematische Analyse von klinischen Prüfdaten ist für die Pharmaindustrie seit vielen Jahren ein gängiges Geschäft. Dabei handelte es sich zunächst um abgegrenzte Auswertungen streng strukturierter und qualitätsgesicherter Daten. Diese Tätigkeit wird mit Big Data ausgeweitet und vertieft. Darüber werden klinik-, arzneimittel- ja sogar konzernübergreifende Analysen möglich. Neben den Ergebnissen von klinischen Tests (clinical trials) werden strukturierte und unstrukturierte Daten aus dem Forschungs- und

231 https://www.bmbf.de/de/bessere-therapien-dank-medizininformatik-4473.html
232 Schepers/Peuker in Langkafel S. 44 ff.
233 Dazu auch Von Kalle/Ücker/Eils/Winkler/Schickhardt in Stiftung Datenschutz (2017) S. 87 ff.
234 Deutscher Ethikrat S. 63 f., 66.
235 Bartens, Sauberes Wissen für die Medizin, SZ 26.1.2018, 16.
236 Beispiel für eine unzulässige Verarbeitung in ULD, Tätigkeitsbericht 2015, Kap. 4.6.6 (S. 61 f.).

dem Behandlungsbereich, aus DNA-Tests oder aus anderen Quellen in Wirkstoffanalysen mit einbezogen.[237]

Verschreibungspflichtige **Arzneimittel** unterliegen einer Kennzeichnungspflicht auf Verpackungsebene. Damit wird zum einen das Inverkehrbringen von Fälschungen zu verhindern versucht. Eine weitere Funktion des Verfolgens der Logistikkette von Arzneimitteln besteht darin, im Fall von unerwünschten Arzneimittelwirkungen deren Weg von der Produktion über die Distribution bis zur Einnahme nachvollziehen und damit evtl. die Ursache der Schäden feststellen zu können. Das jeweilige Arzneimittel kann während der gesamten Wertschöpfungskette unter Bezugnahme auf den jeweiligen Akteur authentifiziert und verfolgt werden. Auf diese Weise können auch Arzneimittel gezielt wieder aus dem Verkehr genommen werden, z. B. wenn das Verfallsdatum überschritten wurde oder unerwartete Wirkungen in einer Charge aufgetreten sind. Die Arzneimitteldaten können letztlich elektronisch im Patienten-Daten-Management-System (PDMS) der verabreichenden Einrichtung, etwa des Krankenhauses oder der Pflegeeinrichtung, dokumentiert werden. Die im Rahmen dieser Medikamentenlogistik anfallenden Daten können auch zur Überprüfung der Wirksamkeit der Medikamente sowie zur Auswertung für Hersteller, Verbände wie Kliniker genutzt werden (s. u. 10.2).[238]

Entsprechende, in geringerem Maße regulierte Prozesse gibt es für die Entwicklung, Produktion und den Einsatz von **Medizinprodukten**. Medizinprodukte der Klasse III, wozu Herzschrittmacher, Stents, künstliche Gelenke und Elektroden gehören, werden auf Chargenebene gekennzeichnet. Teilweise erfolgt auch eine detailliertere Kennzeichnung auf Produktebene (s. u. 10.3).[239]

Es ist nicht nur feststellbar, dass sich IT-Unternehmen zunehmend mit Gesundheitsthemen befassen (s. u. 3.14); umgekehrt drängen Pharmaunternehmen immer stärker in die informationstechnische Bearbeitung ihres bisherigen biochemischen Tätigkeitsfeldes. Die Novartis AG, einer der weltweit größten Pharmakonzerne, begann 2010 damit, **Mikrochips in Medikamente** einzubauen (Smart Pills), die nach der Einnahme Messewerte aus dem Innern des Körpers erfassen und an ein ärztliches Empfangsgerät übermitteln (sog. Insideables). Damit kann die Wirkung von Medikamenten „vor Ort" überprüft werden oder, ob ein Patient regelgemäß bestimmte Medikamente einnimmt.[240]

Auch **jenseits von F+E** wird Big Data in der Pharmaindustrie umfassend eingesetzt. Das beginnt in der Personalentwicklung, wo z. B. zwecks Recruitment Kongress-, Patent- und Personalunterlagen wie wissenschaftliche Veröffentlichungen analysiert werden.[241] Auch im Vertrieb wird Big Data eingesetzt, um auf der Basis detaillierter Analysen potenzielle

237 Bange, Big Data revolutioniert die Pharmabranche, www.bi-scout.com 24.2.2017; Ottleben, Big Data weist der Pharmaindustrie in die Zukunft, www.laborpraxis.vogel.de 19.6.2017.
238 Laslo in Langkafel S. 195 ff.
239 Laslo in Langkafel S. 201.
240 Microchip kontrolliert Medikamenteneinsatz im Körper, DANA 2010, 165 f.
241 Bhardway, Zeitgemäße Datenanalyse in der Pharmaindustrie, industrie.de 19.10.2016.

Produktabnehmer im Bereich der medizinischen Leistungserbringer oder aber die Endverbraucher direkt anzusprechen (s. u. 4.8, 4.9).

3.14 Portalanbieter

Mit dem Bedeutungszuwachs des Internets für den Gesundheitsbereich hat die Rolle der Internetportalanbieter mit ihren speziellen wie allgemeinen Diensten an Wichtigkeit gewonnen.[242] Diese Dienste adressieren sowohl Gesundheitsdienstleister wie auch den Endkunden als Verbraucher bzw. Betroffenen. Im Folgenden sollen vorrangig die Angebote für den Endkunden behandelt werden. Diese umfassen inzwischen praktisch alle mit digitalen Diensten erbringbaren Funktionen, u. a. Kommunikation (z. B. soziale Netzwerke), die Cloudspeicherung (persönliche Patientenakte), Adressverwaltung, Zeitplanung (Kalender), Informationssuche oder Navigation.

Das Internet ist eine große Wissensquelle für den Gesundheitsbereich, über die sich Experten wie Laien informieren können. Aus gesundheitsrelevanten Suchanfragen und Kommunikationsangaben lassen sich gesundheitsbezogene Rückschlüsse ziehen. Die Vermittlung von Wissen in diesem Bereich ist nicht trivial. Die Kompetenz von Patienten wird erhöht. Zugleich besteht die Gefahr, dass die beschränkte Fähigkeit der Ein- und Zuordnung der Informationen zu gravierenden Fehleinschätzungen führt, so dass Ärzte ironisch die Meinung vertreten, es bedürfe der Einführung einer neuen Abrechnungsziffer „Entgoogeln".[243]

Der Umstand, dass Menschen diese Dienste nutzen und dass damit deren Daten, auch ihre Gesundheitsdaten, Portalanbietern zur Kenntnis gelangen und von diesen kommerziell weiterverwendet werden, ist kein Hinweis darauf, dass die Betroffenen ihre Vertraulichkeitserwartung aufgäben. Es kann auch keine Rede davon sein, dass wir uns in einem Zeitalter des „Post Privacy" befänden, in dem Öffentlichkeit vor Privatsphäre käme und informationelle Selbstbestimmung durch kollektive Datenverarbeitung abgelöst würde.[244]

Die großen US-amerikanischen IT-Konzerne investieren durchgängig in die Entwicklung medizinischer Anwendungen und stellen hierfür Mediziner, Chemiker und Biologen ein. Diese Entwicklung, von der z. B. Google, Amazon, Facebook, Microsoft und Apple erfasst sind, wird von der Idee befeuert, dass die Dechiffrierung der Biologie, das Verständnis von Krankheiten und der Schlüssel für deren Bekämpfung ein Datenproblem sei, das im Wesentlichen von Softwareexperten gelöst werden könne.[245] Selbst die

242 Deutscher Ethikrat S. 13 f.

243 Müller, App auf Rezept, Der Spiegel 29/2017, 70.

244 Raum in Stiftung Datenschutz (2017) S. 124; Schaar u. Schramm in Stiftung Datenschutz (2016) S. 93 ff. u. S. 103 ff.; Weichert DuD 2012, 718; Schneider/Härting CR 2015, 819; Heller, Post-Privacy: Prima leben ohne Privatsphäre, 2011

245 Schulz, Computer gegen Krebs, Der Spiegel 45/2017, 69; Deutscher Ethikrat S. 76.

Fahrdienstvermittler Uber engagiert sich im Health-Care-Bereich und bewirkt damit dessen teilweise Entprofessionalisierung.[246]

Googles Vorstandschef Larry Page erklärte im Jahr 2014: „Im Moment analysieren wir keine Daten aus dem Gesundheitswesen. Täten wir dies, könnten wir jedes Jahr 100.000 Leben retten."[247] Page hatte dabei Google Flu Trends (GFT) im Blick. Dieses Angebot zielt darauf ab, aus der Auswertung von Internetsuchen Indikatoren für Epidemien abzuleiten. Zunächst meinte man euphorisch, darüber innerhalb eines Tages akkurate Aussagen zum Ausbruch z. B. von Grippeerkrankungen vornehmen zu können, um zeitnahe Vorkehrungen treffen bzw. Maßnahmen ergreifen zu können. Eine distanzierte Bewertung zeigte dann aber, dass solche Verfahren gewisse Hinweise geben können, dass sie aber auch stark fehler- und manipulationsanfällig sind. Inzwischen wurde GFT durch das Prognosemodell ARGO abgelöst.[248]

Google bietet inzwischen eine große Zahl spezieller medizinischer Anwendungen an, z. B. Arztkonsultationen per Videochat.[249] Google stellt Internetnutzenden, bei denen sich Hinweise auf Depression zeigen, einen „PHQ-9-Fragebogen" bereit, der im klinischen Bereich entwickelt wurde und mit dem die Betroffenen erkennen können sollen, ob die Inanspruchnahme eines Arztes angezeigt ist.[250]

Die auf KI spezialisierte Google-Tochtergesellschaft Deep Mind arbeitet schon längere Zeit mit dem staatlichen britischen National Health Service (NHS) zusammen und stellt u. a. Medizinern die Applikation „Streams" zur Verfügung, die die Anfälligkeit für akutes Nierenversagen berechnet. Als Referenzdatenbank hat die NHS Deep Mind die Patientendatensätze von 1,6 Mio. Patienten zur Verfügung gestellt, was rechtlich in Frage gestellt wird. Ein Sprecher von Deep Mind erklärte, dass die Daten „niemals für kommerzielle Zwecke verwendet oder mit Google-Produkten, -Diensten oder Werbung kombiniert worden sind – und es niemals werden".[251]

Unter der Parole „Healthcare Next" betreibt Microsoft einige Dutzend Medizinprojekte. Dabei geht es um so unterschiedliche Anwendungen wie medizinische Spracherkennung, über die Ärzte ihre Beobachtungen während laufender Untersuchungen direkt in den Computer diktieren, personalisierte Medizin und den Einsatz von KI bei der Behandlung. Ein Schritt zum umfassenden KI-Einsatz ist die Erfassung von Milliarden Seiten wissenschaftlicher Literatur zu biologischen Prozessen, therapeutischen Mechanismen und klinischen Studien, die mit semantischen Methoden erschlossen werden. Mit der Online-App Healthvault – einem Gesundheitsschließfach – ermöglicht es Microsoft den Patienten

246 Lorenz, Stop Comparing Healthcare Startups To Uber, www.forbes.com 23.5.2017.
247 Zit. nach Mühl, Die Vermessung des Körpers, FAZ 16.07.2014 = www.faz.net 17.07.2014.
248 Langkafel in Langkafel S. 20 ff.; Raum in Stiftung Datenschutz (2017) S. 137.
249 Google bietet Arztsprechstunde per Videochat, DANA 2014, 171 f.
250 Weber, Der Test der Datenkrake, SZ 16./17.9.2017, 37.
251 1,6 Mio. PatientInnendaten des NHS für Deep Mind, DANA 2017, 105 f.

bzw. Menschen generell, ihre sensitiven medizinischen Daten zentral in der Cloud zu speichern und bei Bedarf z. B. Ärzten bereitzustellen.[252]

Das sog. soziale Netzwerk Facebook mit inzwischen 2 Mrd. aktiven Mitgliedern weltweit, nimmt, soweit Gesundheitsdienstleister das Netzwerk nutzen, keine Rücksicht auf die Vertraulichkeitserwartungen der Kunden der über die Plattform agierenden Dienstleister.[253] Anhand der Nutzungsdaten werden Untersuchungen durchgeführt, um Rückschlüsse auf sexuelle Vorlieben, psychologische Dispositionen und vieles mehr abzuleiten.[254] Das Unternehmen setzte sein Netzwerk gezielt ein, um verdeckt mit Posts psychologische Tests an den Mitgliedern durchzuführen.[255] Der ehemalige Präsident und Mitgründer von Facebook Sean Parker erklärte, dass man bei der Konzeption ganz bewusst auf Suchtfaktoren und süchtig machende Features gesetzt habe, welche „die Verwundbarkeit der menschlichen Psyche" ausnutzen. Ähnlich äußert sich der ehemalige Vizepräsident von Facebook Chamath Palihapitiya, wenn er sagt: „Facebook programmiert die Menschen."[256] Gründer Mark Zuckerberg finanziert den Aufbau eines „menschlichen Zellatlas" und lässt ein mit 600 Mio. US-Dollar ausgestattetes Forschungszentrum u. a. alle Zellen kartografieren, wodurch neue Medikamente möglich werden sollen. Der oben erwähnte Ex- Facebook-Präsident Sean Parker hat ein nach ihm benanntes Institut für Krebsimmuntherapie auf den Weg gebracht.[257]

Das Healthkit von Apple ist eine zentrale Sammelstelle für unterschiedlichste Gesundheitswerte der Nutzer der Smartphones dieses Unternehmens. Die Daten werden über Mobilgeräte und Applikationen erzeugt und sowohl Apple, den Applikationsanbietern wie auch den Betroffenen über Apples Health-App unter Einsatz des Smartphone-Betriebssystems iOS zur Kenntnisnahme und zur weiteren Analyse bereitgestellt. Ein entsprechendes Angebot besteht für Android-Smartphones mit „Google Fit".[258] Apple startete in den USA einen Dienst, mit dem es dem Nutzer jederzeit und überall möglich sein soll, auf seine „Health Records" per iPhone oder iPad in vertraulicher Weise zuzugreifen, und kooperiert hierbei mit einigen der größten Lieferanten von Gesundheitsdaten, u. a. den Unternehmen Epic Systems, Cerner Corp und Athenahealth.[259]

Wegen des offensichtlichen Suchtpotentials der Nutzung von Apple-Geräten haben zwei Großinvestoren von Apple den Technologiekonzern aufgefordert, untersuchen zu lassen, wie sich die übermäßige Nutzung von Smartphones auf Jugendliche auswirkt und Sucht-

252 Schulz, Computer gegen Krebs, Der Spiegel 45/2017, 68 ff.
253 Facebook legt Patientenkontaktdaten offen, DANA 2017, 51 f.
254 Facebook-Psychologie, www.psychomeda.de/psychologie-blog/facebook-psychologie.html; Dambeck, Zeig mir deine Likes - und ich weiß, wer du bist, www.spiegel.de 11.03.2013.
255 Facebook experimentiert mit Mitgliedern, DANA 2014, 126 f.; Deutscher Ethikrat S. 139 f.
256 Graff, Asoziale Medien, SZ 15.12.2017, 11; Kreye, Risiken und Nebenwirkungen, SZ 16./17.12.2017, 4.
257 Schulz, Computer gegen Krebs, Der Spiegel 45/2017, 69.
258 Schumacher in Langkafel S. 238; Klose in Stiftung Datenschutz (2017) S. 103.
259 Apple startet neuen Dienst für Medizindaten, www.spiegel.de 25.1.2018.

Gegenmaßnamen zu ergreifen. Die beiden Fonds befürchten, dass das Thema negative Folgen auf den Aktienkurs von Apple haben könnte.[260]

Amazons Gesundheitsabteilung erprobt unter dem Codenamen 1492 virtuelle Arztbesuche, und wie sich medizinische Daten in großem Stil in der Cloud speichern und auswerten lassen. Der Konzern betätigt sich im Arzneimittel-Online-Handel, ohne dabei die strengen Anforderungen der beruflichen Schweigepflicht zu beachten.[261]

3.15 Gesundheits-Applikationsanbieter

Um den Einsatz von Smartphones, Fitness-Trackern und sonstigen Wearables hat sich ein großer Markt von Gesundheitsangeboten entwickelt, der mit den Begriffen „mobile Health" bzw. „mHealth" beschrieben wird. Hierzu gezählt werden können auch Gesundheitsanwendungen im „Smart Car", im „intelligenten Auto", etwa eine medizinische Basisuntersuchung des Fahrers jeweils zum Fahrtbeginn.[262] Mobile-Health-Angebote umfassen inzwischen über eine Millionen Dienstleistungen in den Bereichen Fitness, Gesundheit, Lifestyle, Sport und Medizin. Diese setzen regelmäßig auf den Betriebssystemen von Android (Google) und iOS (Apple) auf und erfassen über Sensoren Gesundheitsdaten und ermöglichen die Kommunikation hierüber.[263] In der im Auftrag des Bundesministeriums für Gesundheit erstellten Studie „Chancen und Risiken von Gesundheits-Apps" (CHARISMHA) wird ein Überblick über die Marktlage in Deutschland gegeben (zu Chancen und Risiken s. u. 4.5).[264] Internet-Plattformen wie HealthOn liefern Nutzern Hintergrund- und Test-Informationen über Health-Apps.[265]

Eine Weiterentwicklung im Bereich mobile Health ist „intelligente" Kleidung, sind sog. Smart Clothes. Dabei handelt es sich zumeist um Sportkleidung, in die Sensoren integriert sind, mit denen Körperfunktionen gemessen werden.[266] Es wird schon über ein digitales Netzwerk innerhalb des menschlichen Körpers („in-body internet") spekuliert, das Organe überwacht und koordiniert. Per Algorithmus kann dabei an die betroffene Person z. B. die Empfehlung oder Anweisung gegeben werden, was sie essen, welche Medikamente sie einnehmen oder wie sie sich verhalten sollte.

Betroffen von Gesundheits-Apps sind nicht nur die Anwender selbst, sondern potenziell auch deren Schutzbefohlene. Gemäß der Vorstellungen der Anbieter sollen Eltern ihre Kinder mit Gesundheitsüberwachungsinstrumenten unter Kontrolle behalten, etwa der App uGrow („Du wächst") von Philips, mit welcher unter dem Motto „Die App sagt dir, was dein Kind dir nicht sagen kann" jedes Detail eines Kleinkinderlebens aufgezeichnet und geteilt

260 Apple-Investoren beklagen iPhone-Sucht, SZ 9.1.2018, 1, 4.

261 Schulz, Computer gegen Krebs, Der Spiegel 45/2017, 69; Amazon-Apotheken wegen Schweigepflichtverletzung abgemahnt, DANA 3/2017, 163 f.

262 Müller, App auf Rezept, Der Spiegel 29/2017, 69.

263 Überblick bei Knoke, 1000 Schritte sollst du gehen, SZ 17./18.09.2016, 66; Schmundt, Falsch vermessen, Der Spiegel 3/2017, 107; Timm MedR 2016, 687 f.

264 http://www.charismha.de/; dazu Dostert, Downloads gegen den Schmerz, SZ 11.8.2017, 14.

265 www.healthon.de

266 Schmidt, Am Start, SZ 2016, 17.

werden kann: Stillzeit, Schlafdauer, Schlafposition, Essensmenge, Windelwechsel. Verhält sich das Baby ungewöhnlich, steht per Videotelefonat ein Arzt bereit. Auf der CES-Messe stellte ein US-Start-up einen „intelligenten Strumpf" für Kinder vor, der nachts Herzfrequenz, Temperatur, Sauerstoffversorgung und Schlafqualität des Kindes überwachen soll.[267]

Diese privat eingesetzten Applikationen werden teilweise kritisch bewertet. So wird vorgetragen, dass deren Einsatz zu einer **verstärkten Inanspruchnahme des Gesundheitssystems** führen könne, z. B. weil Fehlalarme ausgelöst werden, oder weil zu ärztlich unbegleiteten, gesundheitsgefährdenden Aktivitäten motiviert wird. Angesichts der grundrechtlichen Relevanz von eHealth-Applikationen wurde schon von verschiedenen Seiten gefordert bzw. vorgeschlagen, nicht nur Medizinprodukte, sondern generell mHealth-Anwendungen spezifischen Zertifizierungen, Zulassungsverfahren oder Kontrollverfahren zu unterwerfen.[268]

Ein sowohl informations- wie auch biotechnisch äußerst differenziertes Angebot wird mit **23andMe** erbracht. Diese Google-Ausgründung bietet seit 2009 nach Einsendung eines Direct-to-Consumer-(DTC-)Tests einer Speichelprobe eine individuelle Genomanalyse für 99 US-Dollar an. Dabei wurden zunächst detaillierte Auskünfte erteilt über potenzielle Krankheitsdispositionen und über darauf angepasste Verhaltensweisen. Wegen mangelnder Seriosität verbot die US-Aufsichtsbehörde Food&Drug Administration (FDA) im Jahr 2013 den weiteren Vertrieb des Tests.[269] Analysen zur genetischen Abstammung sowie die rohen DNA-Daten werden aber weiterhin über das Internet durch 23andMe vertrieben.

Genetische Lifestyle-Analysen finden immer wieder neue Anwendungsfelder und machen selbst vor Kindern nicht Halt: Das US-amerikanische Start-up Orig3n bietet z. B. Gentests wie das Programm „Child Development" an, das Aufschluss geben soll, welche Sportart zum Kind passt, ob es ein Mathe-Genie wird, Lernschwächen drohen oder eine Anfälligkeit für bestimmte Krankheiten vorliegt. Der Test „Behavior" verspricht Auskunft, ob ein Kind suchtgefährdet ist, zu Panikattacken neigt oder ein Aggressionsproblem entwickeln könnte.[270]

---

267 Hulverschmidt/Schieder, Der Spion in der Wiege, SZ 13./14.1.2018, 25.

268 Rebitschek/Gigerenzer/Wagner, Kritische Voraussetzungen für ein digitales Gesundheitswesen in Deutschland, ZBW Leibnitz-Informationszentrum Wirtschaft, Wirtschaftsdienst 2017 (10), 702 f.; Raum in Stiftung Datenschutz (2017) S. 133; Gaßner/Strömer VersR 2015, 1220; vgl. Grünbuch der Europäischen Kommission über Mobile-Health-Dienste, COM(2014)219final S. 4; vgl. Düsseldorfer Kreis, Orientierungshilfe zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter v. 16.6.2014; Artikel-29-Arbeitsgruppe, Stellungnahme 02/2013 zu Apps auf intelligenten Endgeräten v. 27.2.2013; von Riegen, Datenschutzbeauftragter schlägt Gütesiegel für Gesundheits-Apps vor, wwww.heise.de 6.11.2017; Siegel für Gesundheits-Apps? DANA 2015, 179; Weichert, mHealth und der Datenschutz, KVB Forum 9/2014, 12 f.

269 23andMe Gentest-Firma zwischen Verbot und Verheißung, DANA 2014, 38 ff.; Langkafel in Langkafel S. 34 f.; Deutscher Ethikrat S. 62; Schmergal, In der App-Falle, Der Spiegel 17/2017, 41.

270 Hulverschmidt/Schmieder, Der Spion in der Wiege, SZ 13./14.1.2018, 25.

3.16 Anbieter der Big-Data-Technik

Bei den wichtigen Anbietern von Big Data handelt es sich durchgängig um IT-Unternehmen, die ihr informationstechnisches Know-how, ihre Software und Hardware den Anwendern zur Verfügung stellen, die dann ihre Daten einführen und verarbeiten. Regelmäßig unterscheiden sich diese Technologieanbieter von den Anwendern. Teilweise sind aber auch Big-Data-Analysen Bestandteil eines umfassenderen Dienstleistungsangebots. Dies gilt z. B. für Portalanbieter (s. o. 3.14), Gesundheitsapplikationsanbieter (s. o. 3.15) oder Unternehmen aus dem Bereich medizinischer Marktforschung (s. u. 4.8).

Das in Deutschland führende Unternehmen für Big Data im Gesundheitsbereich ist SAP, das mit seinen HANA-Produkten in vielen Gesundheitssektoren vertreten ist, so u. a. in der Medizinforschung, in der Krebsdiagnostik, bei Krankenkassen oder bei der Verschreibungsanalyse.[271] Ein weiterer solcher deutscher Anbieter ist Siemens[272] oder Datapine. Viele weltweit tätigen Analytics-Anbieter haben ihren Sitz in den USA, einige dieser Unternehmen stellen ihre Dienste in der Cloud bereit, etwa Oracle oder SAS. Weitere große Anbieter sind u. a. IBM, CSC oder Cardadigm.[273] Aus den USA kommen auch IT-Unternehmen mit Big-Data-Angeboten, die selbst Gesundheitsanwendungen einsetzen. Dies gilt z. B. für Microsoft und Google.

3.17 Arbeitgeber und Betriebsärztliche Dienste

Big Data hat auch im Verhältnis zwischen Arbeitgeber und Beschäftigten Einzug gehalten. Mit Hilfe von Datenanalysen versuchen Unternehmen ihre Personalentscheidungen zu optimieren, z. B. bei der Bewerberauswahl, bei Beförderungen oder bei Maßnahmen der Mitarbeiterbindung. Im Rahmen der Überwachung der Produktions-, Logistik- oder sonstiger Prozessabläufe erfolgt oft indirekt, manchmal aber auch gezielt eine Verhaltens- und Leistungskontrolle der Beschäftigten. Dabei finden auch sensitive Daten Eingang in die Auswertung, etwa zur Gewerkschaftszugehörigkeit oder zur Gesundheit.[274] Die Einbeziehung von Gesundheitsdaten wird u. a. damit gerechtfertigt, dass ein besonderes Risiko am Arbeitsplatz besteht oder dass die Gesundheit und die Leistungsfähigkeit des Beschäftigten zentrale Aspekte für eine regelgerechte Beschäftigung seien. Die Verarbeitung erfolgt beim Arbeitgeber im Produktionsprozess sowie in der Personalverwaltung. Über Datenanalysen (People Analytics) werden Personal-, Unternehmens- und sonstige Daten miteinander verknüpft, um Unternehmens- und insbesondere Personalentscheidungen zu unterstützen.[275]

Hinsichtlich der Verarbeitung von Gesundheitsdaten gibt es Sonderregelungen, soweit die Verarbeitung beim Betriebsarzt erfolgt. Anzuwenden ist hier insbesondere das

271 Eberhardt in Langkafel S. 133 ff.
272 Zimmermann-Rittereiser/Schaper in Langkafel S. 155 ff.
273 Von Grätz, Findungsprozesse, EHealthCom 5/2014, 14 ff.
274 Dzida NZA 2017, 541 ff.; Deutscher Ethikrat S. 71.
275 Dzida NZA 2017, 542.

Arbeitssicherheitsgesetz (ASiG). Außerdem gilt für den Betriebsarzt die berufliche Schweigepflicht (s. u. 6.8). Das Patientengeheimnis ist eine Verpflichtung, die einer Big-Data-Nutzung entgegensteht. Regelmäßig bedarf es hierfür der Einwilligung der Betroffenen in der spezifischen Form einer Schweigepflichtentbindung.[276]

Die Erfassung von Gesundheitsdaten durch Arbeitgeber beginnt regelmäßig schon bei der Bewerbung und im Einstellungsverfahren. Dabei werden immer wieder Daten in großem Umfang und einer großen Tiefe erhoben, ohne dass dies mit der Begründung des Arbeitsverhältnisses gerechtfertigt werden kann.[277] Die Möglichkeiten sowie die Begehrlichkeiten, mit Hilfe von Big Data gesundheitsrelevante Aspekte einzubeziehen sowie hierzu Analyseangebote von kommerziellen Unternehmen zu nutzen, nehmen zu.[278]

Während des Arbeitsverhältnisses werden Daten über den Arbeitnehmer, die Erbringung seiner Arbeitsleistung sowie zum Arbeitsplatz und die damit verbundenen Prozesse Daten erfasst. Die Flexibilisierung von Arbeitszeiten und der Arbeitsorte, die Nutzung digitaler Unternehmenstechnik außerhalb der Arbeit sowie die dienstliche Nutzung privater Geräte (bring-your-own-device – BYOD) führen dazu, dass die klare Trennung zwischen Arbeit und Freizeit aufgehoben wird. Erfasst werden dabei oft auch Gesundheitsdaten, etwa Angaben über krankheitsbedingte Abwesenheiten.[279] Durchgeführte Gesundheitsanalysen erfolgen oft nicht ausschließlich im Interesse des Arbeitgebers. Arbeitnehmer können hiervon profitieren, z. B. durch Vorsorgeprogramme oder durch eine angepasste Gestaltung des Arbeitsplatzes oder der Arbeitszeiten.[280] Sie können aber auch die Grundlage für offene oder verdeckte Diskriminierungen sein.

Eine spezifische Form einer gesundheitlichen Beschäftigtenüberwachung sind die Doping-Kontrollen bei Leistungs- und Spitzensportlern. Diese haben eine globale normative Grundlage im Code der World Anti-Doping Agency (WADA) und zugleich in Deutschland auf nationaler Ebene durch das Anti-Doping-Gesetz.[281] Bei Profisportlern, z. B. Fußballspielern in den oberen Spielklassen, erfolgt regelmäßig eine umfassende Erfassung sowohl der Trainings-, Vorbereitungs- und Spieltätigkeit mit Hilfe von Big Data, wobei viele höchstpersönliche Angaben über die körperliche und seelische Verfassung einfließen.[282]

---

276 Weichert in Kühling/Buchner Art. 9 Rn. 49, 146.

277 Intimer Gesundheitscheck bei Beschäftigteneinstellung, DANA 2010, 27 f.; Bluttests beim NDR, DANA 2010, 28; Daimler verlangt Blutproben von BewerberInnen, DANA 2009, 152.

278 Deutscher Ethikrat S. 74 f.

279 Bahn sammelt Daten kranker Mitarbeiter, DANA 2009, 109 f.; Drogeriekette Müller erfasst systematisch Krankengeschichten, DANA 1999, 71; Daimler speichert Krankendaten, DANA 2009, 73; Daimler speichert unzulässig Daten über kranke MitarbeiterInnen, DANA 2009, 26.

280 Deutscher Ethikrat S. 75.

281 Anti-Doping-Gesetz v. 10.12.2015, BGBl. I S. 2210; Kornbeck, Einwilligung oder gesetzliche Regelung? DANA 2017, 17 ff.; Schlarmann ZD 2016, 572 ff.; Mortsiefer, Datenschutz im Anti-Doping-Kampf, 2011; Niewalda, Dopingkontrollen im Konflikt mit allgemeinem Persönlichkeitsrecht und Datenschutz, 2011'; Weichert, Dopingbekämpfung und Persönlichkeitsschutz, DANA 2011, 166 f.; ders., Datenschutz im Anti-Doping-Kampf, DuD 2011, 702 ff.

282 Laukenmann, Die Entschlüsselung des Fußballs, SZ 10.11.2017, 16.

In den USA ist die Gesundheitskontrolle von Beschäftigten durch die Arbeitgeber umfassender und weniger eingeschränkt als in Deutschland. Beschäftigte werden zunehmend gedrängt, an firmeninternen Vorsorgeuntersuchungen, biometrischen Tests und Gesundheitskursen teilzunehmen, um so die Kosten für die Krankenversicherung zu reduzieren.[283] Firmen wie Walmart oder Time Warner nehmen die Dienste von Gesundheitsanalysefirmen wie Castlight Health in Anspruch, um sich über mögliche Schwangerschaften von Angestellten zu informieren.[284] 2017 wurde ein Gesetz verabschiedet, das es Unternehmen künftig erlaubt, von Beschäftigten Gentests zu verlangen bzw. deren Ergebnisse offenzulegen, indem im Weigerungsfall höhere Versicherungskosten geltend gemacht werden können.[285]

3.18 Der „Betroffene“

Es gibt wohl kaum eine Institution, die nicht öffentlich den Anspruch für sich formuliert, im Interesse und zum Wohl der Betroffenen zu handeln. Dies gilt insbesondere im Gesundheitsbereich, wo durchgängig die Behauptung in den Raum gestellt wird, im Interesse des Patienten und dessen körperlichen und seelischen Wohls zu handeln. Bei anderen Verarbeitungen wird das Konsum-, das Komfort- oder das Unterhaltungsinteresse des Betroffenen an der digitalen Verarbeitung von Gesundheitsdaten betont. Im Konsumbereich „profitiert“ der Verbraucher, in Beschäftigungsverhältnissen der Arbeitnehmer. Dabei ist der Betroffene aber regelmäßig nur Objekt; der Verarbeiter erklärt zu wissen, was für diesen gut oder schlecht ist. Die Bestimmungsmacht über den Betroffenen basiert auf der bei digitalen Anwendungen regelmäßig bestehenden Informations- und Machtasymmetrie zwischen Verantwortlichem bzw. Verarbeiter und dem Betroffenen.[286]

Diese Asymmetrie hat mehrere Dimensionen: Den Betroffenen fehlen zumeist die finanziellen, die technischen wie die kognitiven Ressourcen für ein selbstbestimmtes Handeln. Hinsichtlich der Kenntnisse fehlt es oft an den technischen Grundkenntnissen, an den Kenntnissen über die verwendeten Verfahren, über die organisatorischen und ökonomischen Hintergründe und Strukturen und zumeist über die rechtlichen Rahmenbedingungen, Zwänge und Möglichkeiten. Von „selbstinduzierter Fremdbestimmung“ ist die Rede, wenn trotz dieses Ungleichgewichts der Betroffene sich auf derartige Verarbeitungen einlässt.[287] Es ist nun das Anliegen des Datenschutzes, des Verbraucherschutzes, des Arbeitnehmerschutzes wie auch des Patientenschutzes, diese Fremdbestimmung zurückzudrängen und die tatsächlichen Erwartungen und Interessen der

283 Firmen drängen Beschäftigte zu Gesundheitstests, DANA 2016, 103.
284 Deutscher Ethikrat S. 75.
285 Viciano, Gentest sind Privatsache, SZ 18./19.3.2017, 33; Arbeitgeber dürfen Gentes fordern, DANA 2017, 106.
286 Mühlbacher/Kaczynki in Langkafel S. 244.
287 Deutscher Ethikrat S. 80.

Betroffenen stärker zu berücksichtigen. Dies kann dadurch erreicht werden, dass für die Betroffenen Transparenz und Wahlmöglichkeiten verbessert werden.[288]

Der Betroffene ist als System- oder Verfahrensnutzer, aber auch im datenschutzrechtlichen Sinn, digitales Subjekt. Dies kommt vor allem zum Tragen, wenn er sich selbst organisiert, sich in Gruppen zusammenschließt und kommuniziert. Im Gesundheitsbereich erfolgt eine kollektive Selbstorganisation oft in virtuellen Selbsthilfegruppen zum Erfahrungsaustausch und zur Wahrnehmung gemeinsamer Interessen.[289]

Der Betroffene ist derjenige, der über die Einwilligung (s. u. 8.8) oder über Vertragsregelungen (s. u. 7.4) in Bezug auf die Verarbeitung bei Verantwortlichen ein (Mit-) Bestimmungsrecht hat und wahrnehmen kann.[290] Er kann durch seine Einwilligung oder durch sonstige Maßnahmen dafür sorgen, dass Daten oder Gewebeproben für Big Data zur Verfügung gestellt werden, etwa um den medizinischen Fortschritt voranzubringen.[291] Er ist zumeist Eigentümer des Endgeräts, über das Daten generiert werden und bestimmt als „Skribent" hierüber durch sein Verhalten mit.[292] Es wird deshalb auch als „Prosument" bezeichnet.[293] Er entscheidet sich – mehr oder weniger bewusst – durch sein Verhalten für oder gegen den Einsatz eines Systems oder Verfahrens. Inwieweit er seine eigenen Vorstellungen und Wünsche einbringen kann und diese berücksichtigt werden, wird zwar weitgehend durch das Marktangebot vorgegeben. Seine Vorstellungen und Wünsche können direkt und ausdrücklich erhoben und gespeichert werden; sie können sich aber auch implizit aus dem Verhalten ergeben und bedürfen dann zumeist der Interpretation. Der Prosument kann aber auch – zumindest in einem gewissen Maße – für das Marktangebot bestimmend sein. Dies ist insbesondere dann der Fall, wenn seine Interessen kollektiv organisiert, kommuniziert und rechtlich durchgesetzt werden.[294]

Die Selbstbestimmungsmöglichkeit der Betroffenen verbessert sich potenziell mit der Differenzierung des Marktes der (zumeist mobilen) Endgeräte und der darauf laufenden Applikationen. Der Betroffene handelt zugleich als Verarbeiter und Anwender wie als Kunde, als Subjekt und als Objekt. Durch die Auswahl des Geräts, der genutzten Programme und der dadurch ermöglichten Einstellungen könnte er z. B. bestimmen, ob eine Lokalisierung möglich ist, welche Sensoren aktiviert werden, ob, wie und wie lange und für welchen Zweck Daten geräteseitig oder in der Cloud bzw. beim Dienstanbieter verarbeitet werden.

288 Müller in Stiftung Datenschutz (2017) S. 109 ff.
289 Deutscher Ethikrat S. 24.
290 Deutscher Ethikrat S. 169 ff.
291 Deutscher Ethikrat S. 115.
292 Heckmann/Paschke in Stiftung Datenschutz (2017) S. 81 f.
293 Müller in Stiftung Datenschutz (2017) S. 112.
294 Mühlbacher/Kaczynki in Langkafel S. 243 ff.; Deutscher Ethikrat S. 78 ff.

Im Bereich der Verarbeitung von Gesundheitsdaten kann grob zwischen zwei Funktionen unterschieden werden: Im Lifestyle-Bereich steht das Konsuminteresse des Betroffenen im Vordergrund; die Diensteanbieter sind vorrangig Informationsanbieter. Die z. B. mit Armbändern erfassten Schlafdaten können genutzt werden, um sich mit einem künstlichen Sonnenaufgang synchron zur Leichtschlafphase aufwecken zu lassen. Die Anbieter von Videospielen oder Musik-Streaming-Diensten nutzen erfasste Körperwerte, um den Spannungsverlauf ihrer Spiele oder die Auswahl der vorgeschlagenen Musik an das aktuelle Befinden des Nutzers anzupassen.[295]

Bei speziellen Medizinangeboten dominieren (noch) medizinische Anbieter. Die Grenzen dazwischen sind fließend. Bei den medizinischen Anwendungen stehen die Gesundheitsinteressen des Betroffenen im Vordergrund. Der Anwender hat die Möglichkeit, die behandlungsrelevanten Daten wie z. B. zu Blutdruck oder Blutzucker mit seinem Arzt zu teilen. Bereits 2014 berichteten 70% der US-amerikanischen Ärzte, dass einer oder mehrere ihrer Patienten selbst erhobene Daten zu seiner Gesundheit mit ihnen teilt. 75% der Ärzte waren der Meinung, dass dies zu besseren Ergebnissen für den Patienten führt.[296]

Technischer Anknüpfungspunkt sind bei beiden Funktionalitäten zumeist die eigenen Mobilgeräte, das Smartphone, sog. Wearables und/oder ein winziges Sensor-Pflaster. Fehlt dem mobilen Sensor ein Betriebssystem oder eine eigene IT-Infrastruktur, so erfolgt eine Kommunikation zumeist über Funkschnittstellen (z. B. Bluetooth) mit einem Smartphone oder einem sonstigen Gerät des Betroffenen, von wo aus die Daten an IT- oder gesundheitliche Leistungsanbieter weitergegeben werden. Mit integriertem GPS oder über weitere Technologien kann das Gerät lokalisiert werden. Beschleunigungs-Sensoren und Gyroskope ermöglichen die Erfassung der Bewegungsart des Nutzers mit seinen spezifischen Mustern für Gehen, Laufen, Fahrrad- oder Autofahren. Mit der Kamera können Bilddaten erfasst werden. Durch die Messung der Absorption des Lichts mit dem Kamerasensor kann der Blutfluss im Gewebe und damit die Herzfrequenz gemessen werden. Neben einfachen optischen und Bewegungs-Sensoren kommen immer ausgefeiltere optische, chemische und elektronische Sensoren in die mobilen Geräte. So nutzt z. B. Samsung Simband das Licht mit roter, grüner und blauer Wellenlänge, um in unterschiedliche Hautschichten vorzudringen und anhand der Absorption die Konzentration von Blutgasen wie Sauerstoff oder Kohlenstoff zu erfassen.[297] Die Sensor- und Nutzungsdaten, die Bilder und die Metadaten lassen sich auf verschiedenste Indikatoren hin analysieren und erlauben Rückschlüsse auf den Gesundheitszustand wie auf Gefühle, Stress oder seelische Stimmungen (z. B. Depression).[298] Es gibt „digitale Biomarker", etwa zur Alzheimer-Diagnose. Gemäß einer Studie könnten in den USA deren

295 Schumacher in Langkafel S. 238.
296 Manhattan Research zit. bei Schumacher in Langkafel S. 239.
297 Schumacher in Langkafel S. 235.
298 Schumacher in Langkafel S. 231; Digitale Video-Stressdetektion für Studierende, DANA 2013, 130.

Einsatz allein in der Diabetes-Prävention und -Behandlung sowie bei der Rehabilitation von Asthma-, Lungen-, Herz- und Kreislauf-Kranken jährlich 7 Mrd. Dollar einsparen.[299]

Eine weitergehende aktive Rolle kommt dem Betroffenen zu, wenn er es zulässt, dass digitale Geräte **im oder am Körper implantiert** werden. Diese können zur Authentisierung oder Identifizierung genutzt werden. Sie können aber auch der kontinuierlichen Überwachung von Körperfunktionen, etwa der Herzfrequenz, des Blutdrucks oder der Körpertemperatur, dienen. Die Geräte im und am Körper können zudem über ein Netzwerk, ein „Body Area Network" miteinander verknüpft sein (s. o. 3.15).[300] Sie können, z. B. über eine automatisierte Dosierung der Insulinvergabe, den Lebenskomfort von Patienten stark verbessern.

4 Anwendungszwecke und Chancen

Die Wirtschaft verspricht sich von Big Data im Gesundheitswesen eine **Revolution** bei Forschung, Prävention und Behandlung bei zeitgleicher Kosteneinsparung. Während in Deutschland wegen Datenschutzbedenken teilweise (noch) eine gewisse Reserviertheit hinsichtlich von Anwendungen bestand und besteht, sind in anderen Staaten, allen voran den USA und Großbritannien, weniger Vorbehalte festzustellen.

4.1 Behandlung, Betreuung, Pflege und Nothilfe

Die **medizinische Behandlung** kann mit Hilfe von Big Data in Bezug auf den konkreten Umgang mit dem Patienten verbessert werden. Diese Verbesserung kann sich auf die Kommunikation, die Organisation und Arbeitsteilung bei einer Leistung beziehen, etwa beim Einsatz des Personals, von Krankenhausbetten, von sonstigen Ressourcen oder beim Patientenfluss. Bedienungsfehler können verhindert werden.[301] Einsatzmöglichkeiten bestehen bei der internen Qualitätssicherung (s. u. 4.2), der Vermeidung von Nebenwirkungen beim Arzneimitteleinsatz, dem individuellen und kollektiven Risikoscreening, bei der Behandlungsunterstützung, im Rahmen von personalisierter Medizin (s. o. 2.6) sowie bei Präventions- und Nachbehandlungsmaßnahmen. Big Data unterstützt den Übergang vom einheitlichen standardisierten zu einem flexiblen patientenzentrierten Vorgehen.[302]

Einen massiven Schub hinsichtlich des Anfalls von Gesundheitsdaten bringt die **Telemedizin**. Hierbei werden nicht nur Inhaltsdaten ausgetauscht und dokumentiert; es fallen zusätzlich Kommunikationsdaten an, die Auskunft geben über Standorte, Zeiten, Behandler und Dienstleister. Eine spezifische Form ist die Telekonsultation, bei der sich Mediziner untereinander austauschen. Angesichts der ärztlichen Spezialisierung, der medizinischen Unterversorgung im ländlichen Raum und der Datensammlung von

299 Apps sparen Milliarden ein, Der Spiegel 47/2017, 68.
300 Schumacher in Langkafel S. 234 ff.
301 Schrader, Fehler am Drücker, SZ 15.12.2017, 16.
302 Weichert DuD 2014, 834.

Gesundheitsdaten durch den Patienten selbst gewinnt auch die Arzt-Patienten-Kommunikation an Bedeutung. In Großbritannien bietet die Firma Dr-Ed seit 2011 Fernberatungen und -behandlungen auch in anderen Ländern an. Mit Kunden aus Deutschland wurden in der Muttersprache seitdem bereits mehr als 200.000 Online-Sprechstunden abgehalten. Die Schön-Klinik mit 23 Standorten in Deutschland und Großbritannien bietet seit Dezember 2017 Video-Chats als Ersatz von ambulanten Sprechstunden zur psychotherapeutischen Behandlung an.[303] Das bisher in Deutschland geltende Fernbehandlungsverbot nach § 7 Abs. 4 MBOÄ[304] beginnt angesichts der Nachfrage und den fachlichen Möglichkeiten immer mehr durchlöchert und absehbar aufgehoben zu werden. Die TeleClinic hat mit der Barmenia Krankenversicherung sowie dem Marktführer in der privaten Krankenversicherung DeBeKa in Baden-Württemberg den Auftakt gemacht.[305] In der Schweiz besteht über das telemedizinische Portal „Medgate" schon die Möglichkeit, Medikamentenverordnungen vorzunehmen.[306] Auch der neue, ausschließlich online-agierende Krankenversicherer Ottonova geht über den Umweg Schweiz, um für seine Mitglieder Videokonsultationen anzubieten.[307] Bei ambulanten Chemotherapien besteht für Krebskranke die Möglichkeit, mit Hilfe einer Smartphone-App einen regelmäßigen Kontakt zum Onkologen zu halten und niederschwellig Konsultationen durchzuführen.[308]

Ein weiterer Einsatzbereich ist die **Pflege, Betreuung und Vorsorge**. Hierzu gehören Angebote des Ambient Assisted Living (AAL) zur Verbesserung der Versorgung und der Lebenssituation von behinderten, älteren oder aus sonstigen Gründen hilfsbedürftigen Menschen (s. u. 10.4).[309]

4.2 Qualitätssicherung

Die Qualität der medizinischen Versorgung ist ein zentrales Grundanliegen, welches mit der massenhaften Verarbeitung von Gesundheitsdaten verfolgt wird. Im Rahmen der gesetzlichen Krankenversicherung haben insofern seit 2000 die Anstrengungen zur **Verbesserung der Versorgungsqualität** massiv zugenommen. Seit 2003 sind gemäß § 135a SGB V alle Leistungserbringer in der stationären und ambulanten Versorgung zum einrichtungsinternen Qualitätsmanagement wie auch zu einer übergreifenden Qualitätssicherung verpflichtet. Der Gemeinsame Bundesausschuss (G-BA) legt gemäß § 135 SGB V Mindestanforderungen fest und definiert gemäß § 137 SGB V Regelungen zur Qualitätsprüfung und -beurteilung für die stationäre und vertragsärztliche Versorgung. Im letztgenannten Bereich haben gemäß § 136 SGB V die Kassen(zahn)ärztlichen Vereinigungen eine Prüf- und Förderfunktion. Inzwischen erfolgt eine

303 Schuster SZ 14.12.2017, 28.
304 Rehborn in Prütting § 7 MBOÄ Rn. 10-15; Strategy/pwc S. 108 f.
305 Schlingensiepen, doc.com SZ 06.11.2017, 36; Debeka startet Pilotprojekt in Telemedizin, http://versicherungswirtschaft-heute.de 7.12.2017.
306 Vgl. www.medgate.ch dazu positiv Müller in Stiftung Datenschutz (2017) S. 119.
307 Schlingensiepen, Zur Behandlung ins Nachbarland schalten, SZ 14./15.10.2017, 30.
308 Bartens, Smarte Visite, SZ 22.9.2017.
309 ULD (2010).

sektorenübergreifende datengestützte Qualitätssicherung, für die gemäß § 137a SGB V das Institut für Qualitätssicherung und Transparenz im Gesundheitswesen zuständig ist (s. o. 3.6). In § 299 SGB V wird die Datenverarbeitung für Zwecke der Qualitätssicherung präzise vorgegeben.[310]

4.3 Wirtschaftlichkeitskontrolle

In der vertragsärztlichen Versorgung sind Krankenkassen und Kassenärztliche Vereinigungen nach § 106 Abs. 1 SGB V zur Überprüfung der Wirtschaftlichkeit verpflichtet. Die Qualitäts- und Wirtschaftlichkeitsprüfung im stationären Bereich erfolgt gemäß § 113 Abs. 1 SGB V durch unabhängige Prüfer der Landesverbände der Krankenkassen, die Ersatzkassen und des Landesausschusses des Verbands der privaten Krankenversicherung.[311] Mit Big Data kann eine Optimierung des Ressourceneinsatzes mit dem Ziel der Verhinderung von Kostensteigerungen und der Vermeidung unnötiger oder unverhältnismäßig erscheinender Gesundheitsausgaben erreicht werden.

Ein typischer Anwendungsfall für den Einsatz großer Gesundheitsdatenbestände besteht in der Verwaltung, Verhandlung und Neuberechnung von Vergütungsverträgen (§§ 82 ff. SGB V).

Durch auf Big Data basierten Bonus- und Malussysteme und durch Selbstbeteiligungen der Patienten bzw. entsprechende Tarifierungen soll auf ein kostenbewusstes Verhalten der Patienten Einfluss genommen werden (s. u. 10.5).

4.4 Informationssicherheit

Die Sicherheit von Informationssystemen generell wie von solchen Systemen im Gesundheitsbereich hat für die Betreiber angesichts der Sensitivität der verarbeiteten Daten und der Anwendungen große Bedeutung. In einem IT-Sicherheitsgesetz[312] ist der Schutz kritischer Infrastrukturen vorgesehen. Zu den kritischen Infrastrukturen gehört der Bereich Gesundheit (§ 2 Abs. 2 Nr. 2 BSI-G). Gemäß § 6 Abs. 1 BSI-Kritis-VO werden „wegen ihrer besonderen Bedeutung für das Funktionieren des Gemeinwesens“ im Sektor Gesundheit 1. die stationäre medizinische Versorgung, 2. die Versorgung mit unmittelbar lebenserhaltenden Medizinprodukten, die Verbrauchsgüter sind, 3. die Versorgung mit verschreibungspflichtigen Arzneimitteln und Blut- und Plasmakonzentraten zur Anwendung im oder am menschlichen Körper und 4. die Laboratoriumsdiagnostik als kritische und deshalb informationstechnisch besonders schützenswerte Dienstleistungen behandelt.[313] Für den Bereich Gesundheit hat das Bundesamt für die Sicherheit in der Informationstechnik (BSI) bereits im Jahr 2008 einen Leitfaden zum „Schutz Kritischer Infrastruktur – Risikomanagement im Krankenhaus“ herausgegeben. Im E-Health-Gesetz[314]

---

310 Pötter-Kirchner/Höchstetter/Grüning in Langkafel S. 115 ff.; Kircher in Kingreen/Kühling S. 254 f., 266 ff.; Schneider S. 27 ff.

311 Kircher in Kingreen/Kühling S. 269 f.

312 G. v. 17.5.2015, BGBl. I S. 1324.

313 VO v. 21.6.2017, BGBl. I S. 1902.

314 G. v. 21.12.2015, BGBl. I S. 2408.

werden durch Änderungen des SGB V weitere Sicherheitsvorkehrungen zum Schutz medizinischer IT-Anwendungen vorgesehen.[315] Die Überwachung der IT-Sicherheit, insbesondere die Abwehr von Hacking-Angriffen, erfolgt über hochkomplexe Big-Data-Anwendungen, bei denen oft auch selbstlernende KI zum Einsatz kommt.

4.5 Selbstoptimierung der Betroffenen

Einen völlig neuen Bereich gesundheitsbezogener Datenverarbeitung hat sich die Wellnesswirtschaft geschaffen, indem sie (zumeist internetbasierte) Dienste zur Erfassung körperlicher Leistungsdaten auf den Markt bringt. Mit Hilfe von sog. Wearables (s. o. 3.15), also mobilen mit Sensoren ausgestatteten elektronischen Geräten, erfassen Menschen über sich im Alltag wie z. B. bei (sportlichen) Freizeitaktivitäten oder auch bei der beruflichen Arbeit Gesundheitsdaten zu Bewegungsaktivitäten, Gewicht, Schlaf, Blutdruck, Puls, Stimmung, Lungen- oder sonstige Organaktivitäten. Im Jahr 2015 besaßen 17% der Deutschen mindestens ein solches Gerät.[316] Im Jahr 2014 wurden weltweit 150 Mio. derartige Geräte verkauft, in Deutschland immerhin 3,6 Mio. Schätzungen für das Jahr 2017 gehen von einem weltweiten Verkauf von 310 Mio. Geräten aus.[317] Gemäß einer Bitkom-Studie versuchen 43% der aktiven Sportler, 27% der chronisch Kranken und 26% der Übergewichtigen sich damit zu einem gesünderen Lebensstil zu motivieren. 93% der Chroniker sind demnach bereit, ihre Gesundheitsdaten an ihren Arzt weiterzuleiten.[318] Zentrale Zielsetzungen bei der Nutzung solcher Wearables sind die Selbstmotivation, die Selbstoptimierung und die gesundheitliche Überwachung von Körperfunktionen, um im Bedarfsfall adäquat intervenieren zu können. Unter dem Stichwort „Quantified Self" hat sich hierzu eine weltweite Bewegung entwickelt.[319] Deren Credo kann wie folgt zusammengefasst werden: „Ich messe mich, also bin ich."[320] Oft werden Dienste über Apps erbracht, die auf Smartphones oder sonstigen Geräten installiert sind. Damit verbundene positive Erwartungen sind verbesserte individuelle Anpassung an Situationen (Training, Diagnosen, Verhaltensempfehlungen), die Erhöhung der Effizienz von Ernährung, Einnahme von Mitteln oder sonstigen Maßnahmen und die Erhöhung der Steuerungs- und Entscheidungsmöglichkeit der Betroffenen.[321] Eine spezifische Form der „Selbstvermessung" ist die durch kommerzielle Anbieter vorgenommene Analyse des eigenen Genoms (s. o. 3.14).

Applikationen in den Bereichen Gesundheit, Fitness und Medizin gehören zu den beliebtesten Anwendungen digitaler Mobilgeräte. Das Angebot von sog. mHealth für Android- oder iOS-Geräte (Apple) umfasste schon 2014 97.000 Apps mit einem

315 Raum in Stiftung Datenschutz (2017) S. 125 f.

316 Klose in Stiftung Datenschutz, S. 98 zitiert Ballhaus/Song/Meyer/Ohrtmann/Dressel (März 2015), Whitepaper „Media Trend Outlook – Wearables: Die tragbare Zukunft kommt näher".

317 Deutscher Ethikrat S. 78.

318 Becker, Auf Schritt und Tritt, SZ 7.4.2017, 35.

319 Haferkamp in Stiftung Datenschutz (2017) S. 59 ff.

320 Belliger, 25.8.2015, https://www.bmbf.de/de/ich-messe-mich-also-bin-ich-988.html.

321 Haferkamp in Stiftung Datenschutz (2017) S. 61; Timm MedR 2016, 688; zur Rechtmäßigkeit Dregelies VuR 2017, 256 ff.

Jahresumsatz von ca. 4 Mrd. US-Dollar. 31% der Anwendungen richteten sich an chronische Patienten; 28% adressierten Fitness-orientierte Nutzende.[322] In der Regel gehört zu diesen Angeboten auch ein Kommunikationsangebot, mit dem sich die Nutzer mit ihren Ergebnissen über eine Plattform austauschen können. Diese Kommunikationsangebote sind wiederum zumeist Bestandteil umfassenderer sozialer Netzwerke. PEW Research zufolge maßen 69% der US-amerikanischen Bevölkerung 2014 einen oder mehrere Gesundheitswerte von sich selbst oder von einem Angehörigen.[323] Gemäß einer Analyse der US-Marktforschungsfirma IQVIA Institute für Human Data Science kommen zu den 318.500 Gesundheits-Apps in den einschlägigen Stores von Apple und Google (Herbst 2017) täglich ca. 200 neue Anwendungen hinzu; über die Hälfte der Softwareangebote greift dabei auf Sensordaten zu. Insbesondere im Lifestyle-Bereich hat ein Kampf der Hersteller von Wearables um einen „Platz am Körper der Menschen" begonnen. Es gibt kaum noch ein Körperteil, an dem nicht ein solches Gerät angebracht werden kann, vom Kopf, über Augen, Hals, Haut, Brust, Oberkörper, Arme, Handgelenk, Finger, Hüfte bis zu den Füßen.[324]

Mit Quantified Self wird nicht nur ein Nutzen für den Nutzer verfolgt. Oft ist es erklärtes Ziel, insbesondere bei unentgeltlichen Angeboten, dass die erfassten Daten durch die Anbieter weiterverarbeitet werden. Diese Zweitverwertung verfolgt teilweise eine wissenschaftliche, zumeist aber eine wirtschaftliche Zielrichtung. Durch nicht kompatible Zweitzwecke oder eine zu starke Fokussierung hierauf, z. B. durch Verzicht auf Qualitätsanforderungen, kann es nicht nur zu einer Fehloptimierung, sondern zu kontraproduktiven Effekten kommen.[325]

Die selbstbestimmte Nutzung von Wearables ist Ausdruck der individuellen Selbstbestimmung des Einzelnen. Die Nützlichkeit der Fitness-Tracker für die Betroffenen ist aber umstritten. Bei einer wissenschaftlichen Untersuchung der Effekte des Einsatzes solcher Geräte ließen sich keine positiven Wirkungen, z. B. auf den Body-Mass-Index nachweisen.[326]

Man kann das Selftracking als Ausdruck eines inhumanen Leistungssystems ansehen, das menschliche Schwächen und Ressourcengrenzen unzureichend berücksichtigt.[327] Andere sehen darin schlicht moderne bzw. zeitgemäße Alchimie.[328] Als negative Wirkungen werden benannt: soziale Kontrolle, kollektive Gleichschaltung, Entmündigung und Instrumentalisierung, Überlastung, Autonomieverlust durch Kompetenzverlagerung auf den Algorithmus, Überflutung (mit Irrelevantem), Daueraufmerksamkeit, Vereinseitigung des

322 Schumacher in Langkafel S. 230, 232.
323 Zitiert bei Schumacher in Langkafel S. 229.
324 Schmieder, Ein Band, sie zu knechten, SZ 7.1.2016, 19; detailliert Schmieder/Werner, Hautnah, SZ 9./10.1.2016, 29.
325 Schumacher in Langkafel S. 240; Haferkamp in Stiftung Datenschutz (2017) S. 64 f; zur rechtlichen Bewertung Dregelies VuR 2017, 261 f.; Schmundt, Falsch vermessen, Der Spiegel 3/2017, 107.
326 Schwenkenbecker, Das Ziel ist das Ziel, SZ 10.1.2018, 14.
327 Haferkamp in Stiftung Datenschutz (2017) S. 62.
328 Selke in Stiftung Datenschutz (2017) S. 153 ff.

Fokus, Kompetenzverlust.[329] In der Praxis erweisen sich viele Anwendungen als problematisch, etwa wegen der Fehl- und Falschanzeigen[330], wegen unzureichenden Datenschutzvorkehrungen[331] und ungenügender Anwenderinformation.[332] Eine Studie der Stanford University ergab, dass Fitness-Armbänder den Herzschlag mit einer Abweichung von 5-10% relativ korrekt anzeigten. Die Angaben zum Kalorienverbrauch waren dagegen regelmäßig unbrauchbar.[333] Ob, inwieweit und unter welchen Bedingungen Gesundheits-Apps gesundheitliche Verbesserungen bewirken, ist bisher in wissenschaftlichen Studien nicht hinreichend untersucht. Eine solche Untersuchung erweist sich auch wegen des riesigen Angebots und der dauernden technischen Weiterentwicklung als äußerst schwierig.[334] Das für die Aufsicht im GKV-Bereich zuständige Bundesversicherungsamt bewertet die Nutzung von Fitness-Trackern u. Ä. durch Versicherte bisher nicht als eine qualitätsgesicherte Maßnahme (§ 65a Abs. 1 Nr. 3 SGB V).[335]

4.6 Medizinische Unterstützung

Neben dem ambulanten und dem stationären beginnt sich ein digitaler Sektor im Gesundheitswesen zu etablieren.[336] Während die sog. Life-Style-Angebote zumeist nur einen begrenzten medizinischen Nutzen haben dürften, haben gezielte medizinisch-therapeutische Applikationen regelmäßig positive Effekte. Sie ermöglichen oder erleichtern es den Nutzern, bestimmte gesundheitliche Handicaps zu bewältigen. Wertemaßstab ist in diesen Fällen nicht die kommerzielle Relevanz, sondern die „Lebensdienlichkeit" (Konvivialität, conviviality).[337] Berater der Boston Consulting Group schätzen allein für diesen Bereich den weltweiten Markt für das Jahr 2018 auf 22 Mrd. US-Dollar.[338] Nutzer solcher Anwendungen organisieren sich oft in Internetgruppen, wo sie ihre Erfahrungen austauschen. Da die Teilnehmer sich dabei zumeist zu spezifischen Krankheiten austauschen und qualitative Selbsthilfe praktizieren, sind sie für die Gesundheitswirtschaft von großem Interesse.[339] Durch zwischen Patienten und Arzt geschaltete Gesundheits-Apps besteht die Möglichkeit, orts- und zeitunabhängig mit Hilfe von oft nicht einmal teuren Zusatzgeräten Hirnströme, den Augeninnendruck, ein EKG, den Blutdruck, den Atemalkoholgehalt zu messen, ein Vorhofflimmern zu erkennen, die Lungenfunktion zu prüfen, Herzgeräusche zu speichern oder Innenohraufnahmen zu machen. So hilft z. B. M-Sense bei der Migränediagnostik. An der Universität Magdeburg wird an Neotiv gefeilt,

329 Haferkamp u. Selke in Stiftung Datenschutz (2017) S. 68, 158 f.; Becker, Mein besseres Ich, SZ 7.4.2017, 35.
330 Steinmetz, Sportlich vermessen, Der Spiegel 5/2016, 88.
331 91. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, Wearables und Gesundheits-Apps – Sensible Gesundheitsdaten effektiv schützen! v. 6./7.4.2016; Krempl, Datenschützer decken schwere Mängel im Internet der Dinge auf, www.heise.de 27.9.2016.
332 Schmergal, In der App-Falle, Der Spiegel 17/2016, 41.
333 Jung, Bei Diäten ungeeignet, SZ. 19./20.8.2017, 27.
334 Albrecht, Von Chancen und Risiken, EHealthCom 05/16, 39.
335 Deutscher Ethikrat S. 103.
336 Müller, App auf Rezept, Der Spiegel 29/2017, 67 ff.
337 Selke in Stiftung Datenschutz (2017) S. 157; ders. Digitale Alchimisten, SZ 1./2.7.2017, 5.
338 Dostert, Downloads gegen den Schmerz, SZ 11.8.2017, 14.
339 Weichert in Langkafel S. 165 f. = DuD 2014, 833.

einer Smartphonesoftware, die zuverlässig Alzheimer erkennen soll. Die Barmer Krankenversicherung akzeptiert eine App auf Rezept, mit der schielende Kinder geheilt werden sollen. Von der US-amerikanischen Arzneimittelbehörde FDA wurde ein Heilmittel mit eingebautem Sensor zugelassen, der aus dem Bauch von Schizophrenie-Patienten Daten über die Einnahme von Pillen kontrolliert. Mit Abilife MyCite wird die Medikamenteneinnahme von Problempatienten durch Dritte überprüfbar.[340]

Bei psychischen Leiden handelt es sich regelmäßig um Sachverhalte, bei denen eine digitale Behandlung nicht genügt. Durch die fehlende körperliche Präsenz des Patienten wird ein umfassender Eindruck des Therapeuten verhindert. Sinnvolle digitale Anwendungen sind aber auch hier nicht ausgeschlossen, wenn sie auf seriösen, wissenschaftlich anerkannten Ergebnissen beruhen. So können z. B. Patienten mit Hilfe ihres Handys ihren Tagesablauf dokumentieren, der anschließend mit dem Therapeuten besprochen werden kann. Auch eine Schreibtherapie per E-Mail oder ein Videotelefonat kann patienten- und situationsangemessen sein.[341]

4.7 Genetik

Die Decodierung des menschlichen Genoms war über viele Jahre die vorrangige Aufgabe der Gentechnik. Diese Aufgabe gelang dem „Human Genome Project", einem Zusammenschluss von hunderten Wissenschaftlern aus 40 Nationen sowie dem eigenständig vorgehenden Craig Venter im Jahr 2000. Inzwischen kann ein menschliches Genom fast vollständig mit einem Kostenaufwand von weniger als 1000 US-Dollar dechiffriert werden, mit weiter fallender Tendenz. Dabei handelt es sich um sog. Exom-Analysen, bei denen nicht nur ausgesuchte Genvarianten, sondern sämtliche Gene der untersuchten Person analysiert werden, oder sogar um Gesamtgenomanalysen, die auch die Abschnitte der Erbsubstanz miteinbeziehen, die keine Proteine codieren.[342]

Genetische Forschungsdatenbanken finden immer größere Verbreitung. Der Gründer des chinesischen Online-Händlers Alibaba Jack Ma investiert in die Genanalysefirma Wuxi Nextcode, das aus dem isländischen deCode-Projekt hervorgegangen ist, welches die Erbinformationen von 140.000 Isländern erfasste und untersuchte.[343] 2010 startete in Kalifornien/USA ein großes Genanalyseprojekt eines Gesundheitsversorgers mit 100.000 Probanden.[344] In Großbritannien wollen die Gesundheitsbehörde National Health Service (NHS) und die Pharmafirmen Regeneron und GlaxoSmithKline das Erbgut von einer halben Million Menschen auslesen.[345] In den USA verfolgt die Initiative „All of Us" die Sequenzierung der Gene einer Million Menschen. Einen ähnlichen Umfang soll ein Projekt

340 Hütten, Ein Spion im Bauch, SZ 18./19.11.2017, 37.
341 Ludwig, Auf der digitalen Couch, SZ 27.6.2017, 26.
342 Deutscher Ethikrat S. 62 f.
343 Jack Ma investiert in Gentest, DANA 2017, 109; zur Vorgeschichte deCODE Genetics insolvent, DANA 2010, 36; Gericht erklärt Gendatenbank-Gesetz für verfassungswidrig, DANA 2/2004, 34; Chemiekonzern kauft sich Gencodes der Gesamtbevölkerung, DANA 1/1999, 31.
344 Genanalyse-Großprojekt gestartet, DANA 2010, 37.
345 Staatliche Genkartierung, DANA 2013, 27 f.; Grolle, Jagd auf SCN9A, Der Spiegel 33/2017, 101.

des Pekinger Instituts BGI und des Sequenzierpioniers Craig Venter haben. Der Pharmakonzern AstraZeneca plant gar, 2 Mio. Probanden zu rekrutieren.[346]

Genanalysen eignen sich nicht nur für medizinische Anwendungen, sondern auch für weitere Zwecke. Deren Nutzung im Rahmen der Strafverfolgung war zunächst begrenzt auf die reine Identifikation, also die Zuordnung eines z. B. am Tatort gefundenen Gewebes zu einer Person. Bei Katastrophen sind Genanalysen Standard zur Identifizierung der Opfer. Inzwischen versucht man, aus dem Gencode von Gewebeproben von Verdächtigen oder Opfern körperliche oder gesundheitsbezogene Merkmale abzuleiten und forensisch zu nutzen. Dabei wird mit Big-Data-Methoden gearbeitet, wie sie auch bei medizinischen Genanalysen zum Einsatz kommen.[347]

Für Zwecke der Strafverfolgung verfügt die Polizei über Datenbanken mit sog. genetischen Fingerabdrücken von Material zu Tatortspuren, Straftatverdächtigen und Verurteilten, um diese Personen zuzuordnen. Das bundesdeutsche Bundeskriminalamt (BKA) betreibt eine solche DNA-Datenbank. Die DNA-Datenbank der britischen Polizei wird dafür kritisiert, dass sie auch Daten zu Personen speichern, die keinen Anlass für eine Speicherung gegeben haben. Einen Quantensprung plant das Emirat Kuweit, das unter dem Vorwand der Terrorismusbekämpfung eine DNA-Datenbank aller Bewohner des Emirats sowie auch sämtlicher Geschäftsreisenden und Touristen aufzubauen angekündigt hat.[348] Von Juli bis Oktober 2017 wurde für alle Einwohner der westchinesischen Provinz Xinjiang ein von staatlichen Krankenhäusern durchgeführter Gesundheitscheck angeboten. Im Nachhinein stellte sich heraus, dass die DNA-Proben sowie weitere sensitive Daten von 18,8 Mio. Menschen – praktisch der gesamten Bevölkerung zwischen 12 und 65 Jahren, hiervon ein Großteil der ursprünglichen Bevölkerung der Uiguren, mit denen politische Konflikte bestehen – in einer Datenbank gespeichert werden, die auch für Sicherheitszwecke genutzt wird.[349]

Nach der biotechnischen Dechiffrierung des menschlichen Genoms erfolgt die Zuordnung des genetischen Codes zu Krankheiten, um diese frühzeitig diagnostizieren und vorhersagen zu können. Genetische Faktoren spielen eine wichtige Rolle für die Gesundheit. Im Rahmen von genomweiten Vergleichsstudien wird untersucht, wie oft einzelne Varianten im Genom mit bestimmten Zielmerkmalen, z. B. besonderen Krankheiten auftreten. Über die gefundenen Korrelationen hofft man, genetische Erkrankungsrisiken ableiten zu können.[350] Bei diesen Untersuchungen ergeben sich zunehmend Konstellationen, bei denen die Betroffenen ein unmittelbares Eigeninteresse daran haben können, über erkannte Risiken informiert zu werden. Bei Anlageträgerschaft

346 Grolle, Jagd auf SCN9A, Der Spiegel 33/2017, 101.

347 Schultz/Bartram, Erweiterte DNA-Analyse, Bürgerrechte& Polizei/CILIP 113 (September 2017), 69 ff.; Weichert, Genetische Forensik und Datenschutz, Vorgänge 218 (2/2017) S. 123 ff.

348 DNA-Datenbank für Bevölkerung und Reisende geplant, DANA 2016, 198 f.; DNA-Identifikation zur „Terrorbekämpfung" für alle, DANA 2016, 105.

349 Giesen, Unter falschem Vorwand, SZ 14.12.2017, 7.

350 Deutscher Ethikrat S. 61 f.

für erblichen Brust- und Eierstockkrebs gilt dies z. B. wegen möglicher Vorsorgemaßnahmen oder Therapien.[351]

Der nächste Schritt sind **gentechnische Therapien**. Tests mit der Antisense-Methode waren erfolgreich, bei der Geneffekte stumm geschaltet werden.[352] Es ist ein Ziel, die menschliche Biologie wie Software programmieren bzw. die DNA wie ein Computerprogramm bearbeiten zu können. März 2013 reichte eine Forschungsgruppe der University of California/Berkeley und des Broad Institutes/Cambridge um die Biologinnen Jennifer Doudna und Emmanuelle Carpentier ein Patent zur Veränderung des Erbguts in menschlichen Zellen ein. Die Crispr-Cas9 ist ein molekulares Verteidigungssystem, mit dem sich Bakterien vor Feinden schützen. Doudna und Charpentier gelang es, die daran beteiligten Moleküle für gentechnische Zwecke zu nutzen[353] Seitdem entwickelt sich die Technik mit großer Geschwindigkeit weiter. Genmanipulationen werden inzwischen von fast jedem biomedizinischen Labor beherrscht und sind schon für Kosten von 30 US-Dollar möglich. 2016 wurde in den USA der erste Einsatz mit der Crispr-Cas9-Technik, für die sich der populäre Name „Genschere" etablierte, bei 18 Krebspatienten zugelassen.[354] Mit Hilfe der Einbringung von genmanipulierten Zellen in die Leber soll die Bluterkrankheit geheilt werden.[355] Die Gentherapie, die über Jahre hinweg keine Erfolge vorweisen konnte, scheint seit 2017 auf vielen Ebenen voranzukommen.[356]

In der Zeitschrift „Science" wurde über das „Human Genome Project Write" berichtet. Bei einem Treffen am 10.5.2016 in Boston/USA setzten sich 150 Wissenschaftler und Geschäftsleute aus fünf Kontinenten zum Ziel, das menschliche Erbgut mit künstlicher DNA zu gestalten.[357] Microsoft betreibt für dieses **Genome Editing** eine eigene Abteilung. In den USA ist es Forschern erstmals gelungen, in Embryonen einen festgestellten genetischen Defekt zu korrigieren.[358] Genmanipulationen selbst in der Keimbahn sind zwar ethisch hoch umstritten, aber technisch machbar und werden wissenschaftlich erprobt.[359]

Mit der **reversen Genetik** wird das Ziel verfolgt, biotechnisch bedingte, in der Natur vorgefundene Mechanismen aufzufinden und diese genetischen Mustern zuzuordnen, um diese dann nachzubauen. Die klassische Methode der Genanalyse geht von einer Erkrankung aus, deren genetische Ursachen gesucht werden. Bei der reversen Genetik macht sich die Genforschung auf die Suche nach Menschen mit bestimmten Gendefekten, die bestimmte erwünschte Wirkungen zeigen, z. B. das Verbrennen von Fett, um diese

351 Deutscher Ethikrat S. 72.
352 Hackenbroch, „Das schönste Geschenk", Der Spiegel 52/2017, 100 f.
353 Das Recht an der Gen-Schere, SZ 15.1.2016, 14.
354 Heissler, Therapie bei Dr. Frankenstein, Kieler Nachrichten, Wochenendbeilage 9./10.7.2016, 1. Gen-Schere in Menschenzellen, Der Spiegel 26/2016, 96.
355 Zinkant, Hoffnung auf ein normales Leben, SZ 8.12.2017, 16.
356 Zinkant, Fähren der Hoffnung, SZ 4.1.2018, 14.
357 Zinkant, Schreiben lernen, SZ 9.6.2016, 16; Grolle, Labor der Geheimniskrämer, Der Spiegel 21/2016, 112 f.
358 Zinkant, Das reparierte Baby, SZ 03.08.2017, 12.
359 Grolle, Frankensteins Erben, Der Spiegel 1/2018, 100 ff.

Marker zu extrahieren und dann zu reproduzieren. Beispiel hierfür ist das CCR5-Gen, das verhindert, dass HI-Viren in Zellen eindringen können, was dazu führt, dass Menschen mit diesem „Defekt" immun gegen Aids sind. Hoffnungen werden auch an das SCN9A-Gen geknüpft, das zu einer Unempfindlichkeit von Schmerzen führt. Reverse Genetik setzt voraus, dass die Gen-„Spender" nicht anonymisiert werden, da beim Auffinden interessanter Effekte die Probanden angesprochen und zur Grundlage weiterer Untersuchung genommen werden sollen. Das größte Genomikzentrum der USA, das Broad Institute bei Boston, plant mit dem „Human Knockout Projekt" unter der Leitung von Daniel MacArthur diese Technologie systematisch zu entwickeln.[360]

4.8 Medizinische Marktforschung

Medizinische Marktforschung ist ein Feld, über das wenige Informationen bekannt sind und in dem von den handelnden Unternehmen teilweise gezielt eine kritische öffentliche Berichterstattung bekämpft wird. Weltweit und auch in Deutschland marktführendes Unternehmen ist die QuintilesIMS Holdings, Inc. (kurz IQVIA) mit Hauptsitz in den USA, die Oktober 2016 aus der IMS Health und Quintiles verschmolzen wurde. Das Unternehmen vermarktet Prognosemodelle und -techniken und treibt hierfür über eine Million Produkte des Pharma- und Gesundheitsbereichs. Dies entsprach nach eigenen Angaben über 80% aller Arzneimittel-Verkaufstransaktionen weltweit. Die Analysen basieren auf angeblich anonymisierten Patientendaten, die zusammen mit anderen grundlegenden Daten erfasst werden, um für Interessengruppen aus dem Gesundheitsbereich Zusammenhänge zwischen medizinischen Anwendungen, Patienten, verschreibenden Ärzten und Kostenträgern aufzuzeigen.[361] IQVIA führt, soweit erkennbar, das bisherige Geschäft von IMS Health umfassend fort. Danach bestehen, teilweise vermittelt durch Intermediäre wie AIS-Anbieter oder Apothekenrechenzentren, Verträge mit Ärzten und Apotheken, von denen Diagnose-, Behandlungs- und Verschreibungsdaten mit „Patientenanonymen" pseudonymisierte Einzeldatensätze übermittelt werden.

Weitere Unternehmen sind Insight Health[362] und Medimed. Letztgenanntes Unternehmen war eine Tochter des französischen Unternehmens Cegedim und findet sich heute im Internet unter IMS Health.[363] Gegenleistungen an die medizinischen Leistungserbringer für die pseudonymen Daten sind Honorare, vergünstigte IT-Leistungen oder die Rückmeldung von individuellen, auf die Leistungserbringer ausgerichteten Statistiken. Die Datenlieferung durch die Apothekenrechenzentren werden mit § 300 SGB V gerechtfertigt, wobei streitig ist, ob die dort geforderte Anonymisierung der Datensätze tatsächlich stattfindet (s. o. 3.2.3). Die Praxis von IMS Health und deren Datenbeschaffung über Apothekenrechenzentren, etwa des bayerischen Unternehmens VSA GmbH, war sowohl in Deutschland wie auch in Österreich Gegenstand strafrechtlicher und

360 Grolle, Jagd auf SCN9A, Der Spiegel 33/2017, 100 ff.
361 www.wikipedia.org, IMS Health, abgerufen am 22.12.2017.
362 www.insight-health.de, abgerufen am 22.12.2017.
363 www.medimed.info, abgerufen am 22.12.2017.

datenschutzrechtlicher Ermittlungen sowie zivil- und verwaltungsrechtlicher Verfahren.[364] Die Unternehmen behaupten fälschlich, dass die Patientendatensätze nicht mehr einer konkreten Person zugeordnet werden könnten, also wirksam anonymisiert seien. Da die Pseudonymisierungsverfahren nicht überprüfbar offengelegt wurden, verliefen die Verfahren letztlich im Sande.[365]

Datenabnehmer der medizinischen Marktforschungsunternehmen sind die Pharmawirtschaft, öffentliche Stellen sowie die Versorgungsforschung im privaten wie im GKV-Bereich (Krankenkassen). Die Pharmaunternehmen nutzen die erlangten Daten, die Aufschluss über Patientenstamm und Verschreibungspraxis geben, auch für zielgerichtete Werbung bei medizinischen Leistungserbringern, etwa bei Arztpraxen.[366]

4.9 Werbung und Marketing

Werbung zielt auf die Steigerung des Absatzes von Produkten oder Dienstleistungen ab, indem diese gegenüber potenziellen Abnehmern (Konsumenten, Anwendern) präsentiert und positiv dargestellt werden. Werbung ist in ihrer Herstellung und Vermittlung teuer. Daher ist es für die Werbenden wichtig, deren Wirksamkeit zu überprüfen und zu erhöhen. Dem dienen die Erstellung möglichst präziser Interessen- oder Psychoprofile der (potenziellen) Adressaten und eine bestmögliche Abstimmung von Art und Inhalt der Werbeansprachen hierauf. Aufgabe des psychologischen Profilings ist es, die Zugänglichkeit für bestimmte Angebote zu bewerten. Bei solchen Charakterprofilen wird z. B. unterschieden zwischen Performer, Disziplinierter, Bewahrer, Genießer, Hedonist, Abenteurer.[367] Auf die Identität der Adressaten kommt es dabei regelmäßig nicht an, sondern auf deren Merkmale, die auch unter Pseudonymen zusammengeführt sein können. Ja es genügt oft eine aggregierte Gruppenansprache, wenn die Gruppenmerkmale des Adressaten für seine Werbeempfänglichkeit aussagekräftig sind.

Die klassische Methode der Zuordnung im Internet, also beim Online-Marketing, erfolgt über Cookies, Token, Browser-Fingerprints oder andere Identifikatoren; ausgewertet wird i. d. R. der Clickstream, also die Aktivitätengeschichte des Nutzers. Weitergehende Analysen beziehen zusätzliche verfügbare Daten, etwa zum Kommunikationsverhalten, mitein. Neue Auswertungsmöglichkeiten ergeben sich z. B. durch die Installierung von Gesichtserkennungssoftware auf Geräten, insbesondere auf Smartphones. Darüber lassen

364 Kunze, Interview mit Glaeske, Gläserner Patient, www.zeit.de 22.8.2013; Spiekermann, Verwirrung um Verkauf von „Krankenakten“, www.derstandard.at 30.10.2013; ULD, Tätigkeitsbericht 2015, Kap. 4.6.8 (S. 63 f.); eine ausführliche Darstellung der Auseinandersetzung zwischen dem ULD Schleswig-Holstein und der VSA findet sich in Kauß, Zur Unabhängigkeit der staatlichen Datenschutzkontrollinstanzen, in Plöse/Fritsche/Kuhn/Lüders, „Worüber reden wir eigentlich?“ Festgabe für Rosemarie Will, 2016, S. 591 ff. m. w. N.

365 www.wikipedia.org, IMS Health, abgerufen am 22.12.2017.

366 Zu allem oben Dargestellten Kunze, Behandelt und verkauft, www.zeit.de 31.10.2013.

367 Haspa erstellt psychologische Kundenprofile, DANA 2010, 153 f.; Bußgeld gegen Haspa wegen Kundendatenzugriff und Neuromarketing, DANA 2010, 154.

sich Stimmungen aus den Gesichtsbildern ableiten, auf die Werbeschaltungen zielgerichtet reagieren können.[368]

Werbung im Gesundheitsbereich adressiert entweder den Endverbraucher oder Intermediäre. Bei **Endverbraucherwerbung** kommt es darauf an, dass der Konsument für ein Gesundheitsprodukt besonders empfänglich ist und hierzu in einer der Person angemessenen Weise angesprochen wird. Hierfür sind Informationen über Interessen an Gesundheitsthemen und über individuelle Erkrankungen des Adressaten oder einer Person aus dem sozialen Umfeld des Adressaten von hoher Wertigkeit. Wird dem Adressaten in einer (gesundheitlich) prekären Lage eine (vermeintlich anonym adressierte) Problemlösung angeboten oder werden gezielt individuelle Schwächen angesprochen, so fühlt sich der Adressat i. d. R. verstanden und angenommen und entwickelt eine gesteigerte Bereitschaft, für ein Produkt oder eine Dienstleistung zu bezahlen.[369]

Bei den Werbemethoden kommen **komplexe Techniken** zur Anwendung, die für die Betroffenen zumeist weder in ihrer Funktionsweise noch in ihrer Wirkung erkannt und überschaut werden können. So wurde in zwei österreichischen Apotheken jeweils ein Gesichtsscanner des Pharmakonzerns Bayer Austria installiert, der Geschlecht und Alter erkennen sollte und veranlasste, dass dem Kunden angepasste Werbebotschaften über ein Display angezeigt wurde. Diese Gesichtsanalyse war nicht mit einem Hintergrundsystem verknüpft. Nach empörten öffentlichen Reaktionen wurde der Einsatz wieder eingestellt.[370] Für Betroffene wäre der Einsatz einer solchen Technik nicht erkennbar, wenn sie nicht öffentlich gemacht wird. Im vorliegenden Fall wurde dieser Einsatz sogar positiv geworben. Welche für die Betroffenen intransparenten Schlussfolgerungen aus Konsumdaten gezogen werden können, zeigt der fast legendäre schon vor vielen Jahren bekannt gewordene Fall der US-Supermarktkette Target. Diese hatte aus einer Analyse des Einkaufsverhaltens schwangere Frauen identifiziert und sogar deren Geburtstermine hochgerechnet, um diese dann gezielt mit Produktangeboten zu konfrontieren.[371]

Internetsuchen im Bereich Gesundheit spielen eine große Rolle. Eine aktuelle Untersuchung zeigte bei **Internetnutzenden** für folgende Aktivitäten eine hohe Häufung (Information mindestens einmal monatlich): Gesundheitstipps 38%, Krankheiten 35%, Medikamente 31%, Behandlungen 17%, Arzt- od. Krankenhaussuche 13%. Die dabei generierten Nutzungsdaten werden für Werbeanzeigen verwendet. Die Vermarktung von Produkten und Dienstleistungen im Gesundheitsbereich über das Internet weist eine stark steigende Tendenz auf. Ca. 21 % der Internetnutzenden gaben an, mindestens einmal im Monat Medikamente online zu bestellen. Nur 39% erklären, nie Online-Apotheken in Anspruch zu nehmen.[372] Von großem Werbeinteresse sind Menschen, die sich über das Internet an Selbsthilfegruppen zu spezifischen Krankheiten oder Gesundheitsforen

368 Schmidt, Snowden warnt vor Big Data, Biometrie und dem iPhone X, www.heise.de 23.11.2017.
369 Manolidis, Personalisierung im Healthcare Marketing, PM-Report 2/2017, 15 f.
370 Meineck, Sie sehen aus, als könnten Sie Vitamine brauchen, www.spiegel.de 25.11.2017.
371 Weidlich, Der etwas andere Schwangerschaftstest, fnp.de 13.9.2014.
372 Hoffmann, Online-Beteiligung in Gesundheitsfragen, DIVSI magazin Dezember 2017, 10.

beteiligen. Dabei erfolgt regelmäßig ein Austausch von äußerst tiefgehenden persönlichkeits- und gesundheitsrelevanten Informationen. Die anfallenden Inhalts- und Metadaten sind für Marketingzwecke Gold wert.

Intermediärswerbung adressiert nicht die Endverbraucher, sondern die professionellen Helfer, zu denen die Endverbraucher regelmäßig eine Vertrauensbeziehung haben, etwa zum Arzt oder zum Apotheker. Die Werbeaktivitäten der Pharmaindustrie richten sich vorrangig an die Ärzteschaft, die dazu gebracht werden soll, die Medikamente des jeweiligen Unternehmens zu verschreiben. Ebenso wie bei der Endverbraucherwerbung kommt der Merkmalsanalyse der Adressaten eine zentrale Funktion zu: Wichtig sind hierbei eine genaue Kenntnis des Patientenstamms eines medizinischen Leistungserbringers, also Informationen über Krankheiten, soziale, familiäre und räumliche Bedingungen, Alter, Status (z. B. privat od. GKV-versichert) der Patienten. Wichtig ist zudem ein möglichst aussagekräftiges Profil des Intermediärs, etwa seine Zugänglichkeit für alternative Heilverfahren, sein soziales Engagement, seine finanzielle Situation oder seine Status-Interessen.

5 Spezifische Risiken – individuell, institutionell, gesellschaftlich

Nicht nur Big-Data-Kritiker verweisen darauf, dass mit dieser Methode Risiken verbunden sein können.[373] Die angestrebten Ziele können zumeist nur erreicht werden, wenn diese Risiken unter Kontrolle gebracht werden und wenn dadurch eine hohe Akzeptanz der Bevölkerung für die Methode und für die Ergebnisse der Datenanalysen besteht. Wir leben derzeit in einer Zeit ausgeprägter Technikbegeisterung, bei der Machbarkeit oft die einzige Voraussetzung ist, dass etwas gemacht wird. So werden auch viele Innovationen entwickelt und angewendet, die keine positiven und die negative Effekte auf die Menschen haben. Die Möglichkeiten von Big Data werden oft überschätzt. Den dadurch erlangten Ergebnissen wird oft eine Objektivität unterstellt, die nicht gegeben ist.[374] Im Jahr 2011 wurde deshalb von Ärzten die Aktion „Choosing wisely“ gestartet, mit der Patienten vor Überdiagnosen, Übertherapien und unnötiger Behandlung, die durch falsche Schlussfolgerungen aus Datenanalysen entstehen, geschützt werden sollen.[375]

Risiken bestehen unabhängig davon, ob Big Data im öffentlichen oder im nicht-öffentlichen Bereich eingesetzt wird. Sie basieren regelmäßig darauf, dass zwischen den Betroffenen Datenlieferanten und Betroffenen einerseits und den für eine Anwendung Verantwortlichen andererseits eine ökonomische, technische und strukturelle Machtasymmetrie besteht. Das Verfolgen der Anwenderinteressen führt leicht dazu, dass legitime Betroffeneninteressen übergangen werden und dass das Verarbeitungsverfahren zur Fremdbestimmung der Betroffenen beiträgt.

373 Überblick auch bei Strategy/pwc S. 90 ff.
374 Timm MedR 2016, 690; zu Risiken generell Deutsche Ethikrat S. 71.
375 Bartens, Dr. med. Roboter, SZ 25.10.2017, 14.

Viele der Risiken beruhen darauf, dass mit Hilfe von Big Data **Korrelationen, nicht Kausalitäten** festgestellt werden können. Die Korrelationen geben zumeist nur Auskunft über die Wahrscheinlichkeit bestimmter Ergebnisse, in den seltensten Fällen eine Sicherheit. Die Korrelation von bestimmten ausgewerteten Merkmalen mit einem erlangten Ergebnis kann auf Zufälligkeiten beruhen sowie auf Umständen, über die keine Daten in die Auswertung eingeflossen sind oder deren Gewichtigkeit nicht erkannt und berücksichtigt wurde. Eine seriöse Verwendung von Big Data bedingt in praktisch allen Fällen, insbesondere wenn damit existenzielle Entscheidungen verknüpft sind und es auf die Korrektheit des Analyseergebnisses ankommt, dass eine erkannte Korrelation erfolgreich hinsichtlich der Kausalzusammenhänge plausibilisiert wurde. Gerade im Gesundheitsbereich verbietet sich zumeist eine spekulative Herangehensweise, insbesondere wenn es um Leben und Tod geht und wissenschaftlichere Antworten zur Verfügung stehen.[376]

5.1 Körperliche und seelische Schäden

Es ist offensichtlich, dass der Einsatz von Big Data wertvolle Beiträge zur Vermeidung und Behebung von Gesundheitsbeeinträchtigungen leisten kann (s. o. 4.1). Doch kann auch das Gegenteil bewirkt werden. Die Beeinträchtigung der Integrität und der Verfügbarkeit von für die medizinische Behandlung benötigten Daten kann zu greifbaren gesundheitlichen Schäden führen, etwa wenn nach einem Unfall wegen einer unzutreffenden Datenanalyse oder einer Datenfälschung eine Bluttransfusion mit einer falschen Blutgruppe erfolgt, wenn Medikamentenunverträglichkeiten falsch angezeigt oder Daten hierzu nicht verfügbar sind, oder wenn wegen falscher Eingangsdaten oder anderer Fehler von einem IT-System eine falsche Behandlung vorgeschlagen wird.[377] Solche Beeinträchtigungen entstehen dadurch, dass auf der Grundlage **manipulierter, sabotierter oder falsch berechneter Daten** Falschbehandlungen stattfinden. Da dies nicht nur Konsequenzen für den Einzelnen hat, sondern potenziell auf die gesamte Gesellschaft, wird dem Gesundheitswesen eine Systemrelevanz beigemessen, was dazu führte, dass es informationstechnisch als kritische Infrastruktur eingestuft wird (§ 2 Abs. 2 Nr. 2 BSI-G, s. o. 4.4).

Psychische Schäden mit evtl. körperlichen Folgewirkungen können dadurch ausgelöst werden, dass das Recht auf Nichtwissen missachtet wird und Menschen das Wissen über gesundheitliche Umstände oder Dispositionen aufgedrängt bekommen (s. u. 6.5). Auch das Vorenthalten von gesundheitsbezogenen Daten kann negative gesundheitliche Folgen haben, etwa wenn im Rahmen der medizinischen Forschung personalisierbare Erkenntnisse über die Behandelbarkeit eines Leidens entstehen, die nicht an den Betroffenen oder an seinen Behandler weitergegeben werden.[378] Seelische Beeinträchtigungen können zudem dadurch entstehen, dass in der Öffentlichkeit oder in bestimmten Gruppen

376 Deutscher Ethikrat S. 10, 43 ff.; Timm MedR 2016, 690; Weichert DuD 2014, 834.
377 Münch S. 234 f.; Hacking auf Gesundheitsdaten steigt massiv, DANA 2016, 104.
378 Weichert in Langkafel S. 167 = DuD 2014, 834 f.

diskriminierende oder persönlichkeitsverletzende Informationen, die auf Big Data zurück gehen können, verbreitet werden (s. u. 5.2, 5.4).

Entsprechendes gilt erst recht für **Wirksysteme**, bei denen zwischen der Datenauswertung und einer daraus abgeleiteten Entscheidung keine natürliche Person zwischengeschaltet ist. So stellte die US-amerikanische Arzneimittelaufsicht FDA fest, dass extern ansteuerbare Herzschrittmacher des Herstellers St. Jude Medical Sicherheitslecks aufwiesen, über die deren Funktionalität gestört werden konnte, weshalb Software-Updates bei einer halben Million Patienten nötig wurden. Hacker hätten die Batterien entladen oder den Herzschlag der Patienten verändern können.[379]

Schäden können auch dadurch entstehen, dass wegen eines Angriffs bzw. eines Sicherheitsmangels die für eine Behandlung nötigen Patientendaten nicht verfügbar sind. Diese **Verfügbarkeit** war in vielen Fällen nicht mehr gegeben, als im Mai 2017 mehr als 230.00 Computer in 150 Ländern von der Ransomware (Erpressungssoftware) WannaCry erfasst wurden, darunter auch viele Krankenhäuser, z. B. in Großbritannien, aber auch in Deutschland, deren Daten durch die Software verschlüsselt wurden.[380]

Chance und Risiko zugleich besteht in der Nutzung von Big Data, das angesichts begrenzter Ressourcen bei der Auswahl von Patienten und deren Behandlung zum Einsatz kommt. Dafür hat sich der Begriff **Triage** etabliert. Damit wird ein Verfahren beschrieben, aus einer großen Anzahl von Verletzten oder Kranken darüber zu entscheiden, wie die vorhandenen Mittel am effektivsten zur Behandlung oder Rettung eingesetzt werden sollen. Die Triage-Methode stammt ursprünglich aus dem Bereich der Militärmedizin und diente dort der Auswahl der behandlungsfähigen Soldaten, um diese wieder für den Kampf einsetzen zu können. Vorrangiges Ziel war also nicht das Interesse der Betroffenen, sondern eine für die Kriegsführung optimierte Gesundheitsversorgung.

Heute wird der Begriff auch bei der Prioritätensetzung im Rahmen von **Notfällen, Katastrophen oder der Zuteilung von Organspenden** verwendet. Das Manchester-Triage-System ist ein europaweit eingesetztes System für die Zuordnung von Patienten im Rahmen der Notaufnahme in Krankenhäusern. Was ursprünglich durch geschulte Pflegekräfte standardisiert durchgeführt wurde, kann über erfasste Symptome und weitere Merkmale weitgehend digitalisiert unter Nutzung von Big Data durchgeführt werden.[381]

Während Triage-Verfahren in Notfallsituationen als Entscheidungsunterstützung sinnvoll eingesetzt werden können, kann davon keine Rede mehr sein, wenn auf der Basis Algorithmen Entscheidungen für Krankenversicherungen oder Kliniken getroffen werden, bei denen die statistisch errechnete Lebenserwartung darüber entscheidet, ob zu

379 Zinkant, Herzrasen, SZ 1.9.2017, 1; Baumgärtner/Gebauer/Knobbe/Rosenbach/Wiedmann-Schmidt, Hacker mit Dienstausweis, Der Spiegel 48/2017, 29.

380 Wannacry, Gesundheit braucht Politik 2/2017, 13.

381 Stichwort Triage bei www.pflegewiki.de; Das Manchester Triage System – Ersteinschätzung der Behandlungsdringlichkeit, notfallmedizin.charite.de, 2017.

erwartende Therapiekosten verfügbar gemacht werden. Ein derartiges Verfahren, das auf Diagnosedaten begründet ist, wurde jüngst von dem US-Unternehmen Aspire Health vorgestellt.[382]

5.2 Beeinträchtigung der Vertraulichkeit

Die Menschen haben hohe Erwartungen an die Vertraulichkeit beim Umgang mit ihren Gesundheitsdaten. Werden diese Erwartungen nicht erfüllt, so kann Big Data schnell zu einer Art „Turbo-Version der Optimierungsfalle" führen, bei welcher der Mensch mit seinem Würdeanspruch nicht mehr vorkommt. Dies könnte das „Verscherbeln des großen Erbes der Aufklärung" bewirken, die „Rückführung in selbstverschuldete Unmündigkeit".[383] Die Wahrung der Vertraulichkeit der Behandlungen ist ein zentraler Grundpfeiler für die Akzeptanz des Gesundheitssystems generell wie auch der jeweiligen konkreten Behandlung (s. u. 6.8). Unter Big-Data-Bedingungen verschärft sich das Risiko des Verlustes an Vertraulichkeit. Die Möglichkeiten der Reidentifizierung spezifischer Merkmalskombinationen bei der Analyse von vermeintlich anonymisierten Massendaten steigen. Zudem sind die Verarbeitungsprozesse für die Betroffenen oft völlig undurchsichtig. Dadurch steigt die Gefahr der Diskriminierung, der Stigmatisierung oder der Exklusion.[384]

Der Verlust der Vertraulichkeit muss nicht nur einen Akzeptanzverlust, sondern kann auch materielle Schäden zur Folge haben. Gemäß einer Studie des Ponemon Instituts waren in den USA mit 45% erstmals Hacking-Attacken der wichtigste Grund für Datenlecks im Gesundheitsbereich. Solche Angriffe haben demnach seit 2010 um 125% zugenommen und andere Gründe für Datenverluste (Schlampigkeit von Mitarbeitern, Diebstahl von Computern) überflügelt. Die Vertraulichkeitsverletzungen gehen zunehmend auf Cyberkriminelle zurück. Der Schwarzmarktwert einer durchschnittlichen Krankenakte soll in den USA bei 60 bis 70 Dollar liegen. Dabei geht es z. B. darum, per Identitätsdiebstahl Behandlungen oder die Verschreibung rezeptpflichtiger Medikamente zu erschleichen.[385] Für die Einrichtung hat zudem das Bekanntwerden von Vertraulichkeitsverlusten bei den Kunden bzw. den Patienten einen Vertrauensverlust zur Folge, der ebenso zu finanziellen Einbußen führen kann (s. u. 5.6).

5.3 Beeinträchtigung der Wahlfreiheit

Mit Big Data kann für die Betroffenen ein weitgehender Kontrollverlust über die eigenen Daten sowie indirekt evtl. über die eigene Person einhergehen. Hierzu tragen mangelnde

---

382 Soliman, Der Todesalgorithmus: Computer berechnet Lebenserwartung, daserste.ndr.de 14.12.2017; Welchering, Big-Data-Algorithmen – Wenn Software über Leben und Tod entscheidet, www.zdf.de 20.12.2017; vgl. Lobo, Warum eine Rentenversicherung, wenn ich mit 50 sterbe? www.spiegel.de 14.6.2017.

383 Langkafel in Langkafel, S. 12; von Graetz, Findungsprozesse, EHealthCom 5/2014, 16; zur Vertraulichkeitserwartung auch Deutscher Ethikrat S. 129 ff.

384 Deutscher Ethikrat S. 131 f.

385 Hacking auf Gesundheitsdaten steigt massiv, DANA 2016, 104.

Transparenz und fehlende individuelle Beeinflussbarkeit bei. Dieser Verlust führt zu einer Einschränkung der informationellen und medizinischen Selbstbestimmungsmöglichkeiten.

Durch Anreize (Nudging) oder durch Malus-Systeme können Verhaltensbeeinflussungen stattfinden, derer sich die Betroffenen möglicherweise überhaupt nicht bewusst sind. Hierdurch wird die Freiheit des Menschen, sich selbstbestimmt zu verhalten, beeinträchtigt (s. u. 10.5). Gerade im Gesundheitsbereich können wirtschaftlich, ethnisch oder anderweitig begründete Selektionen zum Ausschluss von Diensteangeboten und zu Manipulationen führen.[386] Entsprechendes kann sich bei selbstlernenden Systemen ergeben, bei denen die individualisierten Empfehlungen und Interaktionen nicht mehr nachvollzogen werden können und dadurch vom Betroffenen nicht erwünschte Ergebnisse erzielt werden.[387]

5.4 Diskriminierung

Während die Manipulation auf eine Beeinflussung des Wissens und des Willens der Betroffenen abzielt, erfolgt bei einer Big-Data-basierten Diskriminierung eine Schlechterbehandlung gegenüber anderen aufgrund von Merkmalen, die keiner vernünftigen Rechtfertigung zugänglich sind. Die Schlechterbehandlung kann darin bestehen, dass einem Menschen medizinische Dienste vorenthalten oder von Versicherern nicht finanziert werden, dass bestimmte Leistungen nur gegen einem unfairen Preis bereitgestellt werden oder z. B., dass Arbeitgeber Bewerber wegen bestimmter Merkmale nicht berücksichtigen.[388]

Eine Rechtfertigung fehlt, wenn die Ungleichbehandlung mit Merkmalen begründet wird, für die rechtliche Diskriminierungsverbote bestehen. Derartige Verbote finden sich in Art. 3 Abs. 3 GG, wonach eine Benachteiligung oder Bevorzugung wegen Geschlecht, Abstammung, Rasse, Sprache, Heimat und Herkunft, Glauben, religiösen oder politischen Anschauungen verboten ist. In Art. 21 GRCh wird dieser Katalog erweitert um folgende Aspekte: Hautfarbe, Ethnie, soziale Herkunft, genetische Merkmale, Zugehörigkeit zu einer nationalen Minderheit, Vermögen, Geburt, Behinderung, Alter, sexuelle Ausrichtung und Staatsangehörigkeit.

Eine Diskriminierung erfolgt tendenziell auch in allen Fällen, bei denen eine per Big Data festgestellte Korrelation zu einer merkmalsbezogenen illegitimen Differenzierung führt. Hinter einer scheinbar wissenschaftlichen rationalen Differenzierung verbirgt sich nicht selten eine rein mathematisch-statistisch begründete Ungleichbehandlung.[389] Stellt ein Algorithmus z. B. an bestimmte Gesundheitsleistungen spezifische körperliche Anforderungen, so werden diejenigen ausgeschlossen, die diesen digitalen Vorgaben auf Grund ihrer körperlichen oder seelischen Konstitution nicht entsprechen können. Es zeigt sich immer wieder, dass Vorurteile beim Programmieren von Algorithmen zu

386 Deutscher Ethikrat S. 120, 137.
387 Deutscher Ethikrat S. 10.
388 Deutscher Ethikrat S. 13.
389 Selke in Stiftung Datenschutz (2017) S. 159 ff.; ders. Digitale Alchimisten, SZ 1./2.7.2017, 5.

Diskriminierungen führen, ohne dass dies den Handelnden bewusst wäre. Selbst beim Einsatz eines scheinbar neutralen Algorithmus kann es dadurch zu diskriminierenden Effekten kommen, dass von personalen Vorurteilen mitbestimmte Daten in die Auswertung einfließen. Kennzeichnend hierfür ist, dass nicht nur klassische Diskriminierungsmerkmale zur Ungleichbehandlung führen, sondern auch Merkmale, die zu diesen klassischen Merkmalen nur in seiner (oft indirekten) Korrelation stehen. Ein ausführlich behandeltes Beispiel ist die Autocomplete-Funktion im Internet, bei der bei Webinterface-Tastatureingaben, z. B. bei Netzsuchen, Treffervorschläge gemacht werden, von denen Diskriminierungen und Persönlichkeitsbeeinträchtigungen einhergehen können.[390]

Eine spezifische Form der Diskriminierung kann darin bestehen, dass sich eine Person weigert, Gesundheitsdaten in digitaler Form zu liefern, also z. B. durch die Verweigerung von Wearables gegenüber einer Versicherung oder einem Arbeitgeber. Dies ist dann der Fall, wenn der Person Vergünstigungen vorenthalten werden, die Nichtverweigerern gewährt werden (s. u. 10.5.3).

Eine weit verbreite Form der Diskriminierung im Gesundheitsbereich ist, dass das medizinische Angebot von der Zahlungsbereitschaft oder Zahlungsfähigkeit des Patienten abhängig gemacht wird. Das Problem der „Mehrklassenmedizin" besteht unabhängig von der Digitalisierung, etwa durch die Trennung zwischen gesetzlicher und privater Abrechnung. Da medizinische Leistungen Kosten verursachen, ist eine finanziell begründete Diskriminierung in einem gewissen Maße systemimmanent. Doch stößt eine derart begründete Ungleichbehandlung auf ethische und rechtliche Grenzen, soweit das Solidarprinzip für eine Leistungserbringung vorrangig ist und die Wesensgehalte von Würde- und Gesundheitsschutz verletzt werden. Finanziell begründete Differenzierungen können innerhalb eines einheitlichen Abrechnungssystems auf der Basis von Datenauswertungen erfolgen. In diesen Fällen steht dann nicht die Legitimität des Abrechnungssystems insgesamt zur Diskussion, sondern die des konkret eingesetzten Verfahrens.

5.5 Kommerzielle Ausbeutung (Beschäftigte, Verbraucher)

Hinter Big Data stehen regelmäßig ökonomische Erwägungen. Diese können in einem Marktvorteil für den Datenverarbeiter liegen, in einem (evtl. nicht gerechtfertigten) Ausschluss von Patienten oder von sonstigen Marktteilnehmern oder in einem übermäßigen Preis. Eine finanzielle Übervorteilung kann in einer ungenügenden Marktkenntnis des schwächeren Betroffenen, in fehlender Marktmacht oder einfach in Gleichgültigkeit begründet sein. Ein Ergebnis ist auch nicht selten die kommerzielle Ausbeutung einer prekären Gesundheitssituation von Menschen zur Maximierung von Unternehmensprofiten.

390 BGH 14.5.2013 – VI ZR 269/12, NJW 2013, 2348 ff. = JZ 2013, 789 ff. = DuD 2013, 663 ff. = MMR 2013, 535 ff. = DANA 2013, 132 f.; LG Wien 24.11.2016 – 13 Cg 16/16t-31, ZD 2016,7, 379; Rassismusvorwurf gegen Google wegen „Autocomplete"-Suchangebot, DANA 2012, 89 f.

Die Grenzen zwischen geschicktem Marktverhalten und „Ausbeutung“ sind fließend. Grenzen werden durch das Recht gezogen. Dieses hinkt aber oft den technischen Möglichkeiten und Praktiken sowie den gesellschaftlichen Notwendigkeiten hinterher. Die ökonomischen Konsequenzen von Big Data im Gesundheitsbereich und die Frage, inwieweit die wirtschaftlichen Erträge gerechtfertigt sind oder nicht, sind bisher noch nicht im Ansatz erörtert, geschweige denn geklärt. Ein Beispiel hierfür ist die Frage, inwieweit medizinische Datensätze wirtschaftlich genutzt werden dürfen, die zuvor sog. Anonymisierungserfahren durchlaufen haben, die zwar den direkten Personenbezug abschneiden, nicht aber die Personenbeziehbarkeit (s. o. 4.8).

5.6 Ansehensverlust, Akzeptanzverlust

Für medizinische Leistungserbringer wie auch für sonstige Unternehmen in den Bereichen Gesundheit und Informationstechnik können rechtliche und ethische Defizite, wenn sie öffentlich werden, zu einem Ansehensverlust und letztlich zu einem Kundenverlust führen. Bei Sicherheitsdefiziten hat dies lange Zeit dazu geführt, dass Unternehmen erfolgreiche Hackingattacken zu verschweigen versuchten. Inzwischen bestehen insofern gesetzliche Meldepflichten (§ 42a BDSGaF, Art. 33, 34 DSGVO, § 8 Abs. 1 BSI-G). Auch setzt sich bei den Unternehmen unabhängig von rechtlichen Verpflichtungen die Einsicht durch, dass bei Sicherheitslecks eine frühzeitige Information der Kunden vertrauensfördernd sein kann, wenn umgehend die sonstigen weiteren Schutzmaßnahmen ergriffen werden.

Im Gesundheitsbereich und bei Internetapplikationen spielt das Kundenvertrauen eine sehr große Rolle. Rechtsverstöße und insbesondere Vertraulichkeitsverletzungen haben regelmäßig Kundenabwanderungen und damit auch finanzielle Verluste zur Folge. Es liegen bisher nur wenige entsprechende Erfahrungen zu Rechtsverstößen und ethischen Grenzverletzungen beim Einsatz von Big Data vor. Doch ist es plausibel, dass insofern Risiken für die Verantwortlichen bestehen. So kündigte das Hasso-Plattner-Institut einen Big-Data-Forschungsauftrag der Schufa, bei dem es darum ging, aus Internetdaten Rückschlüsse auf die Bonität zu ziehen, nachdem es hiergegen in der Öffentlichkeit heftige Kritik gab.[391] Das isländische Gendatenbankprojekt deCode geriet in ethische, rechtliche und ökonomische Schieflage, nachdem bekannt wurde, welche umfassenden Auswertungen hierüber möglich und beabsichtigt sind.[392] Das anschaulichste Beispiel für Akzeptanzprobleme dürfte das Big-Data-Projekt „care.data“ des National Health-Service (NHS), des britischen staatlichen Gesundheitssystems, sein. Dieses ohne hinreichende Beteiligung der Patienten durchgeführte Projekt stieß u. a. deshalb auf Widerstand, weil die erfassten Daten auch für kommerzielle Zwecke weitergegeben und der Polizei zur Verfügung gestellt werden sollten.[393]

391 Hasso-Plattner-Institut kündigt Forschungsauftrag der Schufa, DANA 2012, 118 f.

392 deCODE Genetics insolvent, DANA 2010, 36; Gericht erklärt Gendatenbank-Gesetz für verfassungswidrig, DANA 2/2004, 34; Chemiekonzern kauft sich Gencodes der Gesamtbevölkerung, DANA 1/1999, 31.

393 Lokshin, Patientendaten: Der elektronische englische Patient, www.zeit.de 9.4.2014.

5.7 Gesamtgesellschaftliche Risiken

Die oben aufgeführten Risiken für Individuen und Institutionen können zu Risiken für die gesamte Gesellschaft kumulieren. Diskriminierungen und Beschränkungen der individuellen Freiheiten tragen zu einem gesamtgesellschaftlichen Klima bei, in dem die Menschen von der **Wahrnehmung ihrer demokratischen und sozialen Rechte** abgehalten oder gehindert werden. Diese Befürchtungen haben vielfach Ausdruck in der dystopischen Literatur gefunden. Ein Beispiel ist „Schöne neue Welt" von Aldous Huxley, wo die biotechnische Manipulation von Menschen die Grundlage einer autoritären Gesellschaft schafft. In „Corpus Delicti" von Juli Zeh werden die Menschen durch eine Gesundheitsdiktatur fremdbestimmt, die durch implantierte Chips und eine staatliche Totalkontrolle der darüber erhobenen Körperwerte ermöglicht wird.[394] Der Aspekt gesundheitlicher Fremdbestimmung spielt auch in Dave Eggers „Der Circle" ein Rolle, wo eine von einer Privatfirma ausgehende schleichende, durch Verarbeitung von Daten, auch von Gesundheitsdaten, ausgehende Herrschaftsübernahme dargestellt wird, die u. a. mit folgendem Leitmotiv zu legitimieren versucht wird: „Um zu heilen, müssen wir wissen. Um zu wissen, müssen wir (Daten, T. W.) teilen."[395]

Ein zentrales demokratiepraktisches Problem von Big Data besteht darin, dass diese Verfahren regelmäßig intransparent sind, mit einer hohen Akzeptanz versehen sind, den Nimbus der objektiven Wissenschaftlichkeit genießen und die realen Verantwortlichen oft nicht benannt, manchmal nicht benennbar sind. Demokratie lebt vom **öffentlichen, pluralen und transparenten Diskurs** subjektiver, zumeist interessengetriebener Ansichten, zu dem sich die Mehrheit eine Meinung bilden soll, die letztlich – transponiert über demokratische Mechanismen – in gesellschaftlich relevante Entscheidungen einfließen. Bei Big Data besteht die Gefahr, dass dem Algorithmus Entscheidungsmacht zugewiesen wird, ohne dass dieser politisch zur Verantwortung gezogen werden könnte (s. u. 6.19).

Die Biotechnik mit ihren rasanten Fortschritten eröffnet gesellschaftliche Risiken und ethische Fragen, die in der Öffentlichkeit – anders als die Risiken der Gentechnik in den 1990er Jahren – bisher nur wenig diskutiert werden. Dies mag teilweise auf eine gesellschaftsweite technikeuphorische Grundeinstellung zurückzuführen sein. Auch die informations- und medizintechnische Komplexität trägt dazu bei, dass eine breite **öffentliche Debatte** bisher unterbleibt. Hierfür ausschlaggebend ist aber auch, dass von vielen Verantwortlichen gezielt Transparenz zu den von Ihnen betriebenen Verfahren verweigert und hintertrieben wird. Dies gilt insbesondere für die IT- und Medizininformations-Unternehmen, die mit der kommerziellen Ausbeutung von Gesundheitsdaten ein gutes Geschäft machen.[396]

Neben die Diskriminierungs- und Ausgrenzungsrisiken, die mit der Genanalyse entstehen, tritt mit dem Genome Editing, also dem Eingriff in das Erbgut von Lebewesen und des

394 Zeh, Corpus Delicti – Ein Prozess, 2009.
395 Eggers, Der Circle, 2014, S. 175.
396 Ein Lehrbeispiel hierfür ist die Auseinandersetzung zwischen dem ULD und der VSA, vgl. XX m. w. N.

Menschen das Risiko der Beeinflussung des genetischen Materials von Mensch und Umwelt. Bei der Werbung für diese Techniken werden Präzisionsversprechen gemacht, deren Einhaltung bzw. Realitätsnähe nur beschränkt überprüfbar sind. Im Hinblick darauf, dass die aktuelle technische Entwicklung weitgehend ökonomisch und nicht gemeinwohlgetrieben ist, muss befürchtet werden, dass für die Praxis nicht die Linderung und Eindämmung gesellschaftlicher Krankheiten im Vordergrund steht, sondern größtmögliche Verdienstmöglichkeiten oder unethische Erwägungen wie die Perfektionierung des Menschen über „Designerbabys".[397]

6 Verfassungsrechtliche Grundlagen

Big Data erfolgt nicht im rechtsfreien Raum. Jede praktische Anwendung hat die gesetzlichen Vorgaben zu beachten, deren Ausrichtung und Grenzen durch den verfassungsrechtlichen Rahmen festgelegt sind. Dieser wird auf nationaler Ebene durch das Grundgesetz (GG) gesetzt. Die hier zu findenden Vorgaben werden auf EU-Ebene durch die europäische Grundrechte-Charta (GRCh) konkretisiert und bekräftigt. Da zwischen diesen beiden grundlegenden Werken keine unterschiedlichen Wertentscheidungen, sondern allenfalls unterschiedliche Formulierungen und Konkretisierungsgrade bestehen, werden im Folgenden GG und GRCh gemeinsam behandelt.

Das Grundgesetz gilt für alle vom deutschen Recht erfassten Sachverhalte. Die GRCh gilt gemäß Art. 51 Abs. 1 S. 1 GRCh für die Organe, Einrichtungen, Ämter und Agenturen der Union. Weiterhin gilt sie „für die Mitgliedstaaten ausschließlich bei der Durchführung des Rechts der Union". Der Anwendungsbereich der GRCh erstreckt sich also nicht, wie dies beim GG der Fall ist, auf die gesamte Anwendung des deutschen Rechts, sondern nur, soweit dieses durch europäische Regelungen vorgegeben wird sowie wenn europäisches Recht direkt anwendbar ist. Eine Umsetzung durch nationales Recht ist regelmäßig bei europäischen Richtlinien erforderlich; eine direkte Anwendbarkeit besteht bei Verordnungen, wozu die europäische Datenschutz-Grundverordnung (DSGVO) gehört.

Die grundrechtliche Bewertung von Big Data kann nicht losgelöst von der technischen Entwicklung, den ökonomischen und sozialen Umständen sowie den kulturellen Normen und Werten erfolgen. Trotz einer gewissen Kulturvarianz lassen sich die Grundrechte und ihre Bedeutung zeit- und ortsunabhängig sozialanthropologisch bestimmen. Dieses Verständnis kommt u. a. dadurch zum Ausdruck, dass der Wesensgehalt der Grundrechte zu achten ist (Art. 52 Abs. 1 GRCh). Diese Formulierung ist weniger streng als Art. 19 Abs. 2 GG, wonach der Wesensgehalt nicht „angetastet werden", also unter keinen Umständen beeinträchtigt werden darf.[398]

---

397 Dabrock, Bevor es zu spät ist, SZ 30.8.2017, 2; Gen-ethisches Netzwerk, Faltblatt Genome Editing – Heilversprechen Präzision.

398 Becker in Schwarze, Art. 52 GRC Rn. 7; Borowsky in Meyer Art. 52 Rn. 23-23b; , zum Datenschutz Bock/Engeler DVBl 2016, 593 ff.

Grundrechte zielen vorrangig auf den Schutz des Individuums. Dessen ungeachtet ist es gerade im informationellen Umgang mit Einzelnen oft von größter Relevanz, welchen (möglicherweise identitätsstiftenden) Gruppen bzw. Merkmalseigenschaften eine Person zugeordnet wird. Hieraus lässt sich die Notwendigkeit eines **Kollektiv-Grundrechtsschutzes** ableiten, über den Diskriminierungen vermieden werden sollen.[399] Auch eine anonymisierte Verarbeitung und Nutzung von Daten kann individuell Grundrechte verletzen, wenn dabei Gruppenmerkmale verwendet werden, denen sich der Betroffene in der Praxis nicht entziehen kann.[400]

6.1 Drittwirkung von Grundrechten

Die Ausprägungen der Grundrechte, etwa des allgemeinen Persönlichkeitsrechts (s. o. 6.5, 6.6) schützen nicht nur vor direkten staatlichen Eingriffen, sondern entfalten als **objektive Normen** ihren Rechtsgehalt auch im Privatrecht. Entsprechendes gilt für die Kommunikationsrechte des Art. 5 GG bzw. der Art. 11 u. 13 GRCh. Dies ist inzwischen sowohl vom BVerfG wie auch vom EuGH anerkannt. In dieser Eigenschaft strahlt das Verfassungsrecht auf die Auslegung und Anwendung privatrechtlicher Vorschriften aus.[401]

Den Grundrechten kommt nicht nur eine individuelle, subjektiv-rechtliche, sondern auch eine **gesellschaftliche, objektiv-rechtliche Funktion** zu. Die Verletzung des Rechts beeinträchtigt nicht nur die individuellen Entwicklungschancen des Einzelnen, „sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist".[402] Daraus können sich **staatliche Schutzpflichten** ergeben.[403] Zur staatlichen Schutz- und Gewährleistungspflicht gehört auch der sich aus Art. 19 Abs. 4 GG und Art. 47 GRCh ergebende Anspruch auf gerichtlichen Rechtsschutz.[404]

Dem allgemeinen Persönlichkeitsrecht und den damit zusammenhängenden Grundrechten kommen als Normen des objektiven Rechts eine **Drittwirkung im Bereich der Wirtschaft** zu.[405] Daher können sich aus Persönlichkeitsverletzungen durch Private zivilrechtliche Schadensersatzforderungen oder Ansprüche aus unerlaubter Handlung ergeben.[406] Dieser

399 Zum Kollektivdatenschutz Weichert in Däubler u. a., BDSG, Einl Rn. 51.

400 Ladeur DuD 2016, 364 spricht hierbei in Bezugnahme auf Ridder von „impersonalen Grundrechten"; ein praktisches Beispiel findet sich bei Verbraucherzentrale Bundesverband, Verbraucher als „Eigentümer" von Mobilitätsdaten? Stellungnahme vom 3.11.2017, S. 11 f.

401 BVerfG, NJW 1991, 2411; ständige Rspr.; BVerfG, NJW 2013, 3087; für den Anwendungsbereich des Art. 8 EMRK EGMR 5.9.2017 – Az. 61496/08.

402 BVerfGE 65, 43 = NJW 1984, 422; Seubert, DuD 2012, 100.

403 Papier NJW 2017, 3029; Deiseroth, DVBl 2015, 199; Hoffmann-Riem JZ 2014, 56; Weichert, DANA 2014, 67; Schliesky/Hoffmann/Luch/Schulz/Borchers, Schutzpflichten im Internet, 2014; Rupp, Die grundrechtliche Schutzpflicht des Staates für das Recht auf informationelle Selbstbestimmung im Presse-sektor, 2013; Kutscha, DuD 2011, 464; Kipker/Voskamp, RDV 2014, 84; relativierend Ullrich, DVBl 2015, 204; Bizer DuD 2007, 265.

404 EuGH 6. 10. 2015 – C-362/14, Rn. 95 – Safe Harbor.

405 Für das Europarecht ebenso Selmayr/Ehmann in Ehmann/Selmayr Einf Rn. 36; Däubler Rn. 134a.

406 BGH, NJW 2007, 689; Balthasar, NJW 2007, 664; Helle, JZ 2007, 444.

durch die Rechtsprechung anerkannte Grundsatz wird durch den Entwurf einer digitalen Grundrechte-Charta für Europa bekräftigt (s. u. 6.2). In Art. 1 Abs. 3 dGRCh-E wird die Drittwirkung auf alle Grundrechte erstreckt: „Die Rechte dieser Charta gelten gegenüber staatlichen Stellen und Privaten".

Im Bereich des öffentlichen Rechts erfolgt regelmäßig eine **Abwägung** zwischen öffentlichen Verarbeitungs- und individuellen Schutzinteressen. Im Privatrechtsverkehr muss eine Abwägung der u. U. sich gegenüberstehenden Interessen unterschiedlicher Grundrechtsträger erfolgen.[407] Die staatliche Schutzpflicht gebietet, die Voraussetzungen eines wirkungsvollen informationellen Selbstschutzes bereitzustellen. Dies gilt insbesondere dann, wenn private Stellen ein solches ökonomisches, technisches oder organisatorisches Gewicht haben, dass sie die informationellen Vorgänge zu Personen (Betroffenen) faktisch einseitig bestimmen können.[408]

Die Drittwirkung der Grundrechte ist bei **Big-Data-Anwendungen im Gesundheitsbereich** hoch relevant, da diese geprägt sind von einem Ungleichgewicht zwischen verarbeitender Stelle und Betroffenen, und zwar in informationstechnischer, ökonomischer, rechtlicher und sozialer Hinsicht. Zudem bestehen in vielen Fällen wegen der besonderen (Not-) Situation der Betroffenen weitergehende Abhängigkeiten der Betroffenen, die zu einer verstärkten rechtlichen Bindung der Verantwortlichen führen.

6.2 Weiterentwicklung des Verfassungsrechts

Zwar bestehen seit der Aufklärung in Europa weitgehend einheitliche Überzeugungen zu den verfassungsrechtlichen Grundlagen eines modernen freiheitlichen und demokratischen Gemeinwesens. Diese bestehen in der Anerkennung der Würde und der gleichen und unveräußerlichen Rechte aller Menschen, was Freiheit, Gerechtigkeit und Frieden in der Welt voraussetzt. Dessen ungeachtet sind die Formulierung dieser Grundwerte und deren Konkretisierung von den ökonomischen und sozialen Bedingungen abhängig. Die Informatisierung bzw. Digitalisierung der Gesellschaft hat zu Veränderungen unserer Existenz und der existenziellen Rahmenbedingungen geführt. Ein Ausdruck hierfür ist die GRCh, die z. B. gegenüber dem GG mit dem Grundrecht auf Datenschutz in Art. 8 hierauf eine explizite Antwort gibt. Der Prozess der Modernisierung der Grundrechte und der Anpassung an die technischen Gegebenheiten ist damit aber nicht abgeschlossen. Die Forderung nach einer weiteren **„Digitalisierung" der Grundrechte** steht weiterhin auf der Agenda der politischen Diskussion.[409]

Einen ersten Formulierungsvorschlag für eine „Charta der digitalen Grundrechte der Europäischen Union" wurde Ende 2016 von einer Gruppe prominenter Einzelpersonen

---

407 Giesen, JZ 2007, 918 versucht fälschlich aus Art. 2 GG und weiteren Grundrechten als Gegenrecht ein „Grundrecht auf Datenverarbeitung" abzuleiten.

408 BVerfG 23.10.2006 – 1 BvR 2027/02, Schweigepflichtentbindung, NJW 2007, 576; Papier NJW 2017, 3030.

409 Weichert, Codex Digitalis Universalis in Schmidt/Weichert 345 ff.; ders., Globaler Kampf um digitale Grundrechte, KJ 2014, 123 ff.

vorgelegt.[410] Dieser Entwurf einer **europäischen digitalen Grundrechte-Charta** (dGRCh-E) geht davon aus, dass sich neue Gefährdungen ergeben „durch Big Data, künstliche Intelligenz, Vorhersage und Steuerung menschlichen Verhaltens, Massenüberwachung, Einsatz von Algorithmen, Robotik und Mensch-Maschine-Verschmelzung sowie Machtkonzentration bei privaten Unternehmen“ (Art. 1 Abs. 2 dGRCh-E).

6.3 Würdeschutz

Art. 1 Abs. 1 GG sowie Art. 1 GRCh erklären im Einklang mit völkerrechtlichen Rechtsquellen die Würde des Menschen als unantastbar. Die Menschenwürde kann nicht nur materiell verletzt werden, etwa durch Folter, Sklaverei, Leibeigenschaft, Menschenhandel, Deportation, Vertreibung oder grausame Bestrafung, sondern auch durch **immaterielle Maßnahmen** wie z. B. „Diffamierung, Diskriminierung, Erniedrigung, Brandmarkung, Verfolgung und Ächtung“.[411] Derartige Maßnahmen gehen nicht nur von staatlichen Instanzen, sondern auch von Privaten aus. Die Würdegarantie ist nicht als Abwehrrecht, sondern als Garantie formuliert. Sie begründet daher auch ein Drittwirkung und eine staatliche Schutzpflicht (s. o. 6.1).

Der Würdeschutz ist im Zusammenhang mit den weiteren Grundrechten zu sehen. Er ist für sich alleine eher konturenlos. Es handelt sich hierbei um eine Art Auffanggrundrecht, mit dem ein **absolut geschützter menschlicher Bereich** geschaffen wird.[412] Er schützt höchstpersönliche, intime Zustände und Handlungen und damit den Kernbereich privater Lebensgestaltung.[413] Insofern war es konsequent, dass das BVerfG angesichts der Digitalisierung aller Lebensbereiche eine Weiterentwicklung zu einem eigenständigen Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme vorgenommen hat (s. u. 6.6).[414]

Eine Grunderwägung des Würdeschutzes besteht darin, dass der Mensch **nicht zum bloßen Objekt degradiert** und in seiner Subjektqualität in Frage gestellt werden darf.[415] Dies schließt zwar nicht die Digitalisierung des Menschen sowie von Merkmalen zu seiner Person aus. Doch darf dies nicht dazu führen, dass der Mensch in seiner Behandlung hierauf reduziert wird. Der Mensch ist mehr als die Summe seiner Daten und muss demgemäß auch so behandelt werden.[416] Dies ist z. B. bei ihn betreffenden automatisierten Entscheidungen zu beachten (s. u. 8.9).

Der Bundesgerichtshof (BGH) entschied schon im Jahr 1954 über die Frage der Vereinbarkeit einer technischen Erhebung von körperrelevanten Daten durch einen **Lügendetektor** mit der Menschenwürde. Er stellte eine Verletzung fest, „weil auch das

410 digitalcharta.eu, abgedruckt z. B. in SZ 1.12.2016 25.
411 BayVerfGH BayVBl 1982, 50; Nettesheim, Die Garantie der Menschenwürde, AöR 103 (2005), 79.
412 Hoffmann u. a. S. 28
413 Roggan StV 2011, 762 ff.
414 BVerfG 27.2.2008 – 1 BvR 370/07 u. 1 BvR 595/07, NJW 2008, 822.
415 BVerfG 16.7.1969 – 1 BvL 19/63, NJW 1969, 1707 = BVerfGE 27, 6.
416 Kamps in Langkafel S. 78; Heckmann/Paschke in Stiftung Datenschutz (2017) S. 74 f.

Unbewusste“ antworte und man hiermit beim Menschen „Einblick in seine Seele“ nehmen könne.[417] Die kategorische Ablehnung der Methode wurde über 40 Jahre später vom BGH dahingehend relativiert, dass ein Einsatz der Technik mit Einwilligung eines strafrechtlich Beschuldigten zulässig sein kann, weil die Menschenwürde auch die Freiheit, „über sich selbst zu verfügen und sein Schicksal eigenverantwortlich gestalten zu können“, schützt.[418] Eine Übertragung dieser Rechtsprechung auf den Einsatz von Big Data im Gesundheitswesen führt dazu, dass dieser ohne Gewährleistung der Selbstbestimmung der Betroffenen grundsätzlich nicht zulässig sein kann.

6.4 Schutz von Leben, Unversehrtheit und Gesundheit

Gemäß Art. 2 Abs. 2 S. 1 GG hat „jeder das Recht auf Leben und körperliche Unversehrtheit“. Dieses Recht wird in Art. 2 Abs.1 GRCh mit einem „Recht auf Leben“ bestätigt und in Art. 3 Abs. 1 GRCh dahingehend konkretisiert, dass auch die „geistige Unversehrtheit“ gewährleistet wird. Art. 3 Abs. 2 GRCh enthält „im Rahmen der Medizin und der Biologie“ weitere Präzisierungen, u. a. „a) die freie Einwilligung des Betroffenen nach vorheriger Aufklärung entsprechend den gesetzlich festgelegten Einzelheiten, b) das Verbot eugenischer Praktiken, insbesondere derjenigen, welche die Selektion von Menschen zum Ziel haben“. Art. 35 S. 1 GRCh gewährt jedem Menschen „das Recht auf Zugang zur Gesundheitsvorsorge und auf ärztliche Versorgung nach Maßgabe der einzelstaatlichen Rechtsvorschriften und Gepflogenheiten. In Art. 168 Abs. 1 AEUV ist für die EU vorgesehen, dass bei der Festlegung und Durchführung aller Unionspolitiken und -maßnahmen „ein hohes Gesundheitsschutzniveau sichergestellt“ wird. Das Recht auf Unversehrtheit stellt einen Bezug zum menschlichen Körper und damit zur analogen Welt her. Dessen ungeachtet hat das Grundrecht eine zunehmende digitale Relevanz, nämlich immer dann, wenn die digitale Datenverarbeitung analoge Reaktionen auf den Menschen, also auf dessen körperliche und seelische Unversehrtheit zeigt.[419]

Derartige Auswirkungen ergeben sich beim Einsatz digitaler Technik im Bereich der medizinischen Versorgung, der Behandlung und Pflege. Datenverarbeitung muss so ausgeführt werden, dass Leib und Seele der Menschen nicht beeinträchtigt, sondern gefördert werden. Das gilt in besonderem Maße beim Einsatz von Big Data, also bei komplexer Datenverarbeitung und im Bereich der Apparatemedizin, wo Fehler zu direkten Schäden führen können.

Neben derartigen direkten Auswirkungen finden auch weniger offensichtliche Beeinträchtigungen der Unversehrtheit durch die digitale Verarbeitung generell sowie durch Big Data statt. Cypermobbing, also die über das Internet erfolgende Ehrverletzung, bewirkt nicht nur Verletzungen des allgemeinen Persönlichkeitsrechts der Betroffenen, sondern kann negative Auswirkungen auf die körperliche und psychische Konstitution des

417 BGH 16.2.1954 – 1 StR 578/53, NJW 1954, 649; ähnlich BVerfG 18.8.1981 – 2 BvR 166/81, NJW 1982, 375.
418 BGH 17.12.1998 – 1 StR 156/98, NJW 1999, 657.
419 Hoffmann u. a. S. 113.

Menschen haben. In vielen Fällen ist Cybermobbing hierauf ausdrücklich angelegt. Derartige Auswirkungen können bis zum Suizid führen. Digitale Angriffe können insofern sowohl subjektiv wie auch objektiv die Dimension gewalttätiger Übergriffe erlangen (s. o. 5.1).[420]

Verletzungen der Unversehrtheit bedingen keinen vorsätzlichen Angriff und keine Intention. So führen z. B. auf künstlicher Intelligenz basierende Verfahren des Autocomplete im Internet möglicherweise zu individuellen Merkmalszuweisungen, die über Beleidigungen hinausgehen und eine mit dem Cybermobbing vergleichbare Wirkung entfalten können.[421] Entsprechende Wirkungen können erst recht durch Nachrichtengenerierungen im Internet durch Robots entstehen, die Fake-News verbreiten, die die Betroffenen substanziell verletzen.

Eine andersartige indirekte Beeinträchtigung der Unversehrtheit durch Big Data kann dadurch bewirkt werden, die für das seelische und körperliche Wohlbefinden erforderliche äußere Infrastruktur verletzt oder gar zerstört wird, so dass z. B. die Versorgung mit Lebensmitteln oder mit Medikamenten nicht mehr gewährleistet ist (s. o. 4.4).

6.5 Grundrecht auf Datenschutz

Das Grundrecht auf Datenschutz wurde erstmals vom BVerfG im Volkszählungsurteil 1983 als „Recht auf informationelle Selbstbestimmung“ aus dem allgemeinen Persönlichkeitsrecht gemäß Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG abgeleitet. Es ist inzwischen in Art. 8 GRCh in den EU verfassungsrechtlich normiert und auch darüber hinausgehend, etwa durch den Europäischen Gerichtshof für Menschenrechte (EGMR), aus Art. 8 EMRK abgeleitet [422], anerkannt. Unter den modernen Bedingungen der Datenverarbeitung soll die freie Entfaltung der Persönlichkeit des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe persönlicher Daten geschützt werden.[423] Ein spezifischer rechtlicher Schutz wurde schon vor 1983 im Recht am eigenen Bild und am gesprochenen Wort gesehen.[424] Das BVerfG stellte fest, dass verdachtslose informationelle sowie heimliche Erfassungen besonders schwere Eingriffe darstellen.[425] Zwar ist grds. jedes personenbezogene Datum schutzbedürftig; es gibt kein „belangloses Datum“. Der konkrete Schutzbedarf hängt aber von der Art der Verarbeitung und dem Kontext (Verantwortlicher, Verarbeitungszweck) ab. Informationelle Selbstbestimmung bedeutet nicht nur, von ungewollter Fremdbestimmung verschont zu

---

420 Hoffmann u. a. S. 115.

421 Dazu: Rassismusvorwurf gegen Google wegen „Autocomplete“, DANA 2012, 89 f.; BGH, NJW 2013, 2348 = ZD 2013, 405 mit Anm. Hoeren = DuD 2013, 663 = RDV 2013, 197 = JZ 2013, 789 = MMR 2013, 535; einschränkend OLG Köln, DuD 2013, 413; hierzu generell Weichert, ZRP 2014, 168; ders. in Roggan/Busch, Das Recht in guter Verfassung, Kutscha-Festschrift, 2013, S. 147.

422 Siemen, Datenschutz als europäisches Grundrecht, 2006, S. 51 ff.

423 BVerfG 15. 12. 1983, NJW 1984, 422; grundlegend Eichenhofer in Der Staat 55 (2016), 41-67.

424 Zum Recht am eigenen Bild in sozialen Netzwerken Lauber-Rönsberg NJW 2016, 744; Tausch, Persönlichkeitsrechtsverletzungen durch die Veröffentlichung von Fotos im Internet, 2016.

425 Weichert in Däubler u. a., Einl. Rn. 7.

werden, sondern auch selbstbestimmt in der Interaktion zu anderen Personen und Institutionen Beziehungen eingehen zu können und sich hierbei zu offenbaren.[426]

Wegen seiner zentralen Bedeutung soll Art. 8 GRCh hier wörtlich zitiert werden:

Schutz personenbezogener Daten
(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.
(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.
(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

Gemäß diesen Vorgaben sind für das Grundrecht prägend die Zweckbindung (s. u. 8.6), ein Auskunftsanspruch (s. u. 8.17) sowie die unabhängige staatliche Kontrolle (s. u. 8.19).

Das Grundrecht auf Datenschutz hat eine Schutzfunktion sowohl für das Individuum wie auch für die Gesellschaft.[427] Hinsichtlich der sozialen Funktion geht es nicht nur um den Schutz der Freiheitsrechte und die Wahrung der Demokratie, sondern auch um den gesundheitlichen Schutz der Gesellschaft.

Der Schutz informationeller Selbstbestimmung in Bezug auf Gesundheitsdaten ist auch als Aspekt des Schutzes einer umfassender verstandenen medizinischen Selbstbestimmung zu sehen. Danach hat jede Person das Recht, selbst frei über sich zu entscheiden, einschließlich der Verfügung über den eigenen Körper und die eigene Seele.[428]

Aus dem allgemeinen Persönlichkeitsrecht nach Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG bzw. dem Grundrecht auf Achtung des Privatlebens nach Art. 7 GRCh leitet sich ein Anspruch auf besonderen Schutz der Intimsphäre[429] ab sowie auf einen unantastbaren Kernbereich privater Lebensgestaltung.[430] Er umfasst die Möglichkeit, innere Vorgänge – wie Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art – zum Ausdruck zu bringen; ebenfalls werden dazu Gefühlsäußerungen, Äußerungen des unbewussten Erlebens sowie Ausdrucksformen der Sexualität gezählt. Der Kernbereich ist tangiert, wenn ein Sachverhalt seinem Inhalt nach

426 Deutscher Ethikrat S. 85.
427 BVerfG 15.1.1983 – 1 BvR 209/83 u. a., NJW 2984, 422.
428 Deutscher Ethikrat S. 19, 116 ff.; Rehborn in Prütting § 7 MBOÄ Rn. 5; Weichert DuD 2014, 832.
429 Rössler, Der Wert des Privaten, 2001; Brink in Wolff/Brink Syst. C Rn. 15; Deutscher Ethikrat S. 125 ff.
430 BVerfG 14.9.1989 – 2 BvR 1062/87, BVerfGE 80, 373 = NJW 1990, 563 (Tagebuch); BVerfG 3.3.2004 – 1 BvR 2378/98 u. 1 BvR 1084/99, BVerfGE 109, 279 = NJW 2004, 999 = DVBl 2004, 557 = MMR 2004, 302 (Großer Lauschangriff); Ronellenfitsch in Wolff/Brink Einl. Rn. 25; Weichert in Däubler u. a. Einl. Rn. 18; kritisch Dammann, Der Kernbereich der privaten Lebensgestaltung, 2011.

höchstpersönlichen Charakter hat, ohne wesentlich in Art und Intensität die Sphäre anderer oder die Belange der Gemeinschaft zu berühren.[431]

Die biotechnologische Entwicklung mit der Entzifferung des menschlichen Genoms und der zunehmenden Fähigkeit, aus Gensequenzen Rückschlüsse auf persönliche (körperliche und seelische) Eigenschaften und Anlagen zu ziehen, eröffnet eine völlig neue persönlichkeitsrechtliche Problematik: Angesichts der Unabänderbarkeit genetischer Dispositionen und des Umstands, dass deren Kenntnis, z. B. von unheilbaren Krankheiten, die erst in einigen Jahren ausbrechen werden, massive Einschränkungen der persönlichen Freiheiten bedeuten können, hat sich die Notwendigkeit der Ableitung eines Rechts auf Nichtwissen bezüglich genetischer Daten ergeben.[432] Die Wahrnehmung informationeller Selbstbestimmung liegt u. U. darin, keine Kenntnis von genetischen Dispositionen nehmen zu wollen. Über den genetischen Bereich hinaus stellen sich vergleichbare Fragestellungen bei der medizinischen Diagnostik sowie möglicherweise in weiteren Lebensbereichen.[433]

6.6 Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme

Mit dem Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme reagierte das BVerfG auf die zunehmende Bedeutung informationstechnischer Systeme für die Lebensführung der Menschen und deren Allgegenwärtigkeit.[434] Das mit Urteil im Jahr 2008 aus dem allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) abgeleitete neue Grundrecht soll Schutzlücken schließen, die von anderen Grundrechten, vor allem dem Recht auf informationelle Selbstbestimmung und dem Schutz des Fernmeldegeheimnisses nach Art. 10 GG und der Wohnung nach Art. 13 GG nicht abgedeckt sind. Zielsetzung ist der Schutz des Vertrauens in die eigengenutzten IT-Systeme, die Schaffung einer elektronischen, bzw. genauer, digitalen Privatsphäre. Die heimliche Infiltration eines geschützten informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können, ist danach nur zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut, wie z. B. Leib, Leben, Freiheit oder Person oder für die Existenz der Menschen grundlegende Güter der Allgemeinheit, vorliegen. Ein entsprechendes Grundrecht besteht bisher auf europäischer Ebene nicht und wurde auch nicht vom EuGH aus den sonstigen Grundrechten der GRCh abgeleitet bzw. anerkannt.

---

431 Puschke/Singelnstein, NJW 2005, 3536; Baldus, JZ 2008, 218; Poscher, JZ 2009, 269.

432 Donner/Simon, DÖV 1990, 913; Stumper, DuD 1995, 511, 514; Weichert, DuD 2002, 142; Heckmann/Paschke in Stiftung Datenschutz (2017) S. 79.

433 Vgl. Gendiagnostikgesetz – GenDG, BGBl. I 2009, S. 2529; vgl. Art. 3 Abs. 2 GRCh; BGH, NJW 2014, 2190 = ZD 2014, 465; Schneider, NJW 2014, 3133; Duttge, DuD 2010, 34; Tinnefeld, RDV 2010, 213; Weichert in Däubler u. a., BDSG, Einl. Rn. 56; Röhrig/Weigand in Langkafel S. 110 f.; Bergh/Brandner/Kutscha/Heinze/Schreiweis in Stiftung Datenschutz, S. 29.

434 BVerfG 27.2.2008 – 1 BvR 370/07 u. 1 BvR 595/07, NJW 2008, 822 = DÖV 2008, 459 = MMR 2008, 315 = DVBl 2008, 582.

Spezifischer Gegenstand des Grundrechtsschutzes sind die **von Betroffenen genutzten eigenen, zumeist vernetzten IT-Systeme** und informationstechnischen Komponenten, die im Alltag zum Einsatz kommen, etwa in Form von Geräten im Smart Home oder als mobile Geräte (Smartphone, Tablet, Laptop, Personal Digital Assistant - PDA, Kfz-IT) für die individuelle Persönlichkeitsentfaltung von zentraler Bedeutung geworden sind. Eingriffe in dieses sog. Computergrundrecht bedürfen einer spezifischeren (engeren und präziseren) Grundlage als Eingriffe in das Recht auf informationelle Selbstbestimmung und im Rahmen der Güterabwägung einer höheren Legitimation, so wie diese auch bei Eingriffen nach Art. 10 oder 13 GG gefordert ist. Dies gilt insbesondere für heimliche Eingriffe.

6.7 Kommunikationsgeheimnis

Art. 10 Abs. 1 GG schützt das „Briefgeheimnis sowie das Post- und Fernmeldegeheimnis". Demgemäß garantiert Art. 7 GRCh u. a. das Recht jedes Menschen auf Achtung seiner Kommunikation, wozu auch die Vertraulichkeit der elektronischen Kommunikation gehört. Sind bei der **elektronischen Kommunikation** personenbezogene Daten betroffen, ist neben dem Schutz des Telekommunikationsgeheimnisses zugleich der Schutzbereich des Grundrechts auf Datenschutz (s. o. 6.5) mit erfasst. Während das BVerfG Art. 10 GG als Spezialregelung zum Grundrecht auf informationelle Selbstbestimmung ansieht[435], werden vom EuGH die Art. 7 und 8 GRCh als sich gegenseitig ergänzend behandelt.[436]

Geschützt wird die Telekommunikation, also die **Übermittlung von Informationen**. Welche Vorgänge vom Schutz des Telekommunikationsgeheimnisses erfasst sind, war lange Zeit unklar. Inzwischen dürfte allgemein anerkannt sein, dass der Schutz endet, wenn eine Nachricht beim Empfänger angekommen ist und von diesem abgerufen wurde, so dass er diese zur Kenntnis nehmen und evtl. weiterverarbeiten konnte.[437] Geschützt sind also sowohl Inhalte wie auch Umstände der laufenden Kommunikation. Nicht erfasst sind Inhalte und Umstände, die sich nach Abschluss des Kommunikationsvorgangs im Herrschaftsbereich des Nutzers befinden.[438]

Das **Kommunikationsgeheimnis** unterscheidet sich vom Datenschutz dadurch, dass nicht nur die Daten natürlicher Personen und deren Kommunikation geschützt sind, sondern auch die juristischer Personen und deren Geheimnisse. Dieser Schutz durch Art. 7 GRCh bzw. Art. 10 GG gilt auch für die Kommunikation zwischen juristischen Personen und ist davon unabhängig, ob es sich bei dem Inhalt der Kommunikation um Informationen über natürliche Personen, juristische Personen oder Sonstiges handelt. Dies hat zur Folge, dass selbst die Kommunikation zwischen Maschinen in den Schutzbereich fällt. Erfasst sein

---

435 BVerfG 2.3.2010, 1 BvR 256/08 u. a., Rn. 191, NJW 2010, 836.

436 EuGH 26.7.2017, Gutachten 1/15, PNR, Rn. 122-124; EuGH 21.12.2016, C-203/15, C-698/15, Rn. 112, DVBl 2017, 182; zum Verhältnis Art. 7 zu Art. 8 Michl DuD 2017, 349.

437 BVerfG 13.11.2010, 2 BvR 1124/10, Rn. 13.

438 BVerfG 16.6.2009 – 2 BvR 902/06, BVerfGE 124, 43 ff. = MMR 2009, 674 f.; BVerfG 27.2.2008 – 1 BvR 370/07, BVerfGE 120, 307 f. = NJW 2008, 828; BVerfG 2.3.2006 – 2 BvR 2099/04, BVerfGE 115, 183 ff. = NJW 2006, 978.

können also auch Betriebs- und Geschäftsgeheimnisse, die zusätzlich den Schutz durch Art. 14 GG bzw. 17 GRCh genießen (s. u. 6.16).

6.8 Berufliche Schweigepflicht

Berufsgeheimnisse sind bisher nicht ausdrücklich im GG oder in der GRCh garantiert. Wohl aber haben sowohl das BVerfG wie auch der EuGH[439] einen verfassungsrechtlichen Schutz anerkannt. Gegenüber bestimmten Berufs- und anderen Personengruppen kann von Verfassungs wegen eine besondere Vertraulichkeit Voraussetzung sein, die rechtliche Grenzen bei Eingriffen zur Folge hat. Die Rechtsprechung gesteht **keine absolute Vertraulichkeit** zu; zur Rechtfertigung von Eingriffen wird jedoch der Schutz hochrangiger Güter verlangt.[440]

Beim Schutz beruflich begründeter Vertraulichkeit wird nicht nur auf das Recht auf Datenschutz bzw. auf das allgemeine Persönlichkeitsrecht zurückgegriffen, sondern zudem auf weitere Verfassungsprinzipien.[441] Er findet in Art. 339 AEUV eine normative Konkretisierung für EU-Institutionen. Er geht im Gesundheitsbereich auf den Eid des Hippokrates (von 460 bis 370 vor Christus) zurück, der weiterhin Aktualität hat.[442] Der Schutz des Patientengeheimnisses (ärztliche Schweigepflicht) hat neben dem Datenschutz seine Grundlage im Schutz der Unversehrtheit (Art. 2 Abs. 2 S. 1 GG, Art. 3 GRCh), dem Schutz der Berufsausübung des medizinischen Helfers (Art. 12 GG, Art. 15 GRCh)[443] sowie im Sozialstaatsprinzip (Art. 20 GG bzw. Art. 34, 35 GRCh).[444] Er beruht auf der Erwägung, dass eine Hilfe suchende Person sich einem potenziellen Helfenden nur umfassend anvertrauen wird, wenn sich hieraus keine nachteiligen Folgen ergeben können. Das umfassende Anvertrauen ist für den Helfenden nötig, um adäquat – individuell, kompetent, situationsbezogen und ausreichend – Hilfe leisten zu können. Dies gilt insbesondere, wenn die Hilfe dem Schutz der Unversehrtheit dient und eine staatliche Schutzpflicht besteht, wie dies im Hinblick auf die Gesundheit gegenüber der Allgemeinheit der Fall ist (s. o. 6.1).

Ein zentrales **Begründungsmuster** für den gesteigerten verfassungsrechtlichen Schutz von Berufsgeheimnissen ist der besondere Eingriff ins allgemeine Persönlichkeitsrecht bzw. in das Recht auf informationelle Selbstbestimmung.[445] Bei einem Seelsorger hat das BVerfG sogar auf den Schutz der „Kernbereichs privater Lebensgestaltung“ zurückgegriffen.[446] Das

---

439 EuGH 8.4.2014 – C-293/12 u. C-594/12 Rn. 58, NJW 2014, 712; Hatje in Schwarze Art. 6 EUV Rn. 3.

440 BVerfG 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09 Rn. 131-133, NJW 2016, 1788; MVVerfG 18.5.2000 – LVerfG 5/98, NVwZ 2000, 1038; SächsVerfGH 14.5.1996 – Vf. 44-II/94, NJW 1996, 1954 = DuD 1996, 496 f.

441 Zur anwaltlichen Schweigepflicht BVerfG 12.4.2005 – 2 BvR 1027/02, NJW 2005, 1919; BVerfG 20.4.2016 – 1 BvR 966/09 u. 1 BvR 1140/09, Rn. 257, DVBl 2016, 779.

442 Weichert in Langkafel S. 162 = DuD 2014, 831.

443 Ruffert in Callies/Ruffert, Art. 15 GRCh Rn. 24 “Vertrauensschutz”.

444 Bernsdorff in Meyer Art. 15 Rn. 12; vgl. Hatje in Schwarze Art. 339 Rn. 6; Wegener in Callies/Ruffert, Art. 339 AEUV Rn. 2; zum Vertraulichkeitsschutz des Sozialarbeiters BVerfG 19.7.1972 – 2 BvL 7/71, NJW 172, 2214.

445 BVerfG 23.10.2006 – 1 BvR 2017/02, MMR 2007, 93 f. = DuD 2006, 818 f.

446 BVerfG 25.1.2007 – 2 BvR 26/07.

BVerfG hat in Bezug auf die berufliche Tätigkeit eines Anwalts dargelegt, dass das Mandatsverhältnis nicht mit Unsicherheiten hinsichtlich seiner Vertraulichkeit belastet sein darf. Dies leitet es zwar nicht ausschließlich, aber auch aus der Schutzwirkung der Berufsfreiheit des Art. 12 GG ab. So begründet es ein Abwehrrecht gegenüber hoheitlichen Akten, insbesondere wenn es sich, wie beim Anwalt, um ein „Organ der Rechtspflege" handelt. Dies wird dann nicht nur mit den Unsicherheiten über die Vertraulichkeit zum Berufsgeheimnisträger begründet, sondern auch mit den sich daraus ergebenden beschränkenden Auswirkungen auf die wirtschaftliche Entfaltung.[447] Wird das Vertrauensverhältnis im Rahmen der Telekommunikation beeinträchtigt, so wird Art. 10 GG herangezogen.[448] Hinsichtlich des Vertrauensverhältnisses zu einem Journalisten greift das BVerfG auf die Pressefreiheit nach Art. 5 GG zurück.[449]

6.9 Meinungsfreiheit

Gemäß Art. 5 Abs. 1 S. 1 GG hat jeder „das Recht, seine Meinung in Wort, Schrift und Bild frei zu äußern und zu verbreiten". Das Grundrecht auf Meinungsfreiheit wird ebenso in Art. 11 Abs. 1 GRCh garantiert. Der plurale öffentliche Diskurs ist eine zentrale Grundlage demokratischer Gesellschaften. Das Recht auf Meinungsfreiheit hat mehrere Bezüge zum Gesundheitswesen und zu Big Data. Geschützt werden auch im Internet geäußerte Meinungen, etwa in Blogs, Chatrooms, Online-Portalen oder Bewertungsplattformen[450], die sich auf den Gesundheitszustand von Betroffenen oder auf Gesundheitsdienstleistungen beziehen. Eine relevante Anwendungsform sind Bewertungsportale zu Ärzten, Krankenhäusern oder sonstigen medizinischen Leistungserbringern. Hierüber wird Patienten die Möglichkeit gegeben, einen für sie geeigneten medizinischen Dienst auszuwählen. Durch solche Bewertungen wird zugleich in die berufliche Sphäre der Leistungserbringer gemäß Art. 12 GG und Art. 15 GRCh eingegriffen (s. u. 6.17). Bewertungsportale genießen selbst dann den Schutz der Meinungsfreiheit, wenn sie über anonyme Meldungen beschickt werden. Der darüber hinausgehende Schutz und die besondere Privilegierung für die Presse sind dagegen nicht anwendbar.[451] Der freie Diskurs bezieht sich nicht nur auf die Auswahl medizinischer Dienstleister, sondern hat Bedeutung für sämtliche individuellen und politischen Äußerungen und für dadurch ermöglichte Entscheidungen im Gesundheitsbereich.

---

447 BVerfG 12.4.2005 – 2 BvR 1027/02, NJW 2005, 1919.

448 BVerfG 30.4.2007 – 2 BvR 2151/06, NJW 2007, 2752 f.

449 BVerfG 10.12.2010 – 1 BvR 2020/04, NJW 2011, 1863 f.; BVerfG 27.2.2007 – 1 BvR 538/06 u. a., NJW 2007, 1118.

450 Hoffmann u. a., S. 130 f.

451 BGH 23.9.2014 – VI ZR 358/13, NJW 2015, 489 = AfP 2014, 529 = CR 2015, 116 (Ärztebewertungsportal II), BGH 23.6.2009 – VI ZR 196/08, NJW 2009, 2890; OLG Frankfurt, DuD 2012, 8 = ZD 2012, 274 = RDV 2012, 200; LG Kiel, RDV 2014, 217 = ZD 2014, 323 (LS); LG Kiel, ZD 2015, 278; Arbeitskreis Gesundheit und Soziales der DSB-Konferenz, Leitlinien mit Mindestanforderungen für die Ausgestaltung und den Betrieb von Arztbewertungsportalen im Internet vom 14.3.2013, http://www.datenschutz-berlin.de/attachments/934/Leitlinien_Arztbewertung_final.pdf?1363609731; Kühling NJW 2015, 447; Meyer, K&R 2014, 807; Wilkat, Bewertungsportale im Internet, 2013. Hoffmann u. a. S. 131 ff.

Meinung i. S. d. **freien Meinungsäußerung** umfasst jede Ansicht, Überzeugung, Einschätzung, Stellungnahme und jedes Werturteil ohne Rücksicht auf die Qualität und das Thema.[452] Erfasst wird damit auch der „Laienjournalismus" mit seiner populären Ausgestaltung des Veröffentlichens personenbezogener Daten im Internet (Blogging, private Webseiten).

Meinungsäußerung generell wie auch deren Konkretisierung in Form der Pressearbeit und der Forschung, erfolgt in Form von **Tatsachendarstellungen und Bewertungen** sowie in einer Kombination von beidem. Je weniger eine Veröffentlichung mit der Verbreitung von Meinungen zu tun hat und je stärker sie sich im Bereich streng fachlich gebundener Faktenvermittlung bewegt, umso geringer ist die Erforderlichkeit, zum Schutz der Meinungsfreiheit andere Grundrechte wie z. B. die Datenschutzrechte von Betroffenen zu beschränken. Nicht von der Meinungsfreiheit erfasst werden digitale Hetze, Mobbing sowie Aktivitäten, die geeignet sind, den Ruf und die Unversehrtheit von Menschen zu gefährden (Art. 5 Abs. 2 dGRCh-E). Ebenso wenig geschützt ist die bewusste Verbreitung von falschen Tatsachen (sog. Fake-News).[453]

Entgegen einer teilweise vertretenen Ansicht können Scores, also von Computern berechnete Bewertungen, das **Recht auf Meinungsfreiheit** (Art. 5 GG) nicht für sich in Anspruch nehmen. Dieses Recht steht nur natürlichen Personen zu. Für das Scoring durchführende Unternehmen kommen lediglich die Art. 2 und 14 GG zur Anwendung.[454] Etwas anderes gilt für die Verbreitung von personalen Meinungsäußerungen mit Hilfe von sog. Social Bots, wobei jedoch Dritt- und Persönlichkeitsrechte einer derartigen Meinungsverbreitung klare Grenzen setzen.[455]

Die u. a. in Art. 5 GG garantierten **Kommunikationsgrundrechte** finden ihre Grundlage auch in völkerrechtlichen Verpflichtungen, insbesondere in Art. 10 EMRK und der Auslegung durch den EGMR[456] und Art. 19 AEMR sowie Art. 19 IPbürgR, die Meinungs-, Presse- und Informationsfreiheit garantieren.[457] Die Herstellung praktischer Konkordanz insbesondere zwischen Datenschutz und Kommunikationsfreiheiten[458] ist eine dauernde Herausforderung angesichts der technischen Fortentwicklung der Informations- und Kommunikationsmedien, mit denen personenbezogene Daten in einer Weise verarbeitet werden können, dass eine massive Verletzung des allgemeinen Persönlichkeitsrechts von

---

452 Jarass, Charta der Grundrechte der EU, 2013, Art. 11 Rn. 7.

453 Deutscher Bundestag, Wissenschaftliche Dienste, Fake-News – Definition und Rechtslage, 17.2.2017, WD 10-3000-03/17, S. 8.

454 Weichert, ZRP 2014, 169; ULD/GP Forschungsgruppe S. 52 ff.; a. A. BGH 28.1.2014 – VI ZR 156/13, NJW 2014, 1235 = K&R 2014, 269 i. V. m. BGH 22.2.2011 – VI ZR 120/11, NJW 2011, 2204; OLG München, ZD 2014, 570; LG Berlin, ZD 2014, 369.

455 Steinbach ZRP 2017, 102 f., 105; Golz, Beilage 1 zu K&R Heft 7/8/2017, 30 f.

456 Albrecht/Janson CR 2016, 507 f.

457 Buchner/Tinnefeld in Kühling/Buchner Art. 85 Rn. 9 f.

458 Albrecht/Janson CR 2016, 502; Caspar NVwZ 2010, 1456.

Betroffenen ermöglicht wird.[459] Dabei wird dem EuGH eine eher datenschutzfreundliche, dem EGMR eine eher meinungsfreundliche Grundhaltung zugesprochen.[460]

6.10 Informationsfreiheit

Art. 5 Abs. 1 S. 1 GG garantiert auch das Recht, „sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten". Dem entspricht Art. 11 Abs. 1 S. 2 GRCh, wobei auf europäischer Ebene die Bezugnahme auf allgemein zugängliche Quellen fehlt. Demgemäß verfolgt die Rechtsprechung des BVerfG eine eher restriktive Auffassung und begründet keine Pflicht zur Generierung und Bereitstellung von Informationen, z. B. per Big Data oder über das Internet.[461] Inwieweit Informationsfreiheit Informationsansprüche begründet, ist bisher weder nach deutschem noch europäischem Verfassungsrecht eindeutig geklärt.[462]

Es setzt sich aber immer die Einsicht durch, dass in einer Informationsgesellschaft Informationszugänge zentrale grundrechtliche Funktionen erfüllen. Dies gilt zunächst für Informationen, die über eine Person bei anderen Stellen verarbeitet werden. Dieser Aspekt wird durch das Recht auf informationelle Selbstbestimmung (s. o. 6.5) und den daraus abgeleiteten Auskunftsanspruch (s. u. 8.17) abgedeckt. Der Anspruch auf Informiertheit lässt sich hierauf aber nicht beschränken und muss im Sinne der Informationsfreiheit das bei staatlichen Stellen vorhandene Wissen miteinbeziehen[463], ja selbst bei öffentlicher Relevanz das Wissen, das von Privaten vorgehalten wird (vgl. Art. 9 dGRCh-E). Letztlich stellt sich die Frage, inwieweit darüber hinausgehend eine Teilhabeanspruch am digitalen Leben begründet werden muss (so Art. 3 dGRCh-E).

6.11 Pressefreiheit

Gemäß Art. 5 Abs. 1 S. 2, 3 GG ist die Pressefreiheit und die Freiheit der Berichterstattung durch Rundfunk und Film gewährleistet. Zensur ist verboten. Entsprechend sichert Art. 11 Abs. 2 GRCh die Achtung der Freiheit und der Pluralität der Medien. Die Aufgabe der Presse ist es, Informationen zu recherchieren, bestehende bzw. geäußerte Meinungen wiederzugeben und den Konsumenten das Bilden einer eigenen Meinung zu ermöglichen.[464] Die Medienfreiheit ist konstituierend für die freiheitliche demokratische Grundordnung.[465] Meinungs- und Angebotspluralität ist nötig, um eine Konkurrenz in Bezug auf Tendenz, politische Färbung und weltanschauliche Grundhaltung zu erhalten.[466] Der Begriff der Presse ist grds. weit und entwicklungsoffen zu verstehen und schließt, wie die europäische Regelung erkennen lässt, digitale und online angebotene Medien mit ein.[467]

---

459 Grundlegend dazu Klar DÖV 2013, 103 f; siehe schon Warren/Brandeis DuD 2012, 755 ff.
460 Von Lewinski in Auernhammer Art. 85 Rn. 4 f.
461 BVerfG 20.6.2017 – 1 BvR 1978/13, EuRGZ 2017, 477 f.; Hoffmann u. a. S. 139.
462 Weichert in Erichsen, Hans-Uwe/Schäferbarthold, Dieter/Staschen, Heiner/Zöllner, Jürgen E. (Hrsg.) Lebensraum Hochschule - Festschrift für Albert von Mutius, 2012, S. 79.
463 Wegener, Der geheime Staat, 2006.
464 Hoffmann u. a. S. 139 f.
465 BVerfG 10.12.2010 – 1 BvR 2020/04 Rn. 23, NJW 2011, 1863.
466 BVerfG 28.2.1961 – 2 BvG 1/60 u. 1 BvG 2/60, NJW 1961, 548.
467 Hoffmann u. a. S. 140 ff.

Von der Pressefreiheit erfasst wird die **publizistische Tätigkeit** von Medienunternehmen der Presse, des Rundfunks einschließlich des Fernsehens (Television) und des Films, auch die Aktivität von einzelnen Journalisten. Die Veröffentlichung muss für einen unbestimmten Personenkreis bestimmt sein. Der Umstand, dass Informationen möglicherweise unzulässig erlangt oder weitergegeben wurden, ist im Interesse des Quellenschutzes allein kein Grund, die journalistische Privilegierung aufzuheben. Journalismus setzt professionelles Vorgehen voraus, zu dem eine qualifizierte Recherche gehört. Die Verbreitung von „Fake-News", also von falschen oder sinnentstellenden Texten, Ton- und Bildnachrichten ist nicht geschützt (s. o. 6.9). Die Wahrheitspflicht dient sowohl dem Ehr- und Persönlichkeitsschutz der Betroffenen wie auch der demokratischen öffentlichen Meinungsbildung.

Von der Pressefreiheit erfasst sind nicht nur die Publikationen selbst, sondern auch das **Sammeln der Information** zum Zweck der Publikation, der Schutz des Zugangs zu Informationsquellen sowie der Austausch im Rahmen der Kooperation von Medienunternehmen und Journalisten. Geschützt ist auch die **Aufbereitung** zum Zweck der Berichterstattung. Erfasst sind weiterhin nicht nur die erstmalige Veröffentlichung, sondern auch deren Reproduktion und Archivierung sowie die Bereitstellung von veröffentlichten und unveröffentlichten Informationen in darauf spezialisierten Medienarchiven.[468] Die Beschaffung von Gesundheitsdaten sowie deren Zusammenführung und Analyse mit Big-Data-Instrumenten sind damit eingeschlossen, wenn der Zweck ausschließlich in der publizistischen Nutzung liegt. Erfolgte die Big-Data-Analyse im Vorfeld der späteren journalistischen Nutzung, so wird lediglich die journalistische Beschaffung der Analyseergebnisse durch die Pressefreiheit besonders geschützt.

6.12 Forschungsfreiheit

Art. 5 Abs. 3 GG erklärt Wissenschaft, Forschung und Lehre als frei und verpflichtet zur „Treue zur Verfassung". Art. 13 GRCh privilegiert ebenso Forschung und akademische Freiheit. Grundrechtlich privilegierte Forschung ist ein auf **wissenschaftlicher Eigengesetzlichkeit** (Methodik, Systematik, Beweisbedürftigkeit, Nachprüfbarkeit, Kritikoffenheit, Revisionsbereitschaft) beruhender Prozess zum Auffinden von Erkenntnissen, ihrer Deutung und ihrer Weitergabe. Wissenschaftliche Forschung ist „alles, was nach Inhalt und Form als ernsthafter, planmäßiger Versuch zur Ermittlung der Wahrheit anzusehen ist".[469] Forschung ist nicht dadurch ausgeschlossen, dass das Vorhaben auch Ausbildungs- und Prüfungszwecken dient.[470] Liegen die Voraussetzungen für eine grundrechtlich privilegierte Forschung vor, so ist dies im Rahmen der

468 Caspar NVwZ 2010, 1454.

469 BVerfGE 35, 112 f. = NJW 1978, 1176; Johannes/Richter DuD 2017, 300; zur Erfordernis der Staatsferne Weichert, Informationelle Selbstbestimmung und strafrechtliche Ermittlung, 1990, 231 f.

470 Hoffmann u. a. S. 152.

Normauslegung und -anwendung zu beachten, unabhängig davon, ob der Schutz der Wissenschaftsfreiheit als Gesetzeszweck benannt ist oder nicht.[471]

Das Forschungsprivileg gilt nur für unabhängige Forschung. Der Begriff der Forschung ist jedoch weit auszulegen und schließt private Forschung mit ein.[472] Eine externe Einflussnahme auf den wissenschaftlichen Erkenntnisprozess oder eine Unterordnung unter wirtschaftliche oder sonstige Interessen muss ausgeschlossen sein. Die Finanzierung durch Drittmittel muss nicht, kann aber die Unabhängigkeit beeinträchtigen.[473] Die Unabhängigkeit der Forschung ist nicht allein deshalb beeinträchtigt, weil die Finanzierung des Forschungsvorhabens von einer dritten Stelle erfolgt, die selbst ein Interesse an den (unabhängig erlangten) Erkenntnissen hat. Wissenschaftliche Untersuchungen, die zu Organisations-, Aufsichts- und Kontrollzwecken vorgenommen werden, verfolgen vorrangig keine wissenschaftliche Zielsetzung mehr. Auf die Entwicklung neuer Produkte ausgerichtete Forschung (z. B. der Pharmaindustrie) und rein kommerzielle Markt- und Meinungsforschung (z. B. zum Vertrieb von Gesundheitsleistungen) kommen auch nicht in den Genuss der grundrechtlich begründeten Privilegierung.[474] Etwas anderes gilt, wenn die pharmakologische oder die Markt- und Meinungsforschung die Anforderungen wissenschaftlicher unabhängiger Forschung erfüllen.[475]

Entscheidend für die Annahme der Wissenschaftlichkeit ist im Hinblick auf eine personenbezogene Datenverarbeitung, dass diese streng zweckgebunden erfolgt. Es muss ein wissenschaftliches Erkenntnisinteresse verfolgt werden, wobei dieses sich nicht auf ein eng definiertes Forschungsprojekt beschränken muss. Unter definierten Voraussetzungen können Daten zwischen Projekten, in Forschungsverbünden, wissenschaftlichen Netzwerken und Registern ausgetauscht werden.

Erfasst werden alle „Prozesse, Verhaltensweisen und Entscheidungen“ im Rahmen der Forschungstätigkeit.[476] Dies schließt die Vorbereitung und Planung, die Datenbeschaffung und Auswertung sowie letztlich die Veröffentlichung der Ergebnisse mit ein. Gegenstand forschender Datenverarbeitung können alle Formen von Daten sein, insbesondere Gesundheitsdaten, an deren Auswertung ein großes öffentliches Interesse bestehen kann.[477] Im Rahmen von Big-Data-Forschung findet oft die Nutzung von Daten aus dem Internet statt.[478]

---

471 So wird z. B. im GenDG dieser Zweck nicht explizit genannt, kritisch hierzu Ladeur DuD 2016, 360.

472 ErwGr 159 S. 1 DSGVO.

473 Gola/Schomerus § 40 Rn. 8; Mester in Taeger/Gabel § 40 Rn. 6; kritischer Simitis in Simitis § 40 Rn. 36.

474 Simon/Vesting, CR 1992, 307; Simitis in Simitis § 40 Rn. 43; ähnlich Gola/Schomerus § 40 Rn. 8 f.; Plath/Frey in Plath § 40 Rn. 4, 5, Grages in Plath Art. 89 Rn. 6; Greve in Auernhammer Art. 89 Rn. 4.

475 Hornung/Hofmann ZD-Beilage 4/2017, 5.

476 BVerfG 28.10.2008 – 1 BvR 462/06, BVerfGE 122, 105; BVerfG 26.10.2004 – 1 BvR 911/00 u. a., BVerfGE 111, 354; BVerfG 1.3.1978 – 1 BvR 333/75 u. a., BVerfGE 47, 367.

477 ErwGr 53, 156, 157, 159 DSGVO; Schütze DANA 2017, 191.

478 Hoffmann u. a. S. 152 ff.

6.13 Gleichheitsschutz

Art. 3 Abs. 1 und 2 GG postuliert, dass alle Menschen, insbesondere Männer und Frauen, vor dem Gesetz gleich sind. Dies wird von den Art. 20 und 23 GRCh bestätigt. Der Gleichheitsgrundsatz gilt auch für digitale Sachverhalte, so z. B. im Rahmen der Bereitstellung von Ressourcen zur Gewährleistung des Existenzminimums, beim Zugang zu medizinischen Dienstleistungen oder zu Informationsdiensten im Gesundheitsbereich. Im Rahmen der staatlichen Schutzpflicht können Maßnahmen gefordert sein, die private Anbieter auf die Gleichbehandlung verpflichten.[479] Ungleichbehandlungen im Gesundheitsbereich auf der Grundlage von Big Data sind in vielen Bereichen denkbar. Dies gilt etwa für den Versicherungsschutz durch die direkte oder indirekte Ungleichbehandlung von Männern und Frauen.[480] Aus der Zielsetzung der Gleichbehandlung kann sich für den Staat die Pflicht ergeben, monopolistische Strukturen von Anbietern auf dem (Gesundheits-) Markt zu verhindern.[481]

Der Gleichheitsgrundsatz dient der Verwirklichung von Gerechtigkeit in der Gesellschaft. Gerechtigkeit bedeutet zum einen gleiche Zuteilung von Ressourcen, kann aber auch darauf hinauslaufen, ungleich verteilte Ressourcen auszugleichen. Der Ausgleich wird staatlicherseits über das Sozialstaatsprinzip, generell über das Solidarprinzip verwirklicht (s. u. 6.15). Big Data kann für eine gerechte Ressourcenverteilung als Hilfsmittel zum Einsatz kommen.[482]

Zum Gleichheitsschutz gehört im Kontext von Big Data, inwieweit – für die Öffentlichkeit allgemein bzw. Forschende speziell – gleicher Zugang zu relevanten Datenbeständen besteht bzw. gewährt wird. Hinsichtlich öffentlicher Daten besteht insofern evtl. Anspruch über das Informationsfreiheitsrecht des Bundes sowie der meisten Bundesländer. Der Zugang zu privaten Daten ist bisher weitgehend der Entscheidung der Verfügungsberechtigten überlassen. Gegen Zugangsansprüche zu (gesundheitsrelevanten) Daten können geistiges Eigentum, Betriebs- und Geschäftsgeheimnisse sowie Datenschutzrechte vorgebracht werden (vgl. z. B. §§ 3 ff. IFG-Bund).[483]

Eine Frage der Gleichheit, der Gerechtigkeit sowie des Sozialstaatsgrundsatzes ist es, inwieweit Ansprüche auf bestimmte gesundheitsrelevante Angebote, die auf Big Data zurückgehen, begründet werden. Es ist vorstellbar, dass z. B. aus Gründen der Gesundheitsvorsorge allgemein oder bestimmten Gruppen ausdrückliche Rechte zugewiesen werden müssen.[484]

---

479 Hoffmann u. a. S. 117.
480 EuGH 1.3.2011 – C-236/09, NJW 2011, 907 = VersR 2011, 377 = DB 2011, 821 = DÖV 2011, 364.
481 Hoffmann u. a. S. 117 ff.
482 Deutscher Ethikrat S. 145 ff.
483 Deutscher Ethikrat S. 147 f.
484 Deutscher Ethikrat S. 148 f.

6.14 Diskriminierungsverbote

Sowohl das nationale wie auch das europäische Verfassungsrecht enthält **spezifische Diskriminierungsverbote**: Art. 3 Abs. 3 GG verbietet die Benachteiligung oder Bevorzugung „wegen seines Geschlechts, seiner Abstammung, seiner Rasse, seiner Sprache, seiner Heimat und Herkunft, seines Glaubens, seiner religiösen oder politischen Anschauungen". Art. 21 GRCh konkretisiert und erweitert dies durch zusätzliche Benennung folgender, die Diskriminierung verbietender Merkmale: Hautfarbe, ethnische oder soziale Herkunft, genetische Merkmale, Weltanschauung, Zugehörigkeit zu einer nationalen Minderheit, Vermögen, Geburt, Behinderung, Alter und sexuelle Ausrichtung (s. o. 5.4).

Diese spezifischen Diskriminierungsverbote haben im Hinblick auf Big Data eine zweifache Relevanz: einerseits verbieten sie grundsätzlich die **Nutzung der genannten Merkmale**, von denen einige einen Gesundheitsbezug haben (insbesondere genetische Merkmale, Behinderung, sexuelle Ausrichtung) als in Big-Data-Auswertungen einfließende Bewertungsmerkmale, soweit damit eine nicht gerechtfertigte Wirkung (Bevorzugung wie Benachteiligung) gegenüber den Betroffenen verbunden ist. D. h. rein erkenntnissuchende Analysen werden durch die Diskriminierungsverbote nicht untersagt. Zu beachten ist aber, dass die Grenzen zwischen Erkenntnis und daraus resultierender Diskriminierung abstrakt nicht eindeutig bestimmbar sind. Eine Einzelfallbewertung ist nötig. Auch schwer bestimmbar sind die Grenzen zwischen legitimer Differenzierung und unzulässiger Diskriminierung. Besteht eine Diskriminierungsabsicht, so ist diese in jedem Fall verboten. Besteht aber ein begründeter Sachzusammenhang, so kann sich hieraus eine Rechtfertigung ergeben. Dies gilt insbesondere, wenn die Differenzierung eine rechtliche Grundlage hat.[485]

Das **Allgemeine Gleichbehandlungsgesetz** (AGG) konkretisiert die verfassungsrechtlichen Vorgaben der Diskriminierungsverbote. Das AGG ist z. B. im Rahmen der Merkmalsverwendung bei Scoring-Verfahren zu beachten.[486] Konkretisierungen können sich auch aus anderen Gesetzen ergeben. So darf z. B. die Wahrnehmung von gesetzlich gewährleisteten Rechten, etwa von Datenschutzrechten, zu keiner Benachteiligung führen.[487]

Eine verfassungsrechtlich verbotene Diskriminierung kann sich auch daraus ergeben, dass nicht die in die Big Data-Auswertung einfließenden, wohl aber die **Ergebnisse** eine nicht gerechtfertigte Differenzierung zur Folge haben. Ein äußerlich objektiver Algorithmus kann zu einer objektiven Benachteiligung wegen eines der genannten Diskriminierungsmerkmale führen. Derartige Wirkungen werden beispielsweise bei Internetauswertungen[488] wie auch bei genetischen Untersuchungen immer wieder dokumentiert.[489]

485 BVerfG 22.5.1975 – BvL 13/73, Rn. 93-96, BVerfGE 39, 368.
486 Weichert in Däubler u. a. § 28b Rn. 6; ULD (2005) S. 77; a. A. Kamlah in Plath § 28b BDSG Rn. 27.
487 Weichert in Däubler u. a. § 28b Rn. 6.
488 Zu Autocomplete s. o. 5.4.
489 Zur genetischen Forensik vgl. Weichert, Vorgänge Nr. 218 (2/2017), S. 129 ff.

Vom derzeit bestehenden Recht, auch vom Datenschutzrecht nicht adressiert wird die Fragestellung von merkmalsbezogenen Gruppendiskriminierungen, die sich auf Gruppenzugehörige individuell auswirken können.[490] Als Beispiel kann die Auswertung von Gesundheitsdaten durch Krankenversicherungen benannt werden: Versicherungen können anhand anonymisierter Behandlungs- und Kostendaten ihrer Mitglieder feststellen, welche Personen mit welchen Merkmalen besonders kostenträchtig sind. Die erlangten unstreitig anonymen Auswertungsdaten können zur Grundlage dafür genommen werden, Personen als Beitragszahler besonders zu werben bzw. zu binden bzw. kostenträchtige Mitglieder aus einer Versicherung hinauszudrängen bzw. diese nicht aufzunehmen. Dies bedeutet, dass selbst die anonymisierte Auswertung ursprünglich personenbezogener Daten für Personen, die bestimmte auswertungsrelevante Merkmale aufweisen, äußerst nachteilig wirken kann.

Was aus unternehmerischer Sicht wünschenswert erscheinen mag, kann nicht nur aus individueller Sicht, sondern auch aus demokratischer und freiheitlicher Sicht unerwünscht sein: Normabweichendes Verhalten ist für eine freiheitliche demokratische Gesellschaft insbesondere im Hinblick auf politische Betätigung, aber auch für eine freie Marktwirtschaft im Hinblick auf Konsumverhalten konstituierend. Die Definition, welches normabweichende Verhalten bzw. welche normabweichenden Merkmale gesellschaftlich erwünscht sind, kann nicht einem Unternehmen und dessen kommerziellen Erwägungen überlassen werden, sondern bedarf einer transparenten und demokratischen Festlegung (s. u. 10.5.4).

Das Beispiel zur Kollektivdiskriminierung weist darauf hin, dass Diskriminierung heute nicht mehr nur anhand von anerkannten Diskriminierungsmerkmalen (Alter, Geschlecht, Religion, Ethnie…) erfolgt, sondern auch über einen komplexen Merkmalsmix definiert werden kann. Diese Form der Diskriminierung basiert regelmäßig auf dem Umstand, dass die Algorithmen von Big-Data-Analysen keine Kausalitäten feststellen, sondern lediglich mathematisch-statistische Korrelationen (s. o. 5). Dies führt zwangsläufig dazu, dass von Algorithmen-Entscheidungen Menschen betroffen sind, die keinerlei Grundlage oder Auslöser für diese Entscheidung gegeben haben.

6.15 Sozialstaatsprinzip inkl. Solidaritätsgrundsatz

Gemäß Art. 20 Abs. 1 GG ist die Bundesrepublik ein sozialer Staat. Diese Sozialstaatsklausel begründet eine Schutzpflicht gegenüber wirtschaftlich, sozial, gesundheitlich Schwachen bzw. Gefährdeten. Ziel des Sozialstaatsgrundsatzes ist die Bewältigung sozialer Notlagen und Beeinträchtigungen, wie sie durch Krankheit, Invalidität, Arbeitslosigkeit oder sonstige benachteiligende Lebensumstände herbeigeführt werden. Dieses Prinzip wird in Art. 35 GRCh konkretisiert als „Recht auf Zugang zur Gesundheitsvorsorge und auf ärztliche Versorgung“ sowie in Art. 34 GRCh als „Recht auf Zugang zu den Leistungen der sozialen Sicherheit und zu den sozialen Diensten“. Als Anlässe für diesen Sorgeanspruch werden „Mutterschaft, Krankheit, Arbeitsunfall,

490 Deutscher Ethikrat S. 21.

Pflegebedürftigkeit oder im Alter sowie bei Verlust des Arbeitsplatzes“ genannt. In Gesundheitsangelegenheiten besteht generell eine staatliche Fürsorgepflicht.[491]

Der Begriff der Solidarität bezeichnet soziales Handeln und dem dienliche institutionelle, politische und vertragliche Regelungen, die das Ziel haben, sich gegenseitig und damit auch andere zu unterstützen. Solidarität gründet in Reziprozitätserwartungen. Gesamtgesellschaftlich zielt sie aber auf Gerechtigkeit, nicht nur durch Vermeidung von Diskriminierungen, sondern durch Teilhabe am gesellschaftlichen Leben und an den gemeinschaftlich erwirtschafteten Gütern.[492]

Aus dem Sozialstaatsprinzip kann zunächst der Anspruch auf adäquate soziale Versorgung abgeleitet werden. Diese Versorgung hat ihre gesetzliche Konkretisierung in den Sozialgesetzbüchern gefunden. Für den Gesundheitsbereich besonders relevant sind die Krankenversicherung (SGB V), der Schutz vor Unfällen und vor Unfallfolgen (SGB VII), die Rehabilitation und Teilhabe von behinderten Menschen (SGB IX) sowie die Sicherstellung einer angemessenen Pflege (SGB XI).

Zur sozialen Versorgung gehört auch die Zusicherung der Vertraulichkeit bei sozialen Leistungen (s. o. 6.8). Der dahinter stehende Grundgedanke ist, sich als aus sozialen, gesundheitlichen, ökonomischen, rechtlichen oder familiären Gründen Hilfsbedürftiger vertrauensvoll und umfassend an einen potentiellen Helfenden wenden zu können, ohne die begründete Befürchtung zu haben, dass die dadurch erfolgende Mitteilung von Informationen für ihn nachteilige Folgen hat. Eine umfassende Information ist regelmäßig Voraussetzung für eine adäquate Hilfeleistung, wobei der Hilfsbedürftige oft nicht beurteilen kann, welche Informationen hierfür erforderlich ist, so dass er sich im Zweifel über das Nötige hinaus offenbaren können muss.

Staatliche Fürsorge kann auch in sozialen oder gesundheitsbezogenen informationellen Angeboten bestehen. Hierfür sind die Generierung von Erkenntnissen aus Gesundheitsdaten und deren öffentliche Bereitstellung erforderlich.[493]

Während gegenüber dem Staat über das Sozialstaatsprinzip direkt ein Anspruch auf bestimmte Lebensmindeststandards besteht, besteht ein solcher Anspruch gegenüber Privaten grundsätzlich nicht, kann aber gesetzlich begründet werden. Derartige Begründungen können sich aus familiärer Verbundenheit oder aus einem Arbeitsverhältnis ergeben. Im Kontext von Big Data im Gesundheitsbereich ist die private Krankenversicherung (PKV) von Relevanz. Es kann in Frage gestellt werden, inwieweit die Ausgliederung bestimmter Bevölkerungsteile aus der gesetzlichen Krankenversicherung

491 Weichert in Langkafel S. 163 f. = DuD 2014, 832.
492 Deutscher Ethikrat S. 23, 150 ff.
493 Weichert DuD 2014, 832.

durch Mitgliedschaft in der PKV und damit verbundene zusätzliche Pflichten bzw. Privilegien den Solidargrundsatz verletzt.[494]

Die Frage der Solidarität stellt sich, wenn, evtl. mit Hilfe von Big Data, im Gesundheitssystem aufgrund bestimmter Merkmale z. B. zu Lebensstil, genetischer Disposition oder Krankheiten bestimmte Personen von Leistungen bzw. Ansprüchen ausgeschlossen oder besonders belastet werden. Diese Frage hat durch die Einführung von Telematiktarifen bzw. -angeboten im Versicherungsbereich Aktualität gewonnen (s. u. 10.5.1).

Big Data im Gesundheitsbereich muss nicht zur Gefährdung, sondern kann auch zur Förderung des Solidargedankens beitragen. So kann der Austausch von Erfahrungen, von zu beforschenden Gewebeproben oder von spezifischen Daten zum Zweck einer gemeinschaftsförderlichen Auswertung solidaritätsstärkend sein.[495]

6.16 Grundrechte auf Eigentum

Art. 14 Abs. 1 GG und Art. 17 GRCh schützen das Eigentumsrecht. In Art. 17 Abs. 2 GRCh wird ausdrücklich auch das „geistige Eigentum" unter Schutz gestellt. Von diesem Schutz erfasst werden vermögenswerte Rechte, die vom Zivilrecht als Eigentum zugeordnet sind, so dass der Einzelne „die damit verbundenen Befugnisse nach eigenverantwortlicher Entscheidung zu seinem privaten Nutzen ausüben darf".[496] Darunter fallen neben dem sachenrechtlichen Eigentum i. S. v. § 903 BGB auch weitere dingliche Rechte sowie privatrechtliche Ansprüche und Forderungen. Dazu gehören Vermögenswerte des geistigen Eigentums und des Persönlichkeitsrechts. Immaterielles Eigentum wird durch das Marken- und das Urheberrecht begründet.[497]

In Art. 14 Abs. 2 GG heißt es: „Eigentum verpflichtet. Sein Gebrauch soll zugleich dem Wohl der Allgemeinheit dienen" (ähnlich Art. 17 Abs. 1 S. 3 GRCh). Diese Aussage gilt auch im Hinblick auf per Digitalisierung und Big Data generiertem Eigentum. Insofern ist in jedem Fall zu prüfen, inwieweit Big-Data-Verfahren und -Erkenntnissen eine nicht ökonomisch verstandene Gemeinwohlfunktion zukommt. Dies gilt insbesondere im Hinblick auf den Gesundheitsbereich mit seiner starken Gesellschaftsbezogenheit.[498] Diese Gemeinwohlfunktion kann darin gesehen werden, dass Daten (über Forschung) dem allgemeinen wissenschaftlichen Fortschritt dienen, dass sie zur Grundlage genommen werden für die „informationelle Selbstbestimmung" des Einzelnen über seine Umwelt und seine Gesundheit sowie zur Grundlage für die Mitbestimmung im demokratischen Meinungsbildungsprozess. Diese Aspekte der „Sozialpflichtigkeit von Daten" und des Freiheitsschutzes sind bei der Diskussion um Dateneigentum und um ein Datengesetz zu

494 Deutsche Ethikrat S. 152.
495 Deutscher Ethikrat S. 157 f.
496 BVerfG 31.3.1998 – 2 BvR 1877/97 u. 50/98, E 97, 371; BVerfG 7.12.2004 – 1 BvR 1804/03, E 112, 107; BVerfG 10.6.2009 – 1 BvR 706/08 u. a., E 123, 258.
497 Theißen S. 268 ff.
498 Siehe dazu ErwGr 35, 52 S. 53, 54, 112 S. 1, 159 S. 4-6 DSGVO.

berücksichtigen, in der bisher Fragen ökonomischer Macht und Wertigkeit im Vordergrund stehen (s. u. 9.3).

Der Eigentumsschutz ergänzt die Berufsfreiheit nach Art. 12 GG bzw. Art. 15 GRCh, die den eingerichteten und ausgeübten Gewerbebetrieb und damit auch Betriebs- und Geschäftsgeheimnisse schützt (s. u. 9.2). Bisher ist es durch die Rechtsprechung des Bundesgerichtshofes (BGH) anerkannt, dass sozial relevante Algorithmen als **Betriebs- und Geschäftsgeheimnisse** zumindest gegenüber den Betroffenen nicht offenlegungs- d. h. auskunftspflichtig sind.[499] Auch für eine staatliche Aufsicht können sich hier praktische oder rechtliche Kontrollprobleme und -konflikte ergeben. Es bedarf insofern der gesetzlichen Regulierung einer Offenlegungspflicht und einer rechtlichen Zuordnungspflicht in Bezug auf grundrechtlich relevante Algorithmen.[500]

6.17 Berufsfreiheit

Gemäß Art. 12 Abs. 1 GG haben alle Deutschen „das Recht, Beruf, Arbeitsplatz und Ausbildungsstätte frei zu wählen. Die Berufsausübung kann durch Gesetz oder auf Grund eines Gesetzes geregelt werden." Dieses Recht wird gemäß Art. 15 GRCh in Bezug auf die **Berufswahl** auf alle Unionsbürger ausgeweitet (Abs. 2), in Bezug auf die Berufsausübung auf alle Menschen. Zur Berufswahl gehört die Bewerbung für eine Berufsausübung, die zunehmend über digitale Medien, insbesondere das Internet erfolgt.[501] Geschützt sind auch die Wahl und die Ausübung von Berufen, die in Zusammenhang mit dem Einsatz von Informationstechnik stehen. Dies gilt für Provider, Betreiber von sozialen Netzwerken, Plattformen, Cloudangeboten, Online-Shops und viele mehr. Erfasst sind ebenso berufliche Tätigkeiten im Gesundheitsbereich und Tätigkeiten unter Einsatz von Big Data. Einschränkungen bei der beruflichen Nutzung von Big Data bedürfen einer gesetzlichen Grundlage, bedürfen einer gemeinwohlorientierten Rechtfertigung und müssen den Verhältnismäßigkeitsgrundsatz beachten. Dabei können in einem weiten Maße Gesichtspunkte der Zweckmäßigkeit berücksichtigt werden.[502]

Art. 16 GRCh erkennt zudem die **unternehmerische Freiheit** gemäß dem gesetzten Recht und den Gepflogenheiten an.[503] Dieses Recht wird im nationalen Verfassungsrecht aus den Art. 12 und 14 GG abgeleitet.[504] Die unternehmerische Freiheit erfasst sämtliche wirtschaftliche Tätigkeiten einer natürlichen und juristischen Person.[505] Es bezieht sich auf die Freiheit der Ausübung der Wirtschafts- und Geschäftstätigkeit, die Vertragsfreiheit, die

499 BGH 28.01.2014 – VI 156/13, NJW 2014, 1235; dazu ausführlich ULDGP Forschungsgruppe S. 44 ff.; vgl. Deutscher Ethikrat S. 95.

500 Charta der Digitalen Grundrechte der Europäischen Union, https://digitalcharta.eu/.

501 Hoffmann u. a. S. 197.

502 BVerfG 18.2.1970 – 1 BvR 226/69, E 28, 31.

503 Schneider, Die unternehmerische Freiheit des Art. 16 der Charta der Grundrechte der Europäischen Union als Grenze des europäischen Arbeitnehmerschutzes, 2017.

504 Schwarze in Schwarze Art. 15 GRC Rn. 3; Bernsdorff in Meyer Art. 16 Rn. 2 mit Verweis auf die Verfassungen anderer EU-Mitgliedstaaten.

505 Ruffert in Callies/Ruffert Art. 16 Rn. 3; Schwarze in Schwarze Art. 16 Rn. 4.

Freiheit, zu werben und die Wettbewerbsfreiheit.[506] Eingeschlossen sind Marktzugang, Investitionen, die Ordnung der Geschäftstätigkeit, das Direktionsrecht des Arbeitgebers gegenüber dem Arbeitnehmer, unternehmerische Innovationen, die Einführung und der Betrieb von (Informations-) Technik im Betrieb.[507] Erfasst wird damit auch der unternehmerische Einsatz von Big Data im Gesundheitsbereich.

Von Bedeutung ist im Kontext von Big Data und Gesundheit insbesondere die Ausübungsfreiheit. Diese ist betroffen durch Werbemaßnahmen im Internet, die durch Suchmaschinen oder Bewertungsportale tangiert sein kann.[508]

6.18 Arbeits- und Verbraucherschutz

Gemäß Art. 31 Abs. 1 GRCh hat jede Arbeitnehmerin und jeder Arbeitnehmer „das Recht auf gesunde, sichere und würdige Arbeitsbedingungen (vgl. Art. 154, 156 AEUV). Damit wird nicht nur allgemein ein Kernbereich geschützt; vielmehr wird ein subjektives Recht der Genannten begründet.[509] Arbeitsbedingungen werden auch durch den Einsatz digitaler Techniken berührt, von denen Diskriminierungen, Belästigungen oder gar Gesundheitsbeeinträchtigungen ausgehen können.[510]

Gemäß Art. 38 GRCh stellen die Politiken der Union „ein hohes Verbraucherschutzniveau sicher“. Eine Konkretisierung enthält Art. 169 Abs. 1 AEUV, der auf den „Schutz der Gesundheit, der Sicherheit und der wirtschaftlichen Interessen der Verbraucher“ sowie auf die „Förderung ihres Rechtes auf Information, Erziehung und Bildung von Vereinigungen zur Wahrung ihrer Interessen“ verweist. Bei Art. 38 GRCh handelt es sich um eine Zielvorgabe, aus der sich Einrichtungsgarantien ableiten lassen sowie normative Möglichkeiten der Begrenzung ökonomischer Grundrechte anderer (s. o. 6.16, 6.17).[511]

6.19 Demokratieprinzip, Rechtsstaatlichkeit

Lawrence Lessig hat in seinem Aufsatz „Code ist Law“ aus dem Jahr 2000 darauf hingewiesen, dass mit zunehmender Digitalisierung rechnergestützte Vorgaben immer mehr die Regeln unseres gesellschaftlichen Zusammenlebens bestimmen und damit die Wahrnehmung unserer Freiheitsrechte einschränken, ohne dass hierüber bewusste politische, geschweige denn transparente und mehrheitlich getroffene Entscheidungen zugrunde liegen.[512] Das Ergebnis sind „unkontrollierbare“ und „unverantwortliche“ Entscheidungen mit evtl. hoher gesellschaftlicher oder andere Menschen betreffender Relevanz.

---

506 Schwarze in Schwarze Art. 16 GRC Rn. 3; Bernsdorff in Meyer Art. 16 Rn. 10a-14.

507 Enste/Eyerund, Unternehmerische Freiheit in Gefahr? 2015.

508 Hoffmann u. a. S. 196.

509 Rudolf in Meyer Art. 31 Rn. 12; Knecht in Schwarze Art. 31 Rn. 7.

510 Rudolf in Meyer Art. 31 Rn. 14 ff.

511 Krebber in Callies/Ruffert Art. 38 GRCh Rn. 5; Rudolf in Meyer Art. 38 Rn. 5; Berg in Schwarze Art. 38 Rn. 3, 4.

512 Lessig, Code is Law – On Liberty in Cyberspace, http://harvardmagazine.com/2000/01/code-is-law-html; dazu Buchner, MedR 2016, 660 f.

Damit verweist Lessig auf ein **Transparenz-, Kontroll- und Entscheidungsproblem**, das in besonderem Maße beim Einsatz von Big Data und sog. Künstlicher Intelligenz auftritt: Basiert eine automatisiert vorbereitete oder getroffene Entscheidung für eine hoheitliche oder eine wirtschaftliche Maßnahme nicht auf einer nachvollziehbaren „Wenn-dann-Datenauswertung", sondern auf einem digital generierten komplexen Algorithmus, so kann dies dazu führen, dass die Gründe für diese Entscheidung nicht mehr nachvollzogen und kontrolliert werden können. Selbstlernende Algorithmen lassen sich nicht mehr hinreichend protokollieren bzw. dokumentieren. Selbst im Fall einer nachvollziehbaren Protokollierung kann oft keine einem Menschen oder einer Institution zuordenbare (rechtliche) Verantwortlichkeit begründet werden. Die Verantwortlichkeit für die Programmierung Künstlicher Intelligenz begründet im bestehenden Rechtsregime nicht zwangsläufig die (rechtliche) Verantwortlichkeit für eine auf dieser Grundlage getroffene (rechtlich relevante) Entscheidung. Selbst für den Fall einer theoretisch begründbaren Haftung des Programmierers bleibt das praktische Problem bestehen, dass wegen der Arbeitsteilung bei einer komplexen Programmcode-Generierung eine Verantwortungszuordnung in der Praxis oft nicht möglich ist.

Diese Defizite wirken sich direkt auf die **gerichtliche Kontrolle** durch die Justiz (Art. 19 Abs. 4 GG, Art. 47 GRCh) sowie die **demokratische Kontrolle** durch Parlamente aus (Art. 20 Abs. 1, 2 GG). Richter wie Parlamentarier werden mit technisch geschaffenen Fakten konfrontiert, deren Wirkzusammenhänge von ihnen nicht nachvollzogen, geschweige denn verstanden werden können. Die generierten Fakten sind mit dem Nimbus der digitalen Objektivität und Wissenschaftlichkeit behaftet. Diese normative Kraft des Faktischen entsteht nicht naturwüchsig oder zufällig. Sie wird bestimmt durch diejenigen, in deren Interesse die Algorithmen entwickelt und eingesetzt werden, die dann mehr oder weniger freiwillig und unreflektiert von Verwaltung, Wirtschaft und Menschen genutzt werden. Ergebnis ist die Beeinträchtigung der in Art. 19, 20 GG gewährleisteten Prinzipien von Rechtsstaatlichkeit und Demokratie.

7 Normative Grundlagen allgemein

Die normativen Grundlagen von Big Data im Gesundheitsbereich blieben lange Zeit rudimentär und wurden bzw. werden immer noch oft durch Regelungen auf nationaler oder regionaler Ebene geprägt, die schwerpunktmäßig andere Lebenssachverhalte im Blick haben. Durch Harmonisierungsbestrebungen innerhalb der EU und dem Ziel, einen einheitlichen digitalen Binnenmarkt zu schaffen, verlagert sich der Regelungsschwerpunkt derzeit nach Europa. Darüber hinausgehende internationale Regulierungen haben bisher nur empfehlenden und keinen verbindlichen Charakter.

7.1 Internationales Recht

Am 4.12.1990 beschloss die Generalversammlung der **Vereinten Nationen** (United Nations – UN) „Richtlinien betreffend personenbezogene Daten in automatisierten Dateien". Darin wird die Regelung der Datenverarbeitung der Initiative der einzelnen Staaten überlassen, die sich an bestimmten Prinzipien (Rechtmäßigkeit, Treu und Glauben, Richtigkeit,

Zweckbestimmung, Einsichtnahme, Nichtdiskriminierung) halten soll.[513] Anlässlich der Enthüllungen über die Spionagetätigkeit von Geheimdiensten, insbesondere der US-amerikanischen NSA und des britischen GCHQ, stellte die UN-Vollversammlung 2014 fest, dass die Art. 12 der Allgemeinen Erklärung der Menschenrechte (AEMR) und Art. 17 des Internationalen Paktes für zivile und politische Rechte (IPbürgR), die den Schutz von Privatleben und Schriftverkehr zum Gegenstand haben, auch Schutz vor Überwachen, Abhören und Datensammeln gewähren.[514]

2011 beschlossen die UN „Leitprinzipien für Wirtschaft und Menschenrechte", in denen die Staaten und Wirtschaftsunternehmen zur Beachtung von 31 Prinzipien angehalten werden, die auf die Allgemeine Erklärung der Menschenrechte und insbesondere den Internationalen Pakt über bürgerliche und politische Rechte sowie auf den Internationalen Pakt über wirtschaftliche, soziale und kulturelle Rechte (Internationale Menschenrechtscharta) Bezug nehmen.[515] Die Leitlinien benennen selbst nicht explizit bestimmte Grundrechte, sondern verweisen auf staatliche (gerichtliche und außergerichtliche) wie unternehmensinterne Mechanismen zur Verwirklichung von Grundrechten in Wirtschaftsunternehmen.

Völkerrechtliche Festlegungen zum Umgang von Gesundheitsdaten bei Big Data gibt es bisher nicht. Die UNESCO hat mit ihrer Universellen Deklaration zum Schutz des menschlichen Genoms und der Menschenrechte vom 11.11.1997 das Spannungsverhältnis zwischen Menschenwürde und Gemeinschaftsgut menschlichem Genom beschrieben und erklärt, dass das menschliche Genom kein Gegenstand von Gewinnstreben und von Diskriminierung sein soll. Die Internationale Erklärung über menschliche Gendaten der UNESCO vom 16.10.2003 fordert die Vertraulichkeit von menschlichen Gen- und Genexpressionsdaten sowie Bioproben und lässt Eingriffe nur auf gesetzlicher Grundlage zu. Am 19.10.2005 nahm die UNESCO eine Allgemeine Erklärung über Bioethik und Menschenrechte an.[516]

In der weltweiten Diskussion über die ethischen Anforderungen an medizinische Daten- und Biomaterialbanken hat sich ein weitgehender Konsens entwickelt, der in der Deklaration von Taipeh der World Medical Association (WMA) vom Oktober 2016 festgehalten ist.[517] Die Deklaration zielt insbesondere auf den Datenschutz sowie auf Qualitätssicherung. Die darin enthaltenen Grundsätze werden vom Standing Committee of

513 Burkert in Roßnagel, Handbuch Datenschutzrecht (2003), Kap. 2.3 Rn. 37 f.; Ullrich, RDV 1994, 217–221; Simitis in Simitis, Einl. Rn. 192 ff.; Körner in Schmidt/Weichert S. 426.

514 DuD 2014, 403; dazu Weichert, DuD 2014, 402; vgl. DANA 2014, 119, 176.

515 Dokumentiert unter www.globalcompact.de/wAssets/docs/Menschenrechte/Publikationen/leitprinzipien_fuer_wirtschaft_und_menschenrechte.pdf.

516 Vgl. http://www.unesco.de/infothek/dokumente/unesco-erklaerungen/erkl-bioethik-05-text.html; weitere Nachweise bei ULD (2009) S. 24.

517 World Medical Association (WMA), Declaration of Taipei on Ethical Considerations regarding Health Databases and Biobank, revised by the 67th General Assembly, Taipei, Taiwan, October 2016; zu den Vorläuferdokumenten 1964 und 2004 ULD (2009) S. 23 f.

European Doctors (CPME) insbesondere mit Blick auf die neuen normativen Herausforderungen durch die DSGVO unterstützt.[518] 2016 wurde die Genfer Erklärung über ethische Leitlinien für die biomedizinische Humanforschung durch den Rat der Internationalen Organisationen für medizinische Wissenschaften (CIOMS) gemeinsam mit der Weltgesundheitsorganisation (WHO) überarbeitet und veröffentlicht.[519]

Auch die Empfehlung des Rats der **Organisation für wirtschaftliche Zusammenarbeit und Entwicklung** (OECD) über Leitlinien für den Schutz des Persönlichkeitsrechts und der grenzüberschreitende Verkehr personenbezogener Daten vom 23.9.1980 entfaltet keine rechtliche Bindungswirkung.[520] Auf der Grundlage des Ansatzes der Selbstregulierung sollen die Leitlinien u. a. verhindern, dass sich die Kluft zwischen europäischem und US-amerikanischem Datenschutz weiter vergrößert. [521] 2009 nahm die OECD "Recommendations on Human Biobanks and Genetic Research Databases" (HBGRD) an.[522]

Der **Europarat** hat in seinem „Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten", der Europäischen Datenschutzkonvention 108, Regeln für die automatisierte Verarbeitung von personenbezogenen Daten in automatisierten Dateien und Sicherungsmaßnahmen, insbesondere auch für sensitive Gesundheitsdaten festgelegt.[523] Der Europarat erarbeitete inzwischen eine Vielzahl von Regeln und Empfehlungen, die sich auch auf die komplexe Verarbeitung sensitiver Daten beziehen.[524] Am 23.1.2017 legte der Beirat der Datenschutzkonvention des Europarats „Richtlinien zum Schutz persönlicher Daten in einer Big-Data-Welt" vor, deren Ziel es ist, eine Konkretisierung der Konvention 108 vorzunehmen.[525] Adressiert werden die ethische und sozialverantwortliche Datennutzung, präventive risikoorientierte Maßnahmen, Zweckbindung und Transparenz, Privacy by Design, Einwilligung, Anonymisierung, menschliche Interventionsmöglichkeit, Open Data und Bildungsmaßnahmen.

---

518 CPME endorses the WMA Declaration of Taipei on ethical considerations regarding health databases and biobanks, Press Release 12 April 2017.

519 Council for International Organizations of Medical Sciences (CIOMS), International Ethical Guidelines for Healthrelated Research Involving Humans, https://cioms.ch/wp-content/uploads/2017/01/WEB-CIOMS-EthicalGuidelines.pdf.

520 Simitis in Simitis, Einl. Rn. 184 ff.; dok. bei Simitis/Dammann/Mallmann/Reh, Dokumentation zum BDSG Bd. 2, D 12; Gürtler, RDV 2012, 126; Thießen, Implantate, S. 189 ff.

521 Burkert in Roßnagel Kap. 2.3 Rn. 31.

522 http://www.oecd.org/sti/biotech/guidelinesforhumanbiobanksandgeneticresearchdatabaseshbgrds.htm; zum Entwurf ausführlich ULD (2009) S. 28 ff.

523 Konvention Nr. 108 v. 28.1.1981, in Kraft in 46 Staaten, in Deutschland seit 1985, BGBl. II 1985, S. 538; Simitis in Simitis, BDSG, Einl Rn. 136 ff., 151 ff.

524 Simitis in Simitis, BDSG, Einl Rn. Rn. 178; Weichert in Däubler u. a., BDSG, Einl Rn. 88; ULD (2009) S. 24 ff.

525 Council of Europe, Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic processing of Personal Data, Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, 2017, rm.coe.int/t-pd-2017-1-bigdataguidelines-en/16806f06d0.

7.2 EU-Recht

Neben umfassenden verfassungsrechtlichen Vorgaben (s. o. 6) bestehen im Recht der Europäischen Union (EU) mehrere allgemeine und spezifische Regelungen, die auf Big Data Anwendung finden. Es gibt **Bestrebungen zur Vereinheitlichung** des normativen Rahmens. Diese Bestrebungen beziehen sich auf den Datenschutz mit der vom 25.5.2018 an direkt anwendbaren Europäischen Datenschutz-Grundverordnung (DSGVO)[526], einer für den Polizei- und Justizbereich geltenden Richtlinie (DSRl-JI)[527] sowie einer derzeit im Gesetzgebungsverfahren befindlichen „Verordnung über Privatsphäre und elektronische Kommunikation" (ePrivacy-Verordnung).[528] Weitere europaweite Vorgaben macht die EU mit einer Richtlinie zum Schutz von Geschäftsgeheimnissen.[529] Es ist Ziel der EU, den digitalen Binnenmarkt umfassend normativ zu vereinheitlichen. Bzgl. der Verarbeitung von Gesundheitsdaten gibt es bisher – abgesehen vom Datenschutzrecht – noch keine spezifischen Regelungen oder Regelungsvorschläge der EU.

Es ist weitgehend unstreitig, dass der Regelungsrahmen der EU noch nicht den rechtlichen Bedürfnissen genügt und den modernen technischen Rahmenbedingungen gerecht wird. Von den Kritikern wird dabei zumeist nicht gefordert, dem z. B. in den USA praktizierten Pragmatismus bei der Regulierung zu folgen (siehe aber 8.2). Es soll vielmehr ein Rechtsrahmen geschaffen werden, der Partizipation ermöglicht, für alle Beteiligten **Rechtssicherheit** bringt und zugleich die Voraussetzung schafft, dass die Potenziale eines digital unterstützten Gesundheitswesens umfassend genutzt werden können.[530]

7.3 Nationales Recht

Das nationale Recht der Datenverarbeitung im Gesundheitsbereich ist durch Vielschichtigkeit und Intransparenz gekennzeichnet. Man kann von einem „disparaten Regelungskonzept" sprechen.[531] Im Vordergrund steht das **Datenschutzrecht** mit allgemeinen Gesetzen auf Bundes- und auf Länderebene sowie allgemeinen und speziellen Kirchenregelungen. Für Sozialleistungsträger gilt ein weitgehend eigenständiges und abgeschlossenes Normensystem in den Sozialgesetzbüchern mit allgemeinen Regelungen in den SGB I (insbes. § 35) und X (insbes. §§ 67a ff.) und spezielleren Regelungen in den weiteren SGB, insbesondere dem SGB V zur gesetzlichen Krankenversicherung (GKV).[532] Für den Krankenhausbereich bestehen sowohl auf Bundes-, Länder- und Kirchenebene teilweise sehr spezielle Vorschriften.[533]

---

526 Verordnung (EU) 2016/679 v. 27.4.2016, ABl. L 119 v. 4.5.2016, 1 ff.
527 Richtlinie (EU) 2016/680 v. 27.4.2016, ABl. L 119 v. 4.5.2016, 89 ff.
528 Vorschlag der Europäischen Kommission v. 10.1.2017, COM(2017') 10 final, 2017/0003 (COD); Bericht des Europäischen Parlaments v. 20.10.2017, COM(2017)0010-C8-0009/2017-2017/0003 (COD).
529 Richtlinie (EU) 2016/943 v. 8.6.2016, ABl. L 157 v. 15.6.2016, 1 ff.
530 Wehmeier/Baumann in Langkafel S. 147.
531 Buchner MedR 2016, 661.
532 Weichert in Kühling/Buchner Art. 9 (??) Rn. 170.
533 Weichert in Kühling/Buchner Art. 9 Rn. 172.; Münch S. 83 ff.; Schneider S. 123 ff.; Hauser/Haag S. 14 ff.

Daneben gilt das **Medizinrecht**, das standesrechtliche, bereichsspezifische und allgemeinrechtliche Anteile hat. Als Standesrecht sind in erster Linie die Heilberufsgesetze und die Satzungen der Heilberufskammern zu nennen, an vorderster Front die (Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte (MBOÄ) der Ärztekammern. Für medizinische Spezialbereiche gibt es auf Bundes- und zumeist auf Landesebene besondere Rechtsgrundlagen, etwa zu Arzneimitteln, Medizinprodukten, zum Infektionsschutz, zu Transplantationen und Transfusionen[534], zur Gendiagnostik und zum Embryonenschutz, zu Gesundheitsdiensten oder zur Behandlung psychisch Kranker. Allgemeine Regelungen sind das Strafgesetzbuch mit seiner Regelung zur beruflichen Schweigepflicht (§ 203 StGB) sowie das Bürgerliche Gesetzbuch mit seinen Regelungen zum Behandlungsvertrag (§§ 630a BGB). Haftungsregelungen haben im Bereich der Digitalisierung generell sowie im Datenschutz speziell bisher nur eine untergeordnete Rolle gespielt. Dies kann sich aber unter dem Regime der DSGVO und evtl. verschärfter bzw. präzisierter Haftungsregelungen[535] ändern.[536]

7.4 Privatautonomie vs. Fürsorge

Es gibt keinen allgemeinen Rechtsgrundsatz, dass **Privatunternehmen** gegenüber ihren Vertragspartnern eine Fürsorgepflicht hätten. Das Recht geht davon aus, dass sich Privatpersonen und Unternehmen grds. gleichberechtigt – auf Augenhöhe – gegenüberstehen. Das Zivilrecht kennt aber inzwischen eine Vielzahl von Fallkonstellationen, wo die Dominanz einer Seite den Staat dazu veranlasst hat, sich mit rechtlichen Vorkehrungen schützend vor die schwächere Seite zu stellen (s. o. 6.1).

Diese Erwägung ist grundlegend für die gesamte Entwicklung des **Arbeitsrechts**. Dabei wurde ein hoch differenziertes Rechtssystem mit einer Vielzahl von Gesetzen mit kollektiv- wie mit individualrechtlichen Instrumenten aufgebaut, mit einer eigenständigen Gerichtsbarkeit und mit bereichsspezifischen Regelungen zu bestimmten Fragestellungen (z. B. zur Arbeitszeit, zum Umgang mit Erkrankungen, Schwanger- und Mutterschaft, zu Kündigungen, Urlaub). Insofern ist es erstaunlich, dass diese Regelungen im Arbeitsverhältnis bisher nur sehr wenige Fragestellungen zur Digitalisierung, und dies in sehr allgemeiner Art behandeln (z. B. Mitbestimmungspflicht gemäß § 87 Abs. 1 Nr. 6 BetrVG; vereinzelte Fragen des Datenschutzes gemäß § 32 BDSGaF bzw. § 26 BDSGnF). Dies hat dazu geführt, dass an Stelle des Gesetzgebers die Rechtsprechung die Aufgaben der staatlichen Schutzpflicht des schwächeren Vertragsparts übernommen hat. Dies mag für eine erste Interessenabklärung in einem frühen Entwicklungsstadium sinnvoll gewesen sein. Den vielfältigen Fragestellungen, die sich beim Einsatz von Big Data am Arbeitsplatz auftun, auch soweit diese Gesundheitsthemen zum Gegenstand haben, ist dieser Ansatz aber nicht mehr gewachsen. Hier bedarf es gesetzlicher Antworten.

534 Zum Transfusionsgesetz (TFG) Schneider S. 62 ff.
535 BMVI S. 4, 77, 122, 127 f.
536 Deutscher Ethikrat S. 108 f., 181 f.

Beim Schutz des schwächeren Vertragspartners hat der Verbraucherschutz zumindest hinsichtlich der Digitalisierungsthemen das Arbeitsrecht überholt. Das Verbraucherrecht schränkt die Privatautonomie im Interesse des Schutzes des Schwächeren vor Täuschung und Übervorteilung ein.[537] Dies gilt für die Vertragskontrolle (§§ 305 ff. BGB zu allgemeinen Geschäftsbedingungen) oder im Hinblick auf ein kollektives Klagerecht (UKlaG).[538] Digitale Einzelfragen, wie z. B. Scoring oder automatisierte Entscheidungen wurden aus einem verbraucherspezifischen Blickwinkel geregelt (§§ 6a, 28b BDSGaF, §§ 31, 37 BDSGnF). Auch wenn für das gesamte Regelungskonzept der DSGVO das Verhältnis zwischen Unternehmen und Verbraucher Pate stand, so erweisen sich angesichts der schnellen technischen und ökonomischen Entwicklungen in diesem Bereich immer noch viele Fragen als unbeantwortet.

Der Schutz von Patienten im Verhältnis zu Behandelnden ist Ziel des Patientenrechtegesetzes, das 2013 in Kraft getreten ist.[539] Die Einfügung der §§ 630a-630h BGB soll Patienten und Behandelnde „auf Augenhöhe bringen".[540] Die §§ 630 Abs. 2, 630e, 630g BGB zielen darauf ab, durch Informations-, Aufklärungs- und Einsichtspflichten des Behandelnden mehr Transparenz für die Patienten zu schaffen. Die spezifischen Probleme der erhöhten Intransparenz durch Digitalisierung sowie die sonstigen mit dem Einsatz digitaler Technik und Big Data verbundenen Risiken werden durch das Gesetz aber nicht adressiert.

Angesichts der teilweise extremen informationellen, technischen und finanziellen Machtasymmetrie zwischen Nutzern und IT- bzw. Medizin-Unternehmen als Anbietern besteht für den Gesetzgeber oft keine andere Möglichkeit, als den Unternehmen Schutzpflichten gegenüber ihren Vertragspartnern aufzuerlegen. Der Staat zeigte sich bisher nur sehr beschränkt in der Lage bzw. bereit, durch eine verstärkte Aufsicht dem Schutzauftrag selbst nachzukommen. Angesichts der Geschwindigkeit der technischen Entwicklung, der Komplexität und des Umfangs der Sachverhalte war es ihm bisher nicht möglich, die nötigen gesetzlichen Grundlagen zu schaffen und die administrativen Voraussetzungen für deren Umsetzung zu schaffen.

Hinsichtlich der Datensicherheit bestehen derartige gesetzliche Schutzpflichten (Art. 32 ff. DSGVO; BSI-G). Vergleichbare Pflichten ergeben sich auch z. B. im Hinblick auf die Beseitigung strafbarer Übergriffe durch Online-Inhalte.[541] Vorstellbar ist die Wahrnehmung einer solchen Schutzfunktion auch zur Vermeidung bzw. Bekämpfung von anderen Missbräuchen, insbesondere bei Netzangeboten, z. B. in Bezug auf Mobbing oder Online-Sucht[542]. So wird darüber diskutiert, dass Internetunternehmen Maßnahmen zur Detektion

537 Deutscher Ethikrat S. 108.
538 Zu Klagemöglichkeiten wegen Datenschutzverstößen Weichert DANA 2017, 4 ff.
539 G. v. 20.2.2013, BGBl. I S. 277.
540 Jaeger in Prütting Vorb §§ 630a-h BGB Rn. 3 6.(?)
541 Dazu Netzwerkdurchsetzungsgesetz v. 1.9.2017, BGBl. I S. 3352.
542 Busse/Martin-Jung, Süchtig nach Daten, SZ 26.1.2018, 17.

von Suizidrisiken ergreifen sollen.[543] Mit derartigen Maßnahmen laufen die Unternehmen Gefahr, statt adäquatem Schutz Bevormundung zu praktizieren. Zumeist würden diese Maßnahmen zudem komplexe Datenauswertungen von zum Teil hochsensiblen Daten voraussetzen, die in jedem Fall einer gesetzlichen Legitimation bedürfen. Solche Gesetze können nur auf einer validen empirischen Basis begründet werden und bedürften einer wohldurchdachten Interessenabwägung zwischen Fürsorge- und Selbstbestimmungsinteressen und Berücksichtigung von Missbrauchsgefahren. Wohl aber kann es angebracht sein, die Unternehmen zu reinen Hilfeangeboten zu verpflichten, die ohne Grundrechtseingriffe auskommen.[544]

8 Materielles Datenschutzrecht

Die Regulierung von Big Data mit personenbezogenen Daten erfolgt vorrangig und grundlegend über das Datenschutzrecht, das seine verfassungsrechtlichen Grundlagen im allgemeinen Persönlichkeitsrecht nach Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG bzw. im Grundrecht auf Datenschutz nach Art. 8 GRCh hat (s. o. 6.5). Wie Art. 1 Abs. 2 DSGVO zum Ausdruck bringt, hat das Datenschutzrecht darüber hinausgehend den Anspruch, generell die Grundrechte und Grundfreiheiten natürlicher Personen zu schützen. Es wird immer wieder behauptet, dass die Prinzipien und Zielvorgaben des Datenschutzes mit den Besonderheiten von **Big Data nicht in Einklang** zu bringen seien. Personenbezug, Zweckbindung, Erforderlichkeit, Datensparsamkeit, Einwilligung und Transparenz stünden im Widerspruch zur Eigenlogik von Big Data.[545] Dabei wird übersehen, dass das Datenschutzrecht Instrumente zur gestaltenden Bewältigung informationstechnischer Persönlichkeitsrisiken bereitstellt, nicht zur Verhinderung von nützlichen informationstechnischen Anwendungen.

Im Folgenden wird die Anwendung des Datenschutzrechts auf Big Data im Gesundheitswesen detailliert erörtert. Dabei wird auf die vom 25.5.2018 an geltende Rechtslage Bezug genommen. Von diesem Zeitpunkt an wird der **neue europäische Rechtsrahmen** mit der DSGVO und der DSRI-JI direkt anwendbar sein. Auf die zuvor geltenden Regelungen, insbesondere das BDSGaF sowie auf europäischer Ebene die EG-DSRI, wird Bezug genommen.

8.1 DSGVO und Gesundheit

Die DSGVO befasst sich in einigen Erwägungsgründen mit der Verarbeitung von Gesundheitsdaten. Gemäß ErwGr 52 S. 1 DSGVO soll die **Verarbeitung von Gesundheitsdaten erlaubt** sein, „wenn dies durch das öffentliche Interesse gerechtfertigt ist, insbesondere für die Verarbeitung von personenbezogenen Daten auf dem Gebiet des Arbeitsrechts und des Rechts der sozialen Sicherheit einschließlich Renten und zwecks Sicherstellung und Überwachung der Gesundheit und Gesundheitswarnungen, Prävention

543 Deutscher Ethikrat S. 163.
544 Deutscher Ethikrat S. 26.
545 Deutscher Ethikrat S. 87.

oder Kontrolle ansteckender Krankheiten und anderer schwerwiegender Gesundheitsgefahren. Eine solche Ausnahme kann zu gesundheitlichen Zwecken gemacht werden, wie der Gewährleistung der öffentlichen Gesundheit und der Verwaltung von Leistungen der Gesundheitsversorgung, insbesondere wenn dadurch die Qualität und Wirtschaftlichkeit der Verfahren zur Abrechnung von Leistungen in den sozialen Krankenversicherungssystemen sichergestellt werden soll, oder wenn die Verarbeitung im öffentlichen Interesse liegenden Archivzwecken, wissenschaftlichen oder historischen Forschungszwecken oder statistischen Zwecken dient."

ErwGr. 53 DSGVO präzisiert den gesteigerten Schutz: „Besondere Kategorien personenbezogener Daten, die einen höheren Schutz verdienen, sollten nur dann für gesundheitsbezogene Zwecke verarbeitet werden, wenn dies für das Erreichen dieser Zwecke im Interesse einzelner natürlicher Personen und der Gesellschaft insgesamt erforderlich ist, insbesondere im Zusammenhang mit der Verwaltung der Dienste und Systeme des Gesundheits- oder Sozialbereichs, einschließlich der Verarbeitung dieser Daten durch die Verwaltung und die zentralen nationalen Gesundheitsbehörden zwecks Qualitätskontrolle, Verwaltungsinformationen und der allgemeinen nationalen und lokalen Überwachung des Gesundheitssystems oder des Sozialsystems und zwecks Gewährleistung der Kontinuität der Gesundheits- und Sozialfürsorge und der grenzüberschreitenden Gesundheitsversorgung oder Sicherstellung und Überwachung der Gesundheit und Gesundheitswarnungen oder für im öffentlichen Interesse liegende Archivzwecke, zu wissenschaftlichen oder historischen Forschungszwecken oder statistischen Zwecken, die auf Rechtsvorschriften der Union oder der Mitgliedstaaten beruhen, die einem im öffentlichen Interesse liegenden Ziel dienen müssen, sowie für Studien, die im öffentlichen Interesse im Bereich der öffentlichen Gesundheit durchgeführt werden. Diese Verordnung sollte daher harmonisierte Bedingungen für die Verarbeitung besonderer Kategorien personenbezogener Gesundheitsdaten im Hinblick auf bestimmte Erfordernisse harmonisieren, insbesondere wenn die Verarbeitung dieser Daten für gesundheitsbezogene Zwecke von Personen durchgeführt wird, die gemäß einer rechtlichen Verpflichtung dem Berufsgeheimnis unterliegen. Im Recht der Union oder der Mitgliedstaaten sollten besondere und angemessene Maßnahmen zum Schutz der Grundrechte und der personenbezogenen Daten natürlicher Personen vorgesehen werden."

8.2 Verbot mit Erlaubnisvorbehalt

Eine rechtsstaatliche und grundrechtskonforme Umsetzung von Big Data im Gesundheitsbereich setzt voraus, dass sich die Protagonisten dieser Methode nicht der Vorstellung hingeben, es handele sich hierbei ausschließlich um eine Frage technischer bzw. wissenschaftlicher Machbarkeit. Um das mögliche Potenzial der Informationsverarbeitung auszuschöpfen, ohne die Grundwerte des freiheitlichen und

demokratischen Zusammenlebens zu gefährden, müssen die **in der Verfassung normierten Grundwerte** beachtet werden.[546]

Die Verarbeitung personenbezogener Daten generell wie von Gesundheitsdaten speziell unterliegt einem grundsätzlichen Verbot mit Erlaubnisvorbehalt (Art. 6 DSGVO). Eine Erlaubnis ist durch die Betroffenen über die Einwilligung oder eine vertragliche Absprache möglich wie auch auf Grund eines Gesetzes. Denkbar ist, dass ein Gesetz bei sensitiver Verarbeitung selbst die Verarbeitung auf Einwilligungsgrundlage verbietet oder unter spezifische Anforderungen stellt (Art. 9 Abs. 2 lit. a DSGVO).[547] In der Einwilligung bzw. in der erlaubenden gesetzlichen Regelung muss **alles für die Zulassung Wesentliche** benannt werden.[548] Je sensitiver eine Verarbeitung im Hinblick auf die Zwecke, die verarbeitenden Stellen, die Art der Datenverarbeitung oder die Auswirkungen auf die Betroffenen ist, desto höhere Anforderungen sind an die Konkretheit der Erlaubnis zu stellen. Dies führte z. B. dazu, dass für die Verarbeitung von Daten über Krebserkrankungen in Krebsregistern von den Parlamenten gesetzliche Vorgaben gemacht werden.[549]

Eine weit verbreitete Kritik am bestehenden Datenschutzrecht meint, es reguliere im nicht-öffentlichen Bereich einen verfassungsrechtlich nicht gebotenen **staatlichen Paternalismus**, indem es jede Form der personenbezogenen Datenverarbeitung unter Erlaubnisvorbehalt stelle.[550] Es wird gar vom „Überwachungsstaat um des Datenschutzes willen" gesprochen.[551] Diese Kritik ignoriert, dass eine Konzentration personenbezogener Daten in unserer modernen Informationsgesellschaft ein Macht- und Herrschaftsinstrument gegenüber den betroffenen Menschen darstellt, unabhängig davon, ob dieses in den Händen des Staates oder in den Händen von Privatunternehmen liegt. Legitime Verarbeitungsinteressen werden vom Datenschutzrecht durch Abwägungsklauseln umfassend anerkannt. Gerade bei der Verarbeitung sensitiver Massendaten ohne ausreichende Transparenz und Bestimmungsmöglichkeit der Betroffenen, wie sie bei Big Data im Gesundheitsbereich oft erfolgt, zeigt sich die Relevanz privater oder öffentlicher Datenverarbeitung für das allgemeine Persönlichkeitsrecht und die Freiheiten der Menschen und die Notwendigkeit der gesetzlichen Einhegung.[552]

8.3 Personenbezug

Die Anwendbarkeit des Datenschutzrechts setzt die **Verarbeitung** personenbezogener Daten voraus. Der Begriff der Verarbeitung ist im Hinblick auf Big Data unproblematisch. Gemäß Art. 4 Nr. 2 DSGVO ist er umfassend; er erfasst jeden „ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das

546 Weichert DuD 2014, 837.
547 Weichert in Kühling/Buchner Art. 9 Rn. 48.
548 Weichert in Däubler u. a. Einl. Rn. 20.
549 Weichert DuD 2014, 835 f.
550 Masing NJW 2012, 2306; Gassner in Stiftung Datenschutz (2017) S. 43 f.; Bull, Netzpolitik: Freiheit und Rechtsschutz im Internet, 2013; dagegen Weichert DuD 2013, 246 ff.; siehe auch oben 7.4
551 So Giesen in Stiftung Datenschutz (2016) S. 37; dagegen Weichert RDV 2016, 225.
552 Karg DuD 2013, 75 ff.; so wohl auch Gassner in Stiftung Datenschutz (2017) S. 45 f.

Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung". Vom Recht erfasst sind also sämtliche Prozesse von der Erhebung der Daten über die Speicherung und Auswertung bis hin zur Nutzung der Ergebnisse.

Art. 4 Nr. 1 DSGVO definiert „personenbezogene Daten" (inhaltlich entsprechend § 3 Abs. 1 BDSGaF): „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene 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".

Personenbezogene Daten sind Informationen einer identifizierten oder identifizierbaren natürlichen Person – des Betroffenen. Zur Feststellung der Identifizierbarkeit sollen alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden können, um die Person direkt oder indirekt zu identifizieren. Der Einsatz von Big Data kann dazu führen, dass Daten, die ursprünglich als anonym angesehen wurden, durch die Rekombination mit großen Datenmengen zu einer Reidentifizierung von Betroffenen führen.[553] Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollen alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind (ErwGr 26 S. 4 DSGVO). Identifizierbarkeit ist weit auszulegen. Es muss kein Personenbezug bestehen; es genügt, wenn dieser, u. U. über mehrere Zwischenschritte, hergestellt werden kann. Das ist der Fall, wenn im Umfeld der verantwortlichen Stelle Zusatzwissen vorhanden ist, das abgefragt werden könnte.[554]

Für die Identifizierbarkeit kommt es nicht nur auf die Kenntnisse, Mittel und Möglichkeiten der verarbeitenden Stelle und die dieser normalerweise zur Verfügung stehenden Hilfsmittel an.[555] Identifizierbarkeit ist nicht relativ, sondern objektiv zu bestimmen.[556] Verfügt die speichernde Stelle nicht über die Zuordnungsmöglichkeit zu einem Pseudonym, wohl aber eine andere Stelle, sind die pseudonymisierten Daten personenbezogen, wenn es nicht völlig unrealistisch ist, dass die andere Stelle ihre Kenntnisse zur Verfügung stellt.

553 Spindler MedR 2016, 691 f., 695.
554 Weichert in Däubler u. a., Art. 4 DSGVO Rn. 19; Deutscher Ethikrat S. 54 ff.
555 So aber Gola/Schomerus § 3 Rn. 10; Wojtowicz, PinG 2013, 65.
556 Pahlen-Brandt, DuD 2008, 34; Karg, ZD 2012, 256; Buchner in Taeger/Gabel, § 3 Rn. 13; EuGH ZD 2012, 32 mit Anm. Meyerdierks; tendenziell auch Brink/Eckhardt, ZD 2015, 205.

Die Zuordnungsmöglichkeiten zwecks Identifizierung durch **Verkettung von Datenbeständen** nehmen mit der technischen Entwicklung immer weiter zu.[557] Die Anwendung von Big Data dient oft der Herstellung eines Personenbezugs von als anonym angesehenen Daten. Ein Personenbezug besteht nur dann nicht, wenn Einzelangaben nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeit einer natürlichen Person zugeordnet werden können und damit als anonym behandelt werden können (ErwGr 26, vgl. § 3 Abs. 6 BDSGaF). Da über das globale Internet jede Information weltweit zur Verfügung gestellt werden kann, besteht diese generelle Möglichkeit grds. auch für das für die Identifizierung nötige Wissen. Eine Ausnahme besteht allenfalls dann, wenn das Zusatzwissen auf wenige begrenzt bleibt und dessen Preisgabe nicht nur rechtlich, sondern auch praktisch, z. B. technisch-organisatorisch ausgeschlossen wird.

Die objektiv zu beurteilende Identifizierbarkeit ist unabhängig von der Identität und von den Intentionen der verantwortlichen Stelle. Auf die Zielsetzung bzw. den **Zweck der Verarbeitung**, also einen subjektiven Vorbehalt, kommt es bei der Feststellung der Anwendbarkeit des Datenschutzrechts nicht an. Der Zweck bzw. das Ziel der Verarbeitung ist relevant bei der Beurteilung der Rechtmäßigkeit. Anderenfalls hinge die Anwendbarkeit des Datenschutzrechts davon ab, welche innere Vorstellung eine Stelle von ihrer Verarbeitung hat.[558] Absehbare und zu erwartende Entwicklungen sind zu berücksichtigen.[559]

Es kann grds. nicht darauf ankommen, ob die Beschaffung des für die Identifizierung nötigen Zusatzwissens nur durch **Verstoß gegen Gesetze** erlangt werden kann.[560] Die DSGVO kennt kein „verbotenes Risiko". Der Umstand, dass aus der Ex-ante-Sicht eines Verantwortlichen ein Personenbezug nicht mit vertretbaren Mitteln herstellbar war, befreit nicht von der Anwendbarkeit der DSGVO, wenn dies z. B. einem IT-Unternehmen oder Hacker doch gelingt.[561] Eine andere Sicht würde dazu führen, dass allein durch ein rechtliches Verbot der Personenbezug ausgeschlossen werden könnte. Führt ein rechtliches Verbot in Kombination mit technisch-organisatorischen Sicherungen dazu, dass eine Zuordnung objektiv nicht mehr möglich oder absolut unwahrscheinlich ist, so fehlt es am Personenbezug.

8.4 Genetische und Gesundheitsdaten als sensitive Daten

Das europäische Datenschutzrecht schützt genetische Daten (s. o. 2.1.1) und Gesundheitsdaten (s. o. 2.1) als **besondere Kategorien personenbezogener Daten** gemäß Art. 9 DSGVO in besonderem Maße dadurch, dass die Verarbeitung von einer spezifischen

557 Hansen, Meissner u. a. – ULD, Verkettung digitaler Identitäten, 2007.

558 Weichert, DuD 2009, 351; Klar/Kühling in Kühling/Buchner Art. 4 Nr. 1 Rn. 29; a. A. tendenziell EuGH 19.10.2016, C-582/14, NJW 2016, 3581, Rn. 46, 49; Schneider S. 18 m. w. N.

559 Piltz K&R 2016, 561.

560 Gola/Schomerus § 3 Rn. 10; a. A. Meyerdierks MMR 2009, 9; Arning/Forgó/Krügel DuD 2006, 704 f.; so tendenziell auch EuGH 19.10.2016 – C-582/14, Rn. 49, NJW 2016, 3581.

561 Ernst in Paal/Pauly Art. 4 Rn. 13.

Einwilligung (s. u. 8.8) oder von einem näher die Zwecke benennenden Gesetz erlaubt wird, das „angemessene und spezifische Maßnahmen“ zum Schutz der Betroffenen vorsieht. Diese Regelung bestätigt die zuvor geltenden Regelungen in den §§ 3 Abs. 9, 28 Abs. 6-9 BDSGaF, Art. 8 EG-DSRl, § 7 Abs. 12 SGB XaF. Das besondere Schutzregime dient der Verhinderung von Diskriminierungsrisiken sowie der Verteidigung spezifischer Grundrechte.[562]

In vielen **weiteren Regelungen** wird der Schutz sensitiver Daten präzisiert. Sollen diese in automatisierte Entscheidungen – einschließlich Profiling – einfließen, so benennt Art. 22 Abs. 4 DSGVO hierfür besondere Vorgaben (s. u. 8.9). Im Falle einer umfangreichen Verarbeitung gemäß Art. 35 Abs. 3 lit. b DSGVO, die im Fall von Big Data im Regelfall stattfindet, hat eine Datenschutz-Folgenabschätzung zu erfolgen (s. u. 8.20). Handelt es sich bei der Kerntätigkeit eines Verantwortlichen um die Verarbeitung sensitiver Daten, muss dieser gemäß Art. 37 Abs. 1 lit. a DSGVO einen Datenschutzbeauftragten bestellen. Für die Datenverarbeitung mit einem gewissen Risiko im Drittausland ist gemäß Art. 27 Abs. 1, 2 DSGVO die Benennung eines Vertreters in der EU Pflicht.

8.5 Verantwortlicher

Die datenschutzrechtliche **Verantwortlichkeit** wird in Art. 5 Abs. 2 DSGVO festgelegt.[563] Danach muss der Verantwortliche die Beachtung der Datenschutzgrundsätze nach Art. 5 Abs. 1 DSGVO gewährleisten (Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit) und deren „Einhaltung nachweisen können“.

Die **Begriffsdefinition** des „Verantwortlichen“ enthält Art. 4 Nr. 7 DSGVO: „die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so können der Verantwortliche beziehungsweise die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden“.

Teilweise wird die Ansicht vertreten, dass bei **arbeitsteiliger Datenverarbeitung**, wie sie bei Big Data oft vorkommt, eine Verantwortung für Rechtsverstöße nur bei Vorliegen eines Vertragsverhältnisses besteht, und wenn die Stelle positive Kenntnis von den Tatsachen hat, welche die rechtswidrige Verarbeitung der beteiligten anderen Stelle begründen.[564] Mit der datenschutzrechtlichen Verantwortlichkeit wird auch die zivilrechtliche Passivlegitimation begründet, selbst wenn die Einflussmöglichkeit auf die Datenverarbeitung begrenzt ist.[565] Keine Verarbeitung „im Auftrag“, sondern in eigener Verantwortung ist es, wenn eine Stelle durch Gesetz oder behördliche Anweisung

562 Weichert in Kühling/Buchner Art. 9 Rn. 14-17.
563 Zu ethischen Aspekten der Verantwortung Deutsche Ethikrat S. 158 ff.
564 Petri ZD 2015, 103.
565 A. A. LG Berlin ZD 2015, 235.

verpflichtet wird, Daten für hoheitliche Zwecke zu speichern und vorzuhalten.[566] Kann eine datenschutzrechtliche Verantwortlichkeit bei einem informationstechnischen Mittler nicht begründet werden, so kommt bei Verletzung des allgemeinen Persönlichkeitsrechts eine Haftung als Störer in Betracht.[567]

Die Frage, ob und inwieweit einer **Maschine**, einem Computer oder einem Algorithmus Verantwortung übertragen werden kann, ist sowohl ethisch wie auch rechtlich eindeutig zu verneinen. Zwar kann Informationstechnik dafür genutzt werden, Verantwortung gezielter, differenzierter, schneller und situationsangepasster wahrzunehmen. Dies gilt nicht nur für die Verarbeitung des Verantwortlichen, sondern auch für die Betroffenen, die die Wahrnehmung ihrer subjektive Rechte Software übertragen können.[568] Die Letztverantwortung für das, was ein Rechner tut und veranlasst, muss aber in jedem Fall bei einer Person, also einem Menschen oder einer Organisation (juristischen Person) liegen. Dies gilt selbst für den Einsatz Künstlicher Intelligenz. Selbstlernende Algorithmen können ihre Entscheidungen nur auf der Grundlage ihrer Programmierung und ihrer Fütterung mit Daten fällen. Für den Dateninput wie auch die Programmgestaltung bleiben letztlich die handelnden und damit auch rechtlich zur Verantwortung zu ziehende Personen zuständig (s. o. 2.9).

Bei **komplexen Verarbeitungsverfahren** liegt die Verantwortlichkeit zuweilen bei unterschiedlichen Stellen und teilweise auch beim Betroffenen selbst. Entscheidend ist, wer den Datenverarbeitungsprozess tatsächlich beherrscht.[569] Dabei kann es Schwierigkeiten der Zuordnung geben. Befinden sich die Daten in Verbunddateien und sind mehrere Stellen selbstständig zur Veränderung der Datensätze berechtigt, was bei Big-Data-Verbünden der Fall sein kann, so liegt die Verantwortlichkeit kumulativ bei sämtlichen derart berechtigten Stellen. Ist z. B. ein Verbundteilnehmer zu einer Löschung oder Berichtigung verpflichtet, müssen die anderen Teilnehmer dies auch gegen sich gelten lassen. Erfolgt ein (automatisierter) Abruf eines Verbundteilnehmers von einem Datum, für das nur eine andere Stelle verantwortlich ist, liegt hierin eine Offenlegung.[570]

Eine **gemeinsame Verantwortlichkeit** (Art. 26 DSGVO) ist gegeben, wenn die Verarbeitung selbständige Entscheidungen verschiedener Stellen voraussetzen, d. h. wenn eine Verarbeitung ohne die aktive Beteiligung jeder Stelle nicht denkbar ist. Dies ist bei Big-Data-Anwendungen der Fall, bei denen sich der einzelne Teilnehmer die Verarbeitung des Anderen zurechnen lassen muss. Keine gemeinsame Verantwortlichkeit besteht, wenn die Voraussetzungen des Art. 28 DSGVO (vgl. § 11 BDSGaF), einer Auftragsverarbeitung vorliegen. Bei einer rechtlich zugelassenen Auftragsverarbeitung ist der Auftraggeber

566 Kritisch Simitis RDV 2007, 148.
567 Mantz ZD 2014, 62; KG MMR 2013, 659; LG Hamburg DuD 2013 – Mosley; LG Heidelberg CR 2015, 326; a. A. Voigt K&R 2014, 80; allgemein Peifer AfP 2014, 18.
568 Deutscher Ethikrat S. 161.
569 Art. 29-Datenschutzgruppe, Arbeitsdokument Datenschutz und RFID-Technologie v. 18. 1. 2005, WP 105; Kesten RDV 2008, 100; Deutscher Ethikrat S. 25.
570 VGH Kassel CR 1992, 693.

Verantwortlicher. Ein Vertragsverhältnis zwischen den gemeinsam Verantwortlichen ist nicht nötig. Es genügt, dass sich die Verantwortlichkeit aus den faktischen Umständen ergibt. Die Verantwortlichkeit ist objektiv festzustellen. Soweit ein (gemeinsam) Verantwortlicher keine Kenntnis von einer gemeinsam zuzurechnenden Verarbeitung hat, fehlt es für Sanktionen möglicherweise an der subjektiven Zurechenbarkeit. Spätestens mit Kenntniserlangung können alle einem Verantwortlichen zuzurechnende Pflichten, auch die Umsetzung der Betroffenenrechte, abverlangt werden.[571]

Für die Auftragsverarbeitung genügt es, dass eine Stelle personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. An die Art oder die Form des Auftrags werden keine Anforderungen gestellt. Die rechtliche Zulässigkeit ist in Art. 28 DSGVO geregelt. Sind diese Voraussetzungen nicht gegeben, so kann es sich dennoch um eine (evtl. unzulässige) Auftragsverarbeitung handeln. Derartige Aufträge werden beim klassischen Outsourcing erteilt. Es spielt keine Rolle, in welchem Umfang der Verantwortliche weiß, wie der Auftrag abgearbeitet wird.[572] Liegen die in Art. 28 DSGVO genannten Voraussetzungen vor, so ist der Auftragsverarbeiter nicht Dritter i. S. v. Art. 4 Nr. 10 DSGVO und die Verarbeitung durch ihn ist grds. zulässig. Fehlt es an den Voraussetzungen des Art. 28 DSGVO, so gilt der „Auftragsverarbeiter" als Verantwortlicher (Art. 28 Abs. 10 DSGVO).

Eine spezifische Form der Übernahme von Verantwortung kann darin liegen, dass Betroffene oder verantwortliche Stellen ihre Rolle delegieren.[573] Zwar ist eine Stellvertretung im Datenschutzrecht nicht vorgesehen. Die Betroffenenrechte sind höchstpersönlich. Bei einer vertraglichen Übertragung einer datenschutzrechtlichen Verantwortung hat diese nur im Innenverhältnis, nicht aber gegenüber Dritten Rechtswirkung. Dies ändert aber nichts an dem Umstand, dass eine Delegation möglich ist und die Funktion von Datenagenten oder Datentreuhändern insbesondere bei komplexen Formen der Verarbeitung, wie sie bei Big Data bestehen, sinnvoll sein kann. So lässt sich die Wahrnehmung der Betroffenenrechte delegieren mit der Folge, dass die ökonomische und juristische Kompetenz gegenüber den Verantwortlichen erhöht wird.[574] Auch verantwortliche Stellen können sich eines solchen Treuhänders bedienen, um gemeinsame Interessen bei komplexen Verarbeitungen zu konzentrieren und zu vereinfachen. Damit kann Machtungleichgewichten und Interessenkollisionen entgegen gewirkt werden.[575]

---

571 Weichert ZD 2014, 1; Weichert, Datenschutzrechtliche Verantwortlichkeit – Anspruch und Wirklichkeit, in Breiter/Wind (Hrsg.) Informationstechnik und ihre Organisationslücken, 2011, S. 301 ff.; Weichert DANA 2012, 18 ff.; ähnlich Petri ZD 2015, 103; a. A. VG Schleswig 9.10.2013 – 8 A 14/12, ZD 2014, 51; OVG Schleswig-Holstein 4.9.2014 – 4 LB 20/13, DuD 2014, 839 = ZD 2014, 643 = CR 2014, 801; relativierend BVerwG 25.2.2016 – 1 C 28.14, CR 2016, 729 = K&R 2016, 437 = DuD 2016, 537; Martini/Fritsche, Mitverantwortung in sozialen Netzwerken, NVwZ-Extra 21/2015, 1; vgl. Monreal ZD 2014, 612; Dammann ZD 2016, 312; Artikel-29-Arbeitsgruppe 1/2010, WP 169.

572 Härting Rn. 579; ausführlich Engeler, SchHA 2017, 339 f.; a. A. Schreiber in Plath Art. 4 Rn. 28.

573 Deutscher Ethikrat S. 121.

574 Theißen S. 456; dazu grundlegend ULD (2013).

575 Deutscher Ethikrat S. 184.

Die Aufgabe, Big-Data-Prozesse in einem Unternehmen oder in einem Verbund von Personen und Stellen **verantwortlich zu gestalten**, ist voraussetzungsvoll. Dies gilt zum einen in Bezug auf die Betroffenenrechte (Einwilligungsmanagement, Transparenz, Korrektur, Sperrung/ Verarbeitungsbeschränkung, Löschung)[576] wie aber insbesondere im Verhältnis der daten- und verfahrensbestimmenden Beteiligten. Ein rechtliches Defizit besteht bisher darin, dass die Verantwortlichkeit von den Herstellern von Hardware und Programmen aus datenschutzrechtlicher Sicht bisher wenig diskutiert und normativ nicht präzisiert worden ist. Insofern kann sich eine Verbesserung der unsicheren Situation durch die Etablierung von Zertifizierungsverfahren ergeben (s. u. 8.22.2).[577] Darüber hinausgehend ist es möglich und wünschenswert, Verantwortlichkeiten normativ zu präzisieren.

8.6 Zweckbindung

Eines der zentralen rechtlichen Probleme von Big Data ist die nachträgliche Änderung des Zwecks bei einer personenbezogenen Datenverarbeitung.[578] Der in Art. 8 Abs. 2 GRCh formulierte Grundsatz der „Zweckbindung" wird in Art. 5 Abs. 1 lit. b DSGVO konkretisiert. Danach müssen personenbezogene Daten „für **festgelegte, eindeutige und legitime Zwecke** erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden". Sodann ist eine Privilegierung für im öffentlichen Interesse liegende Archiv-, Forschungs- und Statistikzwecke vorgesehen (dazu näher 8.14). Der Grundsatz der Zweckbindung ist seit dem Volkszählungsurteil des BVerfG fester Bestandteil der deutschen Verfassungsrechtsprechung.[579]

Aufgabe der Zweckbindung ist es, den Betroffenen zu ermöglichen, in ihrem Leben in **verschiedenen Rollen** jeweils eine eigene Identität zu entwickeln und zu entfalten. Sie soll verhindern, dass Persönlichkeitsbilder (s. o. 2.5) entstehen, die für die externe Wahrnehmung und die Behandlung der Person bestimmend werden. Die Konturen der Zweckbindung werden im ErwGr 50 DSGVO näher beschrieben; die äußeren Grenzen der Zweckänderung werden in Art. 6 Abs. 4 DSGVO festgelegt. Bei der Prüfung, ob eine Zweckänderung zulässig ist, hat eine zweistufige Prüfung zu erfolgen: Zunächst bedarf es der Feststellung, dass die Zweckverfolgung rechtmäßig ist; im zweiten Schritt ist zu prüfen, ob die Zweckänderung gegen Art. 6 Abs. 4 verstößt.[580]

Der Zweck wird über den **Verarbeitungskontext** oder durch den Betroffenen, z. B. über seine Einwilligungserklärung definiert. Daten bei einer Behörde dienen der Erledigung von deren gesetzlich definierten Aufgaben. Vertragsdaten von Kunden bei einem Versandhändler dienen zunächst der Abwicklung des Vertragsverhältnisses. Wurden Daten nicht gezielt erhoben, sondern anderweitig erlangt, so erfolgt die Zweckfestlegung

576 Deutscher Ethikrat S. 160.
577 Deutscher Ethikrat S. 162.
578 Spindler MedR 2016, 691.
579 Culik/Döpke ZD 2017, 230; umfassende Nachweise bei Herbst in Kühling/Buchner Art. 5 Rn. 21 Fn. 20.
580 Albrecht/Jotzo Teil 2 Rn. 5 (S. 52); a. A. Plath in Plath Art. 6 Rn. 31; Kramer in Auernhammer Art. 5 Rn. 16.

anlässlich der gezielten Speicherung.[581] Daten aus einer ärztlichen Behandlung dienen zunächst ausschließlich der medizinischen Betreuung des Patienten. Während für den Betroffenen ein ursprünglicher Verarbeitungskontext bei einer Direkterhebung zumeist noch nachvollziehbar ist, geht dieser tendenziell bei Zweck- und damit Kontextänderungen verloren.

Es liegt im Interesse der Transparenz, dass die **Zweckfestlegung** in der Einwilligungserklärung (s. u. 8.8.2) oder einer Vertragspassage erfolgt. Dabei dürfen keine unbestimmten Leerformeln oder Allerweltsbeschreibungen verwendet werden. Generell gilt, dass eine Zweckmitteilung gegenüber dem Betroffenen „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren einfachen Sprache" erfolgen muss (Art. 12 Abs. 1 DSGVO). Soweit der Zweck eindeutig ist, kann er sich auch unausgesprochen aus dem Kontext ergeben. Dabei ist auf einen vernünftigen kundigen Betrachter abzustellen, für den sich das Erwartbare oder Übliche der Datenverarbeitung erschließt.[582]

Der Zweck muss legitim sein. **Legitimität** setzt voraus, das der Zweck gesetzeskonform ist, was z. B. durch eine spezifische gesetzliche Regelung sichergestellt wird. Verfolgt eine Stelle, privat oder öffentlich, verschiedene Aufgaben und Zwecke, so muss grds. eine Trennung nach diesen Aufgaben erfolgen (z. B. Apotheke - Kosmetikgeschäft[583]). Vertragsabwicklung und Werbung sind grds. unterschiedliche Zwecke. Im privaten Bereich besteht für den Verantwortlichen für die verfolgten Zwecke über die Privatautonomie eine weitgehende Bestimmungsmöglichkeit. Nicht mehr erfasst und damit illegitim sind Zwecke oder Zweckverbindungen, die rechtlich ausgeschlossen sind. Illegitim sind auch solche Zwecke, die den Betroffenen unverhältnismäßig bzw. übermäßig beeinträchtigen (vgl. Art. 6 Abs. 4 DSGVO). Unzumutbare intime Angaben, Selbstbezichtigungen sowie Gefahren der sozialen Abstempelung sind auszuschließen.[584] Den Gefahren der Diskriminierung und der Manipulation ist vorzubeugen.[585]

Eine **Zweckänderung** ist durch den Grundsatz der Zweckbindung nicht ausgeschlossen. Durch eine Einwilligung oder auf gesetzlicher Grundlage kann für einen legitimen Zweck die Informations- oder Nutzungssperre der Zweckbindung überwunden werden. Keine Zweckänderung liegt vor, wenn für einen konkreten Zweck eine Vielzahl von Verarbeitungsschritten nötig ist. Wird bei der Weiterverarbeitung ein anderer neuer Zweck verfolgt, so muss auch dieser legitim sein. Ein Prüfungskriterium ist, dass der

581 Wolff in Schantz/Wolff Rn. 418; Weichert in Däubler u. a. § 3 Rn. 31, 34.
582 Frenzel in Paal/Pauly Art. 5 Rn. 27.
583 ULD, 35. TB 2015 Kap. 4.6.9 (S. 64).
584 BVerfG NJW 1984, 422 f.
585 Weichert ZD 2013, 255.

Verantwortliche die Daten für den neuen Zweck selbst hätte erheben dürfen (hypothetische Datenneuerhebung).[586]

Die datenschutzrechtliche Zweckbindung wird als ein Hindernis für Big Data angesehen. Dies gilt jedenfalls dann, wenn Daten, die für unterschiedliche Zwecke erhoben wurden, zusammengeführt und analysiert werden. Es wird gerade als ein Spezifikum von Big Data angesehen, dass Daten „dekontextualisiert" werden und für einen ursprünglich nicht vorgesehenen Zweck verwendet, also „rekontextualisiert" werden.[587]

In personenbeziehbarer Form ist dies zulässig, wenn die rechtlichen Voraussetzungen für eine Zweckänderung gegeben sind (Art. 6 Abs. 4 DSGVO).[588] Der mit der Weiterverarbeitung über Big Data verfolgte Zweck muss selbst wieder präzise definiert werden. Es können aber abstrakt keine festen Grenzen hinsichtlich der zulässigen Zwecke definiert werden.[589] Die Zulässigkeit eines Zwecks hängt von sämtlichen Verarbeitungsumständen ab, wozu auch die technisch-organisatorischen (z. B. Pseudonymisierung, Treuhänderverfahren), die materiellen (z. B. Forschungsgeheimnis; Zeugnisverweigerungsrechte, Beschlagnahmeverbote) und die verfahrensrechtlichen (z. B. Genehmigungspflichten, Zertifizierungsanforderungen) Sicherungen gehören.[590] Ohne derartige verbindliche und damit für den Betroffenen einklagbare Kompensationen für die Zweckausweitung sind Big-Data-Zusammenführungen und -Analysen dagegen regelmäßig europarechts- und verfassungswidrig.[591]

8.7 Geeignete Schutzmaßnahmen

Der Mangel an Konkretheit der Zwecke von Big Data im Gesundheitsbereich kann durch materiell- und verfahrensrechtliche sowie zusätzliche technisch-organisatorische Sicherungen kompensiert werden. Dies lässt sich realisieren durch spezifische Einwilligungsmodelle, durch bereichsbezogene Erlaubnisnormen, durch Transparenz-, Melde- oder Genehmigungsanforderungen, durch Weiterentwicklungen des Verbraucher- oder des Haftungsrechts sowie durch technische-organisatorische Vorgaben für die Verarbeitung und deren konkrete Umsetzung.[592] Die DSGVO erlaubt daher die Durchbrechung der Zweckbindung, setzt aber dann geeignete Garantien bzw. angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Personen voraus (s. o. 8.6, s. u. 8.12, 8.21).[593]

---

586 BVerfG 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, BKA-Gesetz, DVBl 2016, 771 = NJW 2016, 1801, Rn. 287.

587 Deutscher Ethikrat S. 57 f.; Augsberg MedR 2016, 700; Ladeur DuD 2016, 360 f.

588 Weichert ZD 2013, 255.

589 Zur Bereitschaft der Datenweitergabe in Gesundheitskontexten Deutscher Ethikrat S. 58 f.

590 ULD (2009) S. 20 ff.

591 Weichert DuD 2014, 835; Culik/Döpke ZD 2017, 228 ff.

592 Deutscher Ethikrat S. 18 f.

593 So z. B. bei der Erlaubnis zur Verarbeitung besonderer Kategorien personenbezogener Daten in Art. 9 Abs. 2 lit. b, d, g, h, i, j DSGVO oder zu automatisierten Entscheidungen in Art. 22 Abs. Abs. 3, 4 DSGVO.

8.8 Einwilligung

Eine spezifische Form der Wahrnehmung der Selbstbestimmung eines Menschen besteht darin, dass er in die Verarbeitung seiner Daten für bestimmte Zwecke, also z. B. auch für Big-Data-Anwendungen, einwilligt.[594] Die Motivation für die Erteilung einer Einwilligung in die Verarbeitung der eigenen Daten kann sowohl im persönlichen Nutzen, im Nutzen Dritter oder gar dessen einer speziellen Gruppe oder der Gemeinschaft schlechthin liegen.[595] Die datenschutzrechtliche Einwilligung ist in Art. 4 Nr. 11, 7, 8 DSGVO geregelt (bisher § 4a BDSGaF). Danach ist die Einwilligung „jede freiwillig für den bestimmten Fall, in informierter Weise unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden Daten einverstanden ist". Bezieht sich die Einwilligung auf die Verarbeitung sensitiver Daten wie z. B. Gesundheitsdaten, so muss sie sich hierauf explizit beziehen (bisher § 4a Abs. 3 BDSGaF). Dies bedeutet, dass schlüssiges Handeln weitgehend ausgeschlossen ist. Die Erklärung muss ausdrücklich sein; die Nichtnutzung einer Opt-out-Möglichkeit genügt nicht. Das Einholen von Einwilligungen mit dem Kauf eines Geräts oder durch den Abschluss eines Vertrags ist zwar grds. nicht ausgeschlossen. Zu beachten ist aber, dass tatsächlich Wahlmöglichkeit und Freiwilligkeit gewahrt bleiben müssen und dass keine nach Art. 7 Abs. 4 DSGVO unzulässige Koppelung erfolgt.[596] Durch Anreize oder durch Malus-Systeme in Gesundheitsfragen können zielgerichtete Verhaltensbeeinflussungen stattfinden, derer sich die Betroffenen möglicherweise überhaupt nicht bewusst werden, so dass deren Wahlfreiheit eingeschränkt ist.

In einzelnen Gesetzen hat auch der deutsche Gesetzgeber zu erkennen gegeben, dass er an die Einwilligung zur Verarbeitung von Gesundheitsdaten besonders hohe Anforderungen stellt. Dies gilt z. B. für die §§ 7, 8 GenDG in Bezug auf die Information des Betroffenen über die Ergebnisse gentechnischer Untersuchungen.[597] Bei der Offenbarung von über die elektronische Gesundheitskarte erschlossenen Daten verlangt § 291a Abs. 5 S. 1 SGB V die Autorisierung jedes einzelnen Datenverarbeitungsvorgangs (vgl. auch § 291a Abs. 1a S. 1 SGB V in Bezug auf privat Krankenversicherte). Um die Freiwilligkeit sicherzustellen, darf vom Karteninhaber nicht verlangt werden, dass er den Zugriff auf die Daten Dritten gestattet (§ 291a Abs. 8 SGB V).

Das Bundessozialgericht hat die Zulässigkeit einer Verarbeitung sensitiver Daten auf der Grundlage einer Einwilligung unter Hinweis auf die Bedeutung des Sozialdatenschutzes auch dann als unzulässig erklärt, wenn die Verarbeitung nicht durch Sozialleistungsträger

---

594 Deutscher Ethikrat S. 118 ff.

595 Zum Aspekt der Wohltätigkeit durch Einwilligung in Big Data im Gesundheitsbereich Deutscher Ethikrat S. 142 f.

596 Weichert ZD 2013, 255 f.

597 Gassner in Stiftung Datenschutz (2017) S. 46 f.

erfolgt.[598] Für eine solche Fernwirkung des Sozialdatenschutzes auch in Bereiche, auf die das SGB nicht direkt anwendbar ist, gibt es aber keine materiell-rechtliche Rechtfertigung.

8.8.1 Form

Erwägungsgrund 32 DSGVO stellt klar, dass die Einwilligung **auch elektronisch** erfolgen kann, z. B. „durch Anklicken eines Kästchens beim Besuch einer Internetseite (…) oder durch eine andere Erklärung oder Verhaltensweise (…), mit der die betroffene Person in dem jeweiligen Kontext eindeutig ihr Einverständnis mit der beabsichtigten Verarbeitung ihrer personenbezogenen Daten signalisiert". Opt-out-Lösungen genügen nicht. Wohl aber genügen technische Voreinstellungen z. B. im Rahmen eines persönlichen Einwilligungsprofils, das automatisiert mit digitalen Diensten abgeglichen werden kann.[599] Bei der Einholung von Einwilligungen über Allgemeine Geschäftsbedingungen (AGB) sind die §§ 305 ff. BGB zu beachten.[600] Eine Einwilligung muss in der Muttersprache des Marktlandes formuliert sein; eine ausschließlich Englisch verfasster Text genügt zumeist nicht.[601]

Die Einholung der Einwilligung und die dem vorausgehende Aufklärung erfolgen regelmäßig durch die verarbeitende Stelle, ohne dass dies zwingend so sein müsste. Sie sind **zu dokumentieren** und müssen im Zweifelsfall vom Verantwortlichen nachgewiesen werden können (Art. 7 Abs. 1 DSGVO).

Die Einwilligungen können digital in einem **Einwilligungsmanagement** hinterlegt werden, das es ermöglicht, automatisiert den Zugriff auf bestimmte Daten gemäß einem Berechtigungskonzept zuzulassen. Ein solches Konzept kann auch die Wünsche von Betroffenen, von Informationen verschont zu bleiben (Recht auf Nichtwissen, s. o. 6.5) berücksichtigen.[602] Durch die Zugriffsmöglichkeit und Wahlmöglichkeit des Betroffenen kann ihm hierüber eröffnet werden, seine Optionen zu verändern und eine erteilte Einwilligung zu widerrufen.[603] Bei Big-Data-Anwendungen bietet sich eine solche automatisierte Einwilligungsverwaltung an, um einerseits die Selbstbestimmung des Betroffenen wie auch die Zugänglichkeit für Auswertungen bestmöglich zu realisieren.

8.8.2 Inhalt

Auf die Sensitivität oder den **besonderen Charakter der Daten** muss hingewiesen werden, so dass sich der Betroffene bewusst wird, dass er sich mit der ausdrücklichen Erklärung möglicherweise außerhalb des besonderen rechtlichen Schutzes begibt. Zudem besteht die Notwendigkeit der Benennung eines konkretisierten Verwendungszusammenhangs.

---

598 BSG 10.12.2008 – B 6 KA 37'/07 R, MedR 2009, 685, 690; kritisch dazu Brisch/Laue CR 2009, 465; Kleinert DuD 2010, 240; Kühling/Seidel GesR 2010, 231; Kircher in Kingreen/Kühling S. 237 ff.; Spindler MedR 2016, 696.

599 Gassner in Stiftung Datenschutz (2017) S. 40 f.

600 Schneider S. 113 ff.

601 KG Berlin MMR 2016, 601; Dregelies VuR 2017, 260.

602 Bergh/Brandner/Kutscha/Heinze/Schreiweis in Stiftung Datenschutz, S. 29.

603 Bergh/Brandner/Kutscha/Heinze/Schreiweis in Stiftung Datenschutz, S. 19 ff.; Deutscher Ethikrat S. 25.

An den Inhalt der Einwilligung ist bei Gesundheitsdaten ein **erhöhtes Maß an Bestimmtheit und Genauigkeit** zu stellen.[604] Die Einwilligung kann sich nur auf die zugrundeliegende Datenverarbeitung oder im Fall des Art. 22 DSGVO auf den Umstand der automatisierten Entscheidung beziehen, nicht auf den Inhalt der Entscheidung, da die Einwilligungserklärung vor der Datenverarbeitung abgegeben werden muss.[605] Da gemäß Art. 22 Abs. 3 DSGVO zu den Sicherungen die Möglichkeit „des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts und der Anfechtung der Entscheidung gehört", soll durch die Einwilligung keine unangemessene Verkürzung der Betroffenenrechte erfolgen. Aus Nachweisgründen (Art. 5 Abs. 2, 7 Abs. 1 DSGVO) empfiehlt sich für den Verantwortlichen bei der Einholung der Einwilligung die Schrift- oder die protokollierte (elektronische) Textform.[606] Bei Big Data lassen sich rechtliche Regelungen, die ausschließlich die Schriftform der Erlaubniserklärung vorsehen, oft nicht einhalten.[607] Besteht ein europäisch oder national geregeltes Verarbeitungsverbot bezüglich sensitiver Daten, das durch eine Einwilligung nicht aufgehoben werden kann, so kann eine Legitimation für die Verarbeitung auch nicht aus Art. 6 Abs. 1 lit. a DSGVO abgeleitet werden (Art. 9 Abs. 1 lit. a).

Diese aus dem Datenschutzrecht stammenden Anforderungen werden durch das Medizinrecht bekräftigt. Die Einwilligung ist als Entbindung vom Patientengeheimnis Ausdruck nicht nur der informationellen, sondern auch der **medizinischen Selbstbestimmung** und der Patientenautonomie im Arzt-Patienten-Verhältnis.[608] Das im Datenschutzrecht anwendbare Prinzip des „informed consent" stammt ursprünglich aus dem Medizinrecht. Die diesem Prinzip zugrunde liegenden Erwägungen werden nun gerade im Medizinbereich teilweise als Fiktion bezeichnet und in Frage gestellt. Der Patient sei krank und wolle geheilt werden und handle daher nicht selbstbestimmt. Dies gelte insbesondere im Hinblick auf die ihm im Rahmen komplexer Arbeitsteilung und Informationsverarbeitung begegnenden beschränkten kognitiven und emotionalen Möglichkeiten.[609] Diese Erwägungen mögen in vielen Fällen gegeben sein. Sie sind aber nicht in der Lage, das Konzept der Selbstbestimmung in Frage zu stellen. Vielmehr müssen sie Anlass sein, die Rahmenbedingungen für selbstbestimmtes Handeln zu schaffen. Ob sie vorliegen, muss in jedem Einzelfall überprüft und festgestellt werden.

Bei komplexer Datenverarbeitung, wie sie bei Big Data regelmäßig gegeben ist, stellt sich in besonderem Maße das Problem der Informiertheit und der Bestimmtheit. Die nötige Information umfasst die Art der Daten, die Zwecke, die verarbeitenden Stellen und evtl. spezifische Verarbeitungsformen. Um insofern den Willen der Betroffenen bestmöglich

---

604 Kühling/Seidel in Kingreen/Kühling, 102; zu den unterschiedlichen Regelungsansätzen bei Patienteneinwilligungen in EU-Mitgliedsstaaten Reimer/Artmann/Stroetmann DuD 2013, 157.

605 Vgl. Piltz K&R 2016, 636.

606 Dochow GesR 2016, 404; Greve in Auernhammer Art. 9 Rn. 9; Schiff in Ehmann/Selmayr Art. 9 Rn. 30; Schulz in Gola Art. 9 Rn. 15.

607 Heckmann/Paschke in Stiftung Datenschutz (2017) S. 70.

608 Gassner in Stiftung Datenschutz (2017) S. 47.

609 Gassner in Stiftung Datenschutz (2017) S. 48 ff.

abzubilden und diesen zugleich nicht hinsichtlich der Komplexität der von ihm geforderten Entscheidung zu überfordern, bietet sich ein stufenweises bzw. wiederholtes Vorgehen an (sog. layered design, dynamic consent).[610] Insofern gibt es keine Patentlösungen. Vielmehr muss bzw. sollte empirisch untersucht werden, mit welchen Formulierungen welche Vorstellungen bei den Betroffenen ausgelöst werden und wie durch Strukturierung, Verwendung von Icons (vgl. Art. 12 Abs. 7, 8 DSGVO) und unter Berücksichtigung des typischen Wahrnehmungs- und Erklärungshorizonts der Betroffenen eine größtmögliche Information und Selbstbestimmung realisiert werden kann. Ein „Information Overload" kann ebenso zu einer uninformierten Zustimmungserklärung führen wie unzureichende Informationen.[611] Insofern bedarf es der Entwicklung von Fallstudien und darauf basierend der Entwicklung von sprachlichen, kommunikativen und technischen Standards, um einen „empowered consent" ´zu erreichen. In diese Richtung geht die Entwicklung von Aufklärungs- und Beratungsstrategien, „Onepagern", von Vorgaben in Verhaltensregeln (Art. 40 DSGVO), von technischen Prozessen, von Leitlinien und/oder Standards.[612] Bei umfassenden, einheitlich zu behandelnden Verarbeitungsprozessen (z. B. generelle Freigabe für die medizinische Forschung) können auch generelle Einwilligungen zulässig sein (sog. broad consent).[613] Voraussetzung ist dann aber, dass im breiten Anwendungsfeld eine strenge Zweckbindung sowie ethische Standards beachtet werden und die Betroffenen die Möglichkeit eingeräumt bekommen, ihre Einwilligung auf bestimmte Forschungsbereiche oder Teile von Forschungsprojekte zu erteilen. Eine „breite Einwilligung" in kommerzielle Auswertungen z. B. durch Internet-Firmen, wird damit nicht abgedeckt.[614]

Um die Überschaubarkeit für den Betroffenen sicherzustellen, können Einwilligungen zeitlich beschränkt werden. Regelungen hierzu bestehen aber nicht. Einwilligungen können nur so lange Wirksamkeit entfalten, wie für die Betroffenen die Verarbeitungen noch überschaubar sind. Es gibt insofern bisher keine Standards, die z. B. festlegen, wann eine Einwilligung wegen ihrer unbefristeten Geltung unbestimmt und damit unwirksam wird.

8.8.3 Freiwilligkeit

Besteht ein Abhängigkeitsverhältnis zwischen dem Verantwortlichen und dem Betroffenen, eine Machtbeziehung oder eine Art der Über- und Unterordnung in Bezug auf die Verarbeitung der sensitiven Daten, so sind besonders hohe Anforderungen an die Freiwilligkeit einer Einwilligung zu stellen (z. B. Nützlichkeit für den Betroffenen, expliziter Hinweis auf Freiwilligkeit, vgl. § 26 Abs. 2 BDSGnF). Zwar soll bei einem klaren Ungleichgewicht zwischen der betroffenen Person und dem Verantwortlichen die Einwilligung „keine gültige Rechtsgrundlage liefern" (ErwGr 43 S. 1 DSGVO). Dies kann

610 Deutscher Ethikrat S. 122 f. m. w. N.
611 Gassner in Stiftung Datenschutz (2017) S. 52 f.
612 Gassner in Stiftung Datenschutz (2017) S. 55 ff.; Von Kalle/Ücker/Eils/Winkler/Schickhardt in Stiftung Datenschutz (2017) S. 94.
613 Bergh/Brandner/Kutscha/Heinze/Schreiweis in Stiftung Datenschutz (2017), S. 30 f.; kritisch Spindler MedR 2016, 697 f.; Schneider S. 118 ff.
614 ErwGr 33 S. 2, 3 DSGVO; Raum in Stiftung Datenschutz (2017) S. 138 f.

gegenüber Versicherungen der Fall sein,[615] zwischen Ausübenden eines Hilfsberufs und den Hilfebedürftigen, etwa zwischen Arzt und Patient[616] oder im Verhältnis eines IT-Anbieters im Gesundheitsbereich und den Nutzenden.[617] Insofern können aber keine pauschalen Aussagen gemacht werden; es bedarf einer Einzelfallfeststellung. Durch Maßnahmen wie besondere Wahlmöglichkeiten und die Sicherstellung, dass bei einer Einwilligungsverweigerung keine Nachteile entstehen, kann die Unfreiwilligkeit vermieden werden. In ungleichgewichtigen Beziehungen kommt dem Koppelungsverbot nach Art. 7 Abs. 4 DSGVO Bedeutung zu (s. u.).[618]

Keine Freiwilligkeit kann angenommen werden, wenn die Einwilligung zur Bedingung einer sehr erwünschten oder gar dringend benötigten (medizinischen) Dienstleistung gemacht wird. Das Prinzip des „take it or leave it" zerstört die Freiwilligkeit nicht nur, wenn es keine Handlungsalternativen gibt, so wie dies bei Informations-, Kommunikations- und sonstigen Leistungsangeboten im Internet oft der Fall ist, sondern auch, wenn alternative Angebote mit anderen Hürden (unzureichende Bekanntheit, Kosten, zeitlich begrenzte Verfügbarkeit) verknüpft sind. Etwas Anderes kann nur gelten, wenn eine konkrete Datenverarbeitung unter Beachtung des Grundsatzes der Datensparsamkeit für die Erbringung des Dienstes erforderlich ist. In diesen Fällen ist aber rechtlich zumeist nicht mehr eine (auch widerrufbare) Einwilligung gegeben, sondern ein vertragliches Gegenseitigkeitsverhältnis, so z. B. bei selektivvertraglichen Versorgungsmodellen (§ 295a SGB V).[619]

Die Freiwilligkeit von Einwilligungen wird nun durch Art. 7 Abs. 4 DSGVO abgesichert. Danach liegt keine Freiwilligkeit vor, wenn die Erbringung einer Dienstleistung oder die Erfüllung eines Vertrags „von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich ist" (sog. Koppelungsverbot). Eine ärztliche Behandlung darf grds. nicht davon abhängig gemacht werden, dass die dabei erlangten Daten für Big-Data-Analysen genutzt werden können.[620]

Wird eine Einwilligung im Rahmen einer Behandlung abgegeben, so kann dies die Freiwilligkeit beeinträchtigen, insbesondere wenn sich die Einwilligung auf einen behandlungsfremden Vorgang (z. B. Forschung) bezieht. Insofern kann es sinnvoll sein, die Erklärung zeitlich oder institutionell von der konkreten Behandlung zu entkoppeln.

Die Möglichkeit der Legitimation durch Einwilligung besteht auch für die Verarbeitung von sensitiven Beschäftigtendaten. Hinsichtlich der Freiwilligkeit sind dann gesteigerte

615 BVerfG MMR 2007, 93.
616 Dochow GesR 2016, 404; Wedde in Däubler u. a. § 28 Rn. 166; Simitis in Simitis § 28 Rn. 295; Kühling/Seidel in Kingreen/Kühling, 183 f.
617 Theißen S. 337 ff.
618 Dochow GesR 2016, 404; Kühling/Seidel in Kingreen/Kühling, 152.
619 Dies übersieht Gassner in Stiftung Datenschutz (2017) S. 51 f.
620 Vgl. Ladeur DuD 2016, 364.

Anforderungen zu stellen (§ 26 Abs. 2 BDSGnF).[621] Danach liegt Freiwilligkeit insbesondere vor, „wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen". Gegenüber den allgemeinen Anforderungen können keine Abstriche gemacht werden. Konkludente Einwilligungen sind nicht vorgesehen.[622] Wird nach Art. 88 DSGVO durch besondere Rechtsvorschrift in einem bestimmten Bereich eine Einwilligung für unzulässig erklärt, so gilt diese Vorgabe. Dies ist z. B. wegen § 7 Abs. 1 AGG relevant für Informationen über rassische oder ethnische Herkunft, politische Meinungen, religiöse, philosophische und politische Überzeugungen..[623]

8.8.4 Big Data

Die Einwilligungsfähigkeit von **Big-Data-Anwendungen** hat enge Grenzen. Deren Zielsetzung liegt gerade darin, die Bindungen von Verantwortlichkeit, Zweckbindung und begrenzten Datenbeständen aufzubrechen, um neue Erkenntnisse zu erlangen. Bei Big Data geht es oft darum, zweckungebunden und stellenungebunden Auswertungen vorzunehmen. Hierzu einen informed consent einzuholen ist in der Praxis oft schwierig oder gar nicht möglich.[624] Doch kann durch technische Lösungen, z. B. den Einsatz von „Einwilligungsassistenten", versucht werden, wirksame Einwilligungslösungen auch bei Big-Data-Verfahren zu realisieren (s. o. 8.8.1, 8.8.2).

Eine teilweise bestehende Fehlvorstellung ist, dass die Einwilligung und eine gesetzliche Erlaubnis sich gegenseitig ausschlössen. Richtig ist vielmehr, dass **normative Festlegungen** geeignet sein können, eine an und für sich zu unbestimmte und unfreiwillige Einwilligung zu einer legitimen Grundlage für eine komplexe Datenverarbeitung zu machen.[625] Sie können auch anstelle des Opt-in Wege für Opt-out-Modelle eröffnen. Solche Modelle können im Interesse größtmöglicher Datenqualität und Repräsentativität[626] verhältnismäßig sein.

8.9 Automatisierte Einzelentscheidung – einschließlich Profiling

Eine spezifische datenschutzrechtliche Regulierung hat die „automatisierte Entscheidung – einschließlich Profiling" gefunden. Diese ist in Art. 22 DSGVO als Betroffenenrecht normiert.[627] Tatsächlich handelt es sich aber eher um eine generelle **materiell-rechtliche Vorgabe für komplexe Datennutzungen**. Die Regulierung zielt auf die abschließende Verwendung einer Datenanalyse, also den letzten Schritt im Rahmen eines Big-Data-Prozesses. Die Regulierung erfasst aber nicht nur dieses Stadium der Datennutzung,

621 Wedde in Däubler u. a. § 28 Rn. 165; vgl. BAG 11.12.2014 – 8 AZR 1010/13, AuR 2015, 239; Dzida NZA 2017, 543.
622 A. A. Dzida NZA 2017, 544.
623 Gola/Schomerus § 28 Rn. 76; Dzida NZA 2017, 543.
624 Spindler MedR 2016, 696 f.; Weichert DuD 2014, 835; ders. ZD; Dzida NZA 2017, 543.
625 So wohl auch Gassner in Stiftung Datenschutz (2017) S. 54.
626 Deutscher Ethikrat S. 106 f.
627 Albrecht/Jotzo S. 79; Kühling/Martini u. a., S. 338 f.; Martini in Paal/Pauly Art. 22 Rn. 29; Deuster PinG 2016, 77; Buchner in Kühling/Buchner Art. 22 Rn. 12; a. A. Schulz in Gola Art. 22 Rn. 3, 5, 11: organisatorische (Verfahrens-)Vorschrift mit mittelbarem Verbotscharakter.

sondern nimmt aus dieser Perspektive eine umfassende rechtliche Bewertung aller vorangegangenen Verarbeitungsvorgänge von der Erhebung über die Speicherung und Analyse bis hin zur Nutzung vor.[628] Die Vorgängerregelung zu Art. 22 DSGVO ist Art. 15 EG-DSRl, der im deutschen Recht durch § 6a BDSGaF umgesetzt wurde.

Art. 22 basiert nicht auf einem diffusen allgemeinen Unbehagen gegenüber „künstlicher Intelligenz“[629], sondern auf der Erkenntnis, dass die Vorgaben von Algorithmen bei Entscheidungen Betroffene in ihren Rechten und Interessen beeinträchtigen können (s. o. 5.1-5.5). Dass die DSGVO insofern keine präziseren Regelungen zu den modernen Datenanalysemethoden enthält, wird damit begründet, dass nach Ansicht des Gesetzgebers die Entwicklung sich noch in einem frühen Stadium befindet.[630] Tatsächlich erweisen sich immer neue Möglichkeiten des Big Data; künftige Praktiken zeichnen sich teilweise nur in Ansätzen ab. Es ist Versprechen wie Drohung, dass alles mit allem kombinier- und dann auswertbar gemacht wird. Die Zusammenführung und Auswertung von Angaben zu Finanztransaktionen, Bonitätsbewertungen, medizinischen Behandlungen, Konsum, Internetnutzung, Kommunikation über soziale Netzwerke, aus der Berufsausübung, aus der „Smartifizierung“ praktisch aller Lebensbereiche, befindet sich heute noch in einem frühen Stadium.

Hinsichtlich der verfassungsrechtlichen Einordnung von Art. 22 DSGVO sind neben Art. 7 GRCh (s. o. 6.7), soweit Telekommunikation einbezogen ist, und Art. 8 GRCh (s. o. 6.5) weitere Grundrechte bewertungsrelevant: Art. 21 GRCh statuiert Diskriminierungsverbote nach folgenden Merkmalen: Geschlecht, Rasse, Hautfarbe, ethnische und soziale Herkunft, genetische Merkmale, Sprache, Religion, Weltanschauung, politische und sonstige Anschauung, Zugehörigkeit zu einer nationalen Minderheit, Vermögen, Geburt, Behinderung, Alter, sexuelle Ausrichtung und Staatsangehörigkeit. Zu beachten sind zudem verfassungsrechtlich definierte Schutzansprüche in bestimmten Kontexten: der Umgang mit Daten von Kindern und älteren Menschen (Art. 24, 25 GRCh), von Menschen mit Behinderungen (Art. 26 GRCh), im Arbeitsverhältnis (Art. 27-32 GRCh), im Gesundheitswesen (Art. 35 GRCh) und bei Verbraucherbezug (Art. 38 GRCh).[631]

Der europäische Gesetzgeber hat das Profiling in Art. 22 DSGVO – anders als noch in Art. 15 EG-DSRl – zu einem Anwendungsfall automatisierter Entscheidungen erklärt (zum Begriff 2.6). Als Intention führt er aus: „Die betroffene Person sollte das Recht haben, keiner Entscheidung — was eine Maßnahme einschließen kann — zur Bewertung von sie betreffenden persönlichen Aspekten unterworfen zu werden, die ausschließlich auf einer automatisierten Verarbeitung beruht und die rechtliche Wirkung für die betroffene Person entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt, wie die automatische Ablehnung eines Online-Kreditantrags oder Online-Einstellungsverfahren ohne jegliches

628 Weichert in Reiffenstein/Blaschek S. 241; a. A. Buchner in Kühling/Buchner Art. 22 Rn. 4.
629 So Schulz in Gola Art. 22 Rn. 2.
630 Albrecht/Jotzo S. 60, Rn. 6; Deutscher Ethikrat S. 86 f.
631 Weichert in Reiffenstein/Blaschek S. 244 f.

menschliche Eingreifen“ (ErwGr 71 S. 1 DSGVO). Art. 22 DSGVO basiert auf der Erwägung, dass automatisierte Entscheidungen für die Betroffenen ein besonderes Risiko im Hinblick auf Transparenz und Beeinflussbarkeit darstellen, so dass die Nutzung des Datenauswertungsvorgangs als besonders sensitiv angesehen wird.

Keine automatisierte Entscheidung i. S. v. Art. 22 DSGVO liegt vor, wenn ein automatisiertes System auf der Grundlage eines kontextnahen Datensatzes eine (von Menschen) vorfestgelegte Entscheidung trifft, etwa bei Verwendung eines elektronischen Berechtigungsausweises, um Zugang zu einem Raum oder einem Rechner zu erlangen oder bei einer Apparatur, welche die Dosierung einer einem Patienten verabreichten Infusion von der automatisierten Feststellung bestimmter Blutwerte abhängig macht. Erfolgt jedoch automatisiert keine vorfestgelegte überschaubare „Wenn-dann-Entscheidung“, sondern ein komplexer, für den Betroffenen nicht mehr überschaubarer Entscheidungsprozess, dann ist dies ein Fall des Art. 22 DSGVO, auch wenn die Entscheidung letztlich z. B. nur in einem „banalen“ Vorgang, z. B. in der klinischen Entscheidung der Unterbringung in einem Einbett- oder Mehrbettzimmer, besteht.[632] Die fehlende Transparenz hat die fehlende Kontrollierbarkeit und Revisionsfähigkeit der Entscheidung zur Folge. Dieser Verlust entsteht insbesondere, wenn die verwendeten Algorithmen nicht mehr vollständig dokumentiert und damit nicht mehr nachvollziehbar sind.[633] Von Art. 22 DSGVO nicht erfasst sind „automatisierte“ Entscheidungen, bei denen sämtliche (kontextnahen und überschaubaren) Gewichtungen zuvor von Menschen, und nicht von einem automatisierten Verfahren festgelegt wurden.

Art. 22 DSGVO ist immer anwendbar, wenn Entscheidungen mit Auswirkungen für die Betroffenen auf der Grundlage von personenbezogenen Daten mit sog. Künstlicher Intelligenz getroffen werden (s. o. 2.9). Bei derartigen selbstlernenden Systemen fließt das nicht mehr nachvollziehbare, automatisiert erfasste Erfahrungswissen des Systems in die Entscheidung ein.[634]

Es kommt nicht darauf an, ob und inwieweit durch das genutzte Verfahren das Risiko der Fehlerhaftigkeit erhöht wird.[635] Fehlergeneigtheit ist zwar ein oft im Zusammenhang mit automatisierten Entscheidungen thematisiertes Phänomen, aber kein dafür bestimmendes Merkmal. Automatisierte Entscheidungen, etwa im Medizin- und Verkehrsbereich, müssen oft hoch zuverlässig sein, ohne dass dadurch Art. 22 DSGVO ausgeschlossen würde. Es gibt viele automatisierte Entscheidungssysteme, bei denen die Einbeziehung von Menschen deren Fehlerhaftigkeit erhöht, nicht-automatisierte Lösungen also fehlergeneigter sind.

632 Weichert in Däubler u. a. § 6a Rn. 3; Buchner in Kühling/Buchner Art. 22 Rn. 18.
633 Reichwald/Pfisterer CR 2016, 211 f.
634 Reichwald/Pfisterer CR 2016, 211.
635 So aber scheinbar Laue/Nink/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis, 2016, S. 110.

Erfolgt eine automatisierte Entscheidung gemäß Art. 22 DSGVO, so hat dies gemäß der Verordnung rechtliche Konsequenzen. Die Verwendung dieser Technik verpflichtet gemäß Art. 13 Abs. 2 lit. f und Art. 14 Abs. 2 lit. g DSGVO den Verantwortlichen zu „aussagekräftige(n) Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen" für die Betroffenen, egal ob die Daten bei diesen erhoben wurden oder nicht. Art. 15 Abs. 1 lit. h DSGVO begründet zudem einen Anspruch auf „aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person" (s. u. 8.16.1). Gemäß Art. 35 Abs. 3 lit. a DSGVO ist bei derartigen Verfahren eine Datenschutz-Folgeabschätzung erforderlich (s. u. 8.20). In Binding Corporate Rules muss gemäß Art.47 Abs. 2 lit. e DSGVO das Betroffenenrecht des Art. 22 DSGVO inkorporiert werden. Der Europäische Datenschutzausschuss (EDSA) wird in Art. 70 Abs. 1 lit. f DSGVO ermächtigt, „Leitlinien, Empfehlungen und bewährte Verfahren" festzulegen.

Nationalrechtliche Konkretisierungen erfolgten in Deutschland durch Regelungen in den §§ 31, 37 BDSGnF. Gemäß § 31 Abs. 1 BDSGnF ist der Einsatz von Scoring-Verfahren (s. o. 2.4) „zum Zweck der Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses" nur zulässig, wenn das materielle Datenschutzrecht beachtet wird und ein wissenschaftlich anerkanntes mathematisch-statistisches Verfahren zum Einsatz kommt, das nicht nur auf Anschriftendaten beruht. Ursprünglicher Anwendungsfall des Scorings ist der Verbraucher-Kreditvertrag. Inzwischen hat das Scoring aber bei den unterschiedlichsten Konsumentenverträgen Einzug gehalten, etwa im Versicherungswesen. In die Prämienberechnung fließen perspektivisch zunehmend viele Faktoren mit ein, aus denen Rückschlüsse auf besondere Risiken oder Vorteile gezogen werden. Versicherungen berechnen Scores aus Daten über die Kfz-Nutzung oder über gesundheitsrelevante Umstände, um diese im Rahmen der Kfz-Haftpflicht-, der Kranken- oder der Lebensversicherung zu nutzen (s. u. 10.5).[636] Anwendung findet Scoring außerdem bei der Telekommunikation, im Bereich Miete und Leasing sowie bei Lieferverhältnissen. Die Regelung ist auf alle Wirtschaftsbereiche und damit auch im Gesundheitsbereich anzuwenden. Dies wird jedoch vom Regelungsinhalt unzureichend reflektiert.[637] Fehlt eine explizite gesetzliche Erlaubnis, wie sie bei § 37 Abs. 2 BDSGnF besteht, ist auf Basis des § 31 BDSGnF eine Verarbeitung von Gesundheitsdaten nicht zulässig.

Eine nationalstaatliche Konkretisierung des Art. 22 DSGVO erfolgt in § 37 BDSGnF „im Rahmen der Leistungserbringung nach einem Versicherungsvertrag". Bei § 37 handelt es sich um eine Spezialregelung zu § 31 BDSGnF, der wegen seines eigenständigen Regelungsinhaltes vollständig anwendbar bleibt. Automatisierte Entscheidungen sind danach zulässig, wenn 1. „dem Begehren der betroffenen Person stattgegeben wurde" oder 2. „die Entscheidung auf der Anwendung verbindlicher Entgeltregelungen für Heilbehandlungen beruht und der Verantwortliche für den Fall, dass dem Antrag nicht

636 Siedenbiedel, DANA 2015, 24; DANA 2015, 32, 39 f.; Eichler/Kamp in Wolff/Brink Syst. K Rn. 130 ff.; DANA 2014, 171.

637 Helfrich, ZD 2013, 473.

vollumfänglich stattgegeben wird, angemessene Maßnahmen zur Wahrung der berechtigten Interessen der betroffenen Person trifft, wozu mindestens das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung zählt". Nach § 37 Abs. 2 BDSGnF sind solche Entscheidungen auch auf der Grundlage von Gesundheitsdaten erlaubt. Zweck des § 37 ist die digitalisierte Abwicklung von Versicherungsfällen im Massengeschäft von der Schadensmeldung per E-Mail, App oder Messenger-Dienst bis hin zur Entscheidung und deren Umsetzung. Damit sollen Verfahren beschleunigt und Kosten eingespart werden, zumindest wenn dem Begehren des Betroffenen stattgegeben wird. § 37 Abs. 1 Nr. 2 BDSGnF ermöglicht also auch die automatisierte Entscheidung über Versicherungsleistungen privater Krankenversicherungen bei der Anwendung verbindlicher Entgeltregelungen für Heilbehandlungen.

Auch wenn dem Begehren des Antragstellers als von der Entscheidung betroffener Person nicht oder nicht vollständig stattgegeben wird, ist die automatisierte Rechnungsprüfung durch die Private Krankenversicherung zulässig, wenn der Verantwortliche angemessene Maßnahmen zur Wahrung der berechtigten Interessen der betroffenen Person trifft. Hierzu zählt zumindest das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung. Dies kommt insbesondere bei der automatisierten Abrechnung von Leistungsansprüchen durch die private Krankenversicherung zur Anwendung, ermöglicht aber auch die Verarbeitung von sensitiven Daten in anderen Sparten, etwa bei der Unfall- oder der Haftpflichtversicherung. Absatz 2 beruht auf Art. 22 Abs. 4 i. V. m. Art. 9 Abs. 2 lit. g DSGVO. Die Gewährleistung eines bezahlbaren und funktionsfähigen Krankenversicherungsschutzes in der Privaten Krankenversicherung ist, so die Gesetzesbegründung, als gewichtiges Interesse des Gemeinwohls anerkannt. Eine wirtschaftliche Leistungsbearbeitung im Massenverfahren setze den Einsatz von automatisierten Verfahren voraus, insbesondere wenn es um die Anwendung gesetzlicher und somit standardisierter Gebührenordnungen (zum Beispiel Gebührenordnung der Ärzte – GOÄ) geht.[638]

Das Recht, nicht Objekt von automatisierten Entscheidungen von erheblicher Bedeutung für die Lebensführung zu werden sowie das Recht auf Offenlegung und Überprüfung erhält mit der zunehmenden Digitalisierung eine verstärkte Relevanz, die dazu führt, dass die Forderung im Raum steht, diese Rechte explizit zu einem eigenständigen Grundrecht zu erheben (so Art. 7 dGRCh-E).

8.9.1 Wissenschaftlichkeit automatisierter Entscheidungsverfahren

Anders als Art. 22 DSGVO, der insofern keine explizite Regelung enthält, sieht § 31 Abs. 1 Nr. 2 BDSGnF vor, dass Scoringverfahren nur zulässig sind, wenn „die zur Berechnung des Wahrscheinlichkeitswerts genutzten Daten unter Zugrundelegung eines wissenschaftlich anerkannten mathematisch-statistischen Verfahrens nachweisbar für die Berechnung der

638 BR-Drs. 110/17 S. 108.

Wahrscheinlichkeit des bestimmten Verhaltens erheblich sind". Daraus ergibt sich eine Dokumentationspflicht hinsichtlich der genutzten Daten, hinsichtlich deren Relevanz und deren Berechnung (Algorithmus). Mangels hinreichender Dokumentation und Nachvollziehbarkeit wird daraus abgeleitet, dass Verfahren mit selbstlernenden Algorithmen, also der Einsatz von sog. Künstlicher Intelligenz (s. o. 2.9), grds. nicht zulässig ist.[639] Auch sind Verfahren, die auf einer ungenügenden Datenbasis Scores berechnen, unzulässig. Wissenschaftlichkeit muss nicht nur bzgl. der Methode im Allgemeinen gegeben sein, sondern auch bei jeder einzelnen Scoreberechnung. Für die Einbeziehung eines Merkmals zur Scoreberechnung genügt nicht die – evtl. nur gering ausgeprägte – statistische Signifikanz. Nötig ist vielmehr Relevanz bzw. Plausibilität, nicht jedoch Kausalität (s. o. 5).[640]

Zwar sieht **Art. 22 DSGVO** nicht ausdrücklich vor, dass die geregelten automatisierten Entscheidungen wissenschaftlichen Ansprüchen genügen müssen. Diese Anforderung ergibt sich aber indirekt aus folgenden Regelungen: Art. 5 Abs. 1 lit. d DSGVO (Richtigkeit), Art. 5 Abs. 2 DSGVO (Verantwortlichkeit und Nachweispflicht), Art. 22 Abs. 2 lit. b, Abs. 4 DSGVO (angemessene Maßnahmen zum Schutz der Rechte und Freiheiten).

8.9.2 Automatisierte „Entscheidung"

Art. 22 DSGVO und Folgeregelungen knüpfen an eine „ausschließlich auf einer automatisierten Verarbeitung beruhenden **Entscheidung**" an, also einer Computerentscheidung ohne menschliche Einflussnahme. Anstelle des Begriffs „Entscheidung" kann auch von einer Maßnahme gesprochen werden.[641]

Erfasst sind damit nicht nur vollautomatisierte Entscheidungen, sondern auch solche, bei denen ein Mensch vor der Entscheidung deren Inhalt zur Kenntnis nimmt, ohne aber einzugreifen. Erfolgt dagegen eine manuelle Prüfung eines automatisierten Ergebnisses vor einer Entscheidung, und wird dieses bestätigt, so ist Art. 22 DSGVO nicht anwendbar.[642] Über die insofern nötige menschliche Prüftiefe sagt die DSGVO nichts. In jedem Fall müssen aber bei der manuellen Prüfung Aspekte und Erwägungen einfließen können, die automatisiert keine Rolle gespielt haben. Eine rein formale, nicht inhaltliche **Mitwirkung einer natürlichen Person** genügt für den Ausschluss der Anwendbarkeit des Art. 22 nicht. Erst wenn der Mensch seine ihm verliehene Entscheidungsmacht in einem bestimmten Prozess bewusst ausübt und Verantwortung übernimmt, wird Art. 22 verdrängt. Auf die Plausibilität der menschlichen Entscheidung kommt es nicht an.[643] Die Anwendung des Art. 22 DDSGVO wird nicht dadurch ausgeschlossen, dass nach einer getroffenen Entscheidung eine natürliche Person diese nochmals überprüft. Geregelt ist das Fällen der

639 Problematisch deshalb das Vorgehen von Kreditech, DANA 2013, 118.

640 ULD (2005) S. 74; Weichert, DuD 2006, 401 f.; a. A. Hoeren, RDV 2007, 97: mathematische Gesetzmäßigkeit genügt.

641 Buchner in Kühling/Buchner Art. 22 Rn. 23.

642 Härting S. 146.

643 Kühling/Martini u. a. S. 62; Martini in Paal/Pauly Art. 22 Rn. 19; Buchner in Kühling/Buchner Art. 22 Rn. 15; von Lewinski in Wolff/Brink § 6a Rn. 18; Weichert in Däubler u. a. § 6a Rn. 2.

Entscheidung, also deren Bestätigung oder Ausfertigung, nicht das spätere Umsetzen, bei dem Menschen beteiligt sein können.[644]

Für die rechtliche Bewertung spielt es keine Rolle, ob die automatisierte Bewertung der Daten durch eine **andere als die entscheidende Stelle** erfolgt.[645] Erhält z. B. ein Verantwortlicher von einer dritten Stelle einen Score für eine Entscheidung, so muss er sich vergewissern, dass der Score den Anforderungen des Art. 22 DSGVO genügt.

Art. 22 DSGVO ist anwendbar, wenn die Entscheidung eine rechtliche Wirkung entfaltet. Dabei spielt es keine Rolle, ob diese Wirkung für den Betroffenen positiv oder negativ ist. Eine **Nachteilswirkung** wird explizit nicht gefordert, wenngleich der Gesetzgeber insbesondere diese im Blick hatte. Ein fehlender Nachteil kann die Missachtung des Art. 22 nicht rechtfertigen, zumal bei der Feststellung eines Nachteils immer eine subjektive Komponente mitschwingt.[646]

Rechtliche Wirkungen sind z. B. solche, die Einfluss auf einen Vertrag oder ein sonstiges Rechtsverhältnis haben (Entgelte, Ansprüche, Leistungen, Verweigerung einer Leistung, Kündigung eines Vertrags). Dabei kann es um den Erhalt privater oder öffentlicher Leistungen gehen, um den Ausschluss von einem Angebot, die Vorenthaltung einer medizinischen Versorgung oder der Kostenerstattung hierfür, Boni für körperliche Aktivitäten oder die Teilhabe an Vergünstigungen. Art. 22 DSGVO verbietet nicht die unsachlich begründete Ablehnung eines Vertrags oder einer sonstigen Rechtsbeziehung, sondern eine bestimmte technisch vorgegebene diskriminierende Vorgehensweise; er will damit die Privatautonomie stärken.[647]

Art. 22 DSGVO ist auch anwendbar, wenn die Maßnahme den Betroffenen nicht rechtlich, sondern „**in ähnlicher Weise erheblich beeinträchtigt**". Ausschließliche Begünstigungen werden nicht erfasst.[648] Zu beachten ist, dass Vergünstigungen für die Einen regelmäßig zu Beeinträchtigungen bei anderen Betroffenen führen. Beeinträchtigungen sind (nachhaltige) Störungen der wirtschaftlichen oder persönlichen Entfaltung des Betroffenen. Verletzungen des Gleichheitsgrundsatzes machen Art. 22 anwendbar.[649] Da materielle Beeinträchtigungen regelmäßig mit rechtlichen Wirkungen einhergehen, werden von dieser Alternative insbesondere immaterielle Beeinträchtigungen erfasst. Diese dürfen nicht nur kurzfristig und geringfügig, sie müssen erheblich sein. Dabei kann es sich um erhebliche Belästigungen oder faktische Verletzungen des Persönlichkeitsrechts, etwa durch eine automatisierte negative Merkmalszuschreibung handeln.

644 Weichert in Reiffenstein/Blaschek S. 248.
645 Möller/Florax, NJW 2003, 2725, Duhr in Roßnagel S. 1173; Duhr/Naujok/Peter/Seiffert, DuD 2002, 25; ULD (2005) S. 86; a. A. Hoeren, RDV 2007, 98.
646 Anders wohl Buchner in Kühling/Buchner Art. 22 Rn. 25; Piltz K&R 2016, 636.
647 Weichert in Däubler u. a. § 6a Rn. 9.
648 Schulz in Gola Art. 22 Rn. 22.
649 Buchner in Kühling/Buchner Art. 22 Rn. 26; Martini/Nink NVwZ-Extra 10/2017, 3.

Streitig ist, ob Art. 22 DSGVO auch beim Einsatz für Werbezwecke anwendbar ist. Zur Anwendbarkeit auf automatisierte Direktwerbung äußert sich die DSGVO nicht explizit.[650] Die Aufnahme des Profilings, dessen Hauptanwendungsbereich heute die Werbung ist, in den Art. 22 kann nicht nur als Symbolik verstanden werden.[651] Sie signalisiert vielmehr, dass die Norm auf das Marketing anzuwenden sein soll.[652] Hierfür spricht auch, dass die Beobachtung „des Verhaltens von Betroffenen in der Union" durch außereuropäische Anbieter in Art. 3 Abs. 2 lit. b DSGVO ausdrücklich in den Anwendungsbereich der DSGVO einbezogen ist. Gerade Werbemaßnahmen im Gesundheitsbereich haben regelmäßig für die Betroffenen eine invasive Wirkung. Das Geschäftsmodell von mit Daten werbenden Konzernen sollte in Bezug auf europäische Betroffene von den Profiling-Regelungen der DSGVO erfasst werden (ErwGr 24 S. 2 DSGVO). Der Einbeziehung des Werbeprofiling wurde auch dadurch Tribut gezollt, dass Art. 22 kein rigoroses Verbot vorsieht, sondern lediglich „angemessene Maßnahmen" einfordert, wozu bei der Werbung ausdrücklich nach Art. 21 Abs. 2, 3 DSGVO das Recht auf Widerspruch gehört. Worauf sich eine Werbemaßnahme bezieht, ist für die Anwendung des Art. 22 nicht relevant. Dabei kann es sich um Einkaufs- und Konsumtipps, Lese- oder Ernährungsratschläge handeln.[653]

8.10 Allgemeine gesetzliche Verarbeitungserlaubnis

Art. 22 DSGVO kann als datenschutzrechtliche Big-Data-Grundregelung angesehen werden. Er verweist aber auf weitere Rechtfertigungserfordernisse für automatisierte Entscheidungen. Dies ist zum einen die „ausdrückliche Einwilligung der betroffenen Person" (Art. 22 Abs. 2 lit. c DSGVO, s. o. 8.8).

ErwGr. 54 DSGVO weist darauf hin, dass die Verarbeitung auch ohne Einwilligung erfolgen kann: „Aus Gründen des öffentlichen Interesses in Bereichen der öffentlichen Gesundheit kann es notwendig sein, besondere Kategorien personenbezogener Daten auch ohne Einwilligung der betroffenen Person zu verarbeiten. Diese Verarbeitung sollte angemessenen und besonderen Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen unterliegen. In diesem Zusammenhang sollte der Begriff `öffentliche Gesundheit´ (...) und alle Elemente im Zusammenhang mit der Gesundheit wie den Gesundheitszustand einschließlich Morbidität und Behinderung, die sich auf diesen Gesundheitszustand auswirkenden Determinanten, den Bedarf an Gesundheitsversorgung, die der Gesundheitsversorgung zugewiesenen Mittel, die Bereitstellung von Gesundheitsversorgungsleistungen und den allgemeinen Zugang zu diesen Leistungen sowie die entsprechenden Ausgaben und die Finanzierung und schließlich die Ursachen

650 Härting S. 146.

651 So aber Schantz NJW 2016, 1844; Schulz in Gola Art. 22 Rn. 20; wohl auch Herbst in Auernhammer Art. 22 Rn. 8.

652 Hladjk in Ehmann/Selmayr Art. 22 Rn. 9; a. A. Deutscher Dialogmarketing Verband, Europäische Datenschutz-Grundverordnung, Auswirkungen auf das Dialogmarketing, 2016, S. 8; Drewes CR 2016, 725 f.; Buchner in Kühling/Buchner Art. 22 Rn. 26; Martini in Paal/Pauly Art. 22 Rn. 23; Schulz in Gola Art. 22 Rn. 28; zweifelnd Kamlah in Plath Art. 22 DSGVO Rn. 3; Taeger RDV 2017, 4.

653 Weichert in Reiffenstein/Blachek S. 250.

der Mortalität einschließen. Eine solche Verarbeitung von Gesundheitsdaten aus Gründen des öffentlichen Interesses darf nicht dazu führen, dass Dritte, unter anderem Arbeitgeber oder Versicherungs- und Finanzunternehmen, solche personenbezogene Daten zu anderen Zwecken verarbeiten."

„Eine auf einer derartigen Verarbeitung, einschließlich des Profilings, beruhende Entscheidungsfindung sollte allerdings erlaubt sein, wenn dies nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, dem der für die Verarbeitung Verantwortliche unterliegt, ausdrücklich zulässig ist, auch um im Einklang mit den Vorschriften, Standards und Empfehlungen der Institutionen der Union oder der nationalen Aufsichtsgremien Betrug und Steuerhinterziehung zu überwachen und zu verhindern und die Sicherheit und Zuverlässigkeit eines von dem Verantwortlichen bereitgestellten Dienstes zu gewährleisten, oder wenn dies für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und einem Verantwortlichen erforderlich ist oder wenn die betroffene Person ihre ausdrückliche Einwilligung hierzu erteilt hat" (ErwGr 71 S. 3 DSGVO).

Eine weitere Rechtfertigung besteht, wenn die automatisierte Entscheidung „für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist" (s. u. 8.10.2; Art. 22 Abs. 2 lit. a DSGVO).

8.10.1 Erlaubende Rechtsnormen

Für die nationale Normkonkretisierung der DSGVO bedarf es grds. keines formellen Gesetzes; ausreichend ist auch eine sonstige verbindliche, demokratisch legitimierte Rechtsvorschrift: „Wenn in dieser Verordnung auf eine Rechtsgrundlage oder eine Gesetzgebungsmaßnahme Bezug genommen wird, erfordert dies nicht notwendigerweise einen von einem Parlament angenommenen Gesetzgebungsakt; davon unberührt bleiben Anforderungen gemäß der Verfassungsordnung des betreffenden Mitgliedstaats. Die entsprechende Rechtsgrundlage oder Gesetzgebungsmaßnahme sollte jedoch klar und präzise sein und ihre Anwendung sollte für die Rechtsunterworfenen gemäß der Rechtsprechung des Gerichtshofs der Europäischen Union (im Folgenden „Gerichtshof") und des Europäischen Gerichtshofs für Menschenrechte vorhersehbar sein" (ErwGr 41 DSGVO). Bei Selbstregulierungsnormen bedarf es einer hoheitlichen Transformation.[654] Kollektivvereinbarungen können im Beschäftigtenkontext auf der Grundlage von Art. 88 Abs. 1 DSGVO Konkretisierungen vornehmen. Konkretisierende Verhaltensregeln können nur im Rahmen von Art. 40 DSGVO Verbindlichkeit entfalten.

Bei intensiven staatlichen Informationseingriffen bedarf es – im Sinne des Wesentlichkeitsprinzips – für jeden Zweck einer expliziten gesetzlichen Grundlage, so dass die „wesentlichen Entscheidungen" über das Verfahren der hoheitlichen

654 Martini in Paal/Pauly Art. 22 Rn. 34.

Entscheidungsfindung durch das Parlament selbst getroffen werden.[655] Angesichts der Offenheit der DSGVO empfiehlt sich eine normative Konkretisierung insbesondere im Hinblick auf spezifische Verantwortliche und die von diesen verfolgten Zwecke. Eine solche Konkretisierung kann durch Gesetz oder sonstige Rechtsvorschrift erfolgen. Eine weitere Möglichkeit der Festlegung besonderer Anforderungen besteht darin, dass Aufsichtsbehörden Kriterien für die Zertifizierung von automatisierten Entscheidungsverfahren nach Art. 42 Abs. 5 DSGVO festlegen. Explizit erwähnt ist die Konkretisierungsmöglichkeit durch den Europäischen Datenschutzausschuss (EDSA, Art. 70 Abs. 1 lit. f DSGVO). Konkretisierungen empfehlen sich insbesondere, wenn in einem Bereich Big-Data-Anwendungen weit verbreitet eingesetzt werden bzw. werden sollen. Beispiele hierfür sind Verfahren im Bereich der Qualitätssicherung, der Wirtschaftlichkeitskontrolle und der Risikobewertung im Gesundheitsbereich sowie der gesamte Bereich der wissenschaftlichen Forschung, etwa der medizinischen oder der genetischen Forschung.[656]

8.10.2 Erlaubende Verträge

Angesichts der Digitalisierung unserer Rechtsbeziehungen in allen Lebensbereichen nehmen automatisierte Entscheidungsverfahren in **Vertragsverhältnissen** zu. Dies gilt insbesondere für Internet-Aktivitäten von Betroffenen. So handelt es sich z. B. bei der Einrichtung eines Internet-Accounts und damit der Begründung eines Anbieter-Nutzer-Verhältnisses nach § 11 TMG i. d. R. um einen Vertragsabschluss[657], dem oft ein automatisiertes Entscheidungsverfahren zugrunde liegt. Dies ist der Fall, wenn von Seiten des Internetunternehmens nicht voraussetzungslos, sondern unter differenzierten Bedingungen eine vertragliche Bindung eingegangen wird. Dies gilt aber erst recht, wenn das „Ob" oder das „Wie" des Vertragsverhältnisses von einer komplexen Auswertung eines größeren, möglicherweise nicht mehr überschaubaren Datensets abhängig gemacht wird, bei der z. B. eine automatisierte Bonitätsüberprüfung durchgeführt wird.[658]

Zulässig sind nur solche automatisierten Entscheidungen, die „für den Abschluss oder die Erfüllung des Vertrags zwischen der betroffenen Person und dem Verantwortlichen **erforderlich**" sind (Art. 22 Abs. 2 lit. a DSGVO). Es muss einen unmittelbaren sachlichen Zusammenhang zwischen der Datenverwendung und dem konkreten Vertragszweck (Entscheidungs- oder Kalkulationsgrundlage) bestehen, wobei dieser sich auch auf Nebenabreden beziehen kann.[659] Im deutschen Datenschutzrecht gibt es die Erlaubnis für automatisierte Entscheidungen, wenn im Rahmen eines Rechtsverhältnisses dem **Begehren des Betroffenen stattgegeben** wird (§ 6a Abs. 2 Nr. 1 BDSGaF; spezifisch für Versicherungen künftig § 37 Abs. 1 Nr. 2 BDSGnF). Eine entsprechende Regelung ist in

655 Zum Technikrecht generell BVerfG 8.8.1978 – 2 BvL 8/77 (Kalkar), BVerfGE 49, 89 = NJW 1979, 359; zum Datenschutz BVerfG 15.12.1983 – 1 BvR 209/83 u. a. (Volkszählung), NJW 1984, 422.

656 Weichert in Reiffenstein/Blaschek S. 252.

657 Siehe den Überblick bei Schmitz in Hoeren/Sieber, Handbuch Multimedia Recht, 2014, Teil 16.2 Rn. 70 ff.

658 Weichert in Reiffenstein/Blaschek S. 253 f.

659 Martini in Paal/Pauly Art. 22 Rn. 31; Buchner in Kühling/Buchner Art. 22 Rn. 30.

Art. 22 DSGVO nicht ausdrücklich vorgesehen. Zumeist dürften in diesen Fällen die Voraussetzungen von Art. 22 Abs. 2 lit. a (Erfüllung eines Vertrages) vorliegen.

8.10.3 Komplexe Verarbeitungen ohne Entscheidungsrelevanz

Liegen die Voraussetzungen für die Anwendung des Art. 22 DSGVO nicht vor, so können Big-Data-Anwendungen dennoch zulässig sein, wenn mit ihnen **keine Entscheidung** mit Rechtswirkung oder einer erheblichen Beeinträchtigung verbunden ist. In diesem Fall kann die Verarbeitung generell durch Art. 6 DSGVO gerechtfertigt sein; erfolgt dabei eine Verarbeitung sensitiver Daten, so ist eine Rechtfertigung durch die in Art. 9 Abs. 2 DSGVO vorgesehenen Alternativen möglich.

8.11 Datengrundlagen

Die Nutzung der Daten für Big Data ist nur zulässig, wenn die **Verarbeitung dieser Daten für den Zweck** ohne Einsatz des Verfahrens auch zulässig wäre. Der Grundsatz der Zweckbindung (Art. 5 lit. b DSGVO, s. o. 8.6) sowie dessen materiell-rechtliche Konkretisierung (insbes. Art. 6 Abs. 1 lit. f, Abs. 4 DSGVO) bleiben bei Big Data neben der Geltung des Art. 22 DSGVO anwendbar. Verfügt also z. B. eine Stelle über Daten zweckgebunden für andere als Auskunftserteilungszwecke (etwa Voradressdaten zwecks Identifizierung) und dürften diese zu einer Selektion im Versicherungsbereich nicht übermittelt werden, so dürfen diese Daten auch nicht für die versicherungsmathematische Scoreberechnung verwendet werden.[660] Der Anwendbarkeit der Regelungen der DSGVO tut es keinen Abbruch, wenn neben den personenbezogenen Daten auch nicht-personenbezogene Merkmale in ein Big-Data-Verfahren mit einbezogen werden.

Für die Einbeziehung eines Datums in eine automatisierte Entscheidung genügt nicht die – evtl. nur gering ausgeprägte – statistische Signifikanz. Nötig ist vielmehr **Relevanz bzw. Plausibilität**, jedoch nicht Kausalität (s. o. 8.9.1).[661] Für Gesundheitsentscheidungen nicht relevant und daher unzulässig sind regelmäßig Angaben zu datenschutzrechtlichen Auskunftsanfragen, zu abgebrochenen Vertragsverhandlungen, zur Wohndauer, Nationalität, Bildungsabschluss, Geschlecht sowie Familienstand.[662]

Im deutschen Datenschutzrecht war bisher die Berechnung von Scores nach § 28b Nr. 3, 4 BDSGaF ausschließlich mit **Anschriftendaten** wegen der Gefahr einer scorebedingten Diskriminierung über die Wohnadresse verboten. Dieses Verbot besteht weiterhin, aber explizit nur in Bezug auf Vorgänge im Wirtschaftsverkehr (§ 31 Abs. 1 Nr. 3 BDSGnF). Dieses bleibt aber Ausdruck eines allgemein gültigen Grundsatzes, der auch im gesamten Gesundheitsbereich anwendbar ist. Gegen dieses Verbot wird auch verstoßen, wenn neben den Anschriftendaten noch andere Daten genutzt werden, diese aber nur mit einer

660 Weichert in Däubler u. a. § 28b Rn. 7.

661 ULD (2005) S. 74; Weichert, DuD 2006, 401 f.; a. A. Hoeren, RDV 2007, 97: mathematische Gesetzmäßigkeit genügt.

662 LfD Nds., XXI. TB 2011-2012, S. 51.

geringen Gewichtung für eine Entscheidung eingehen.[663] Ein solches datenspezifisches Nutzungsverbot enthält Art. 22 DSGVO zwar nicht. Die nationalen Gesetzgeber sind aber nicht gehindert, derartige Spezifizierungen vorzunehmen (vgl. Art. 22 Abs. 2 lit. b, 23 Abs. 1 DSGVO).[664]

Bei der Heranziehung der für die Analyse herangezogenen Daten müssen die Diskriminierungsverbote des Art. 21 GRCh (vgl. Art. 3 Abs. 3 GG) beachtet werden (s. o. 5.4, 6.14). Diese Grundregeln sind in Deutschland teilweise durch das Allgemeine Gleichbehandlungsgesetz (AGG) konkretisiert worden und müssen bei der Merkmalsauswahl beachtet werden.[665] Diskriminierungsverbote können sich auch aus anderen rechtlichen Regeln ergeben. So darf z. B. die Wahrnehmung von Datenschutzrechten nicht zu einer Beeinflussung der automatisierten Entscheidung führen (vgl. § 6 Abs. 3 BDSG-alt).

Werden bei automatisierten Entscheidungen sensitive Daten i. S. v. Art. 9 Abs. 1 DSGVO, also „besondere Kategorien personenbezogener Daten", einbezogen, so macht dies diese Entscheidungen gemäß Abs. 4 unzulässig, sofern nicht Art. 9 Abs. 2 lit. a od. g DSGVO anwendbar sind und angemessene Schutzmaßnahmen getroffen werden. Erlaubt sind diese Entscheidungen also nur bei ausdrücklicher Einwilligung der Betroffenen (lit. a), oder die Verarbeitung dient „einem erheblichen öffentlichen Interesse" (lit. g).

Durch spezifische Schutzmaßnahmen soll, so ErwGr 71 S. 6 DSGVO, verhindert werden, „dass es gegenüber natürlichen Personen aufgrund von Rasse, ethnischer Herkunft, politischer Meinung, Religion oder Weltanschauung, Gewerkschaftszugehörigkeit, genetischer Anlagen oder Gesundheitszustand sowie sexueller Orientierung zu diskriminierenden Wirkungen oder zu Maßnahmen kommt, die eine solche Wirkung haben." Eine wesentliche, aber nicht alleine ausreichende Schutzmaßnahme kann darin bestehen, dass die Verarbeitung ausschließlich von Personen vorgenommen wird, die einem Berufsgeheimnis unterliegen (Art. 9 Abs. 3 DSGVO).[666]

8.12 Datensparsamkeit

Im Datenschutzrecht gilt der Grundsatz der „Datenminimierung". Nach Art. 5 Abs. 1 lit. c DSGVO muss die Datenverarbeitung „dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein". Datensparsamkeit in zeitlicher Hinsicht wird zudem vom Grundsatz der „Speicherbegrenzung" nach Art. 5 Abs. 1 lit. e DSGVO gefordert. Danach müssen die Daten „in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist". Diese Grundsätze sind eine europäische Fortschreibung des § 3a BDSGaF („Datenvermeidung und Datensparsamkeit",

663 BT-Drs. 16/13219; ULD/GP Forschungsgruppe S. 38; Hammersen/Eisenried, ZD 2014, 343; a. A. wohl Ehmann in Simitis § 28 b Rn. 73; unklar Behm, RDV 2010, 70.

664 Weichert in Reiffenstein/Blaschke S. 256.

665 ULD (2005) S. 77; LfD Nds. RDV 2006, 132; a. A. Kamlah in Plath, BDSG, 2013,§ 28 b Rn. 27.

666 Weichert in Kühling/Buchner Art. 9 Rn. 132-148.

der folgenden Wortlaut hat: „Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen sind an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert."

Datensparsamkeit lässt sich dadurch realisieren, dass **schon bei der Datenerhebung** der Personenbezug beseitigt wird oder erhobene Rohdaten umgehend aggregiert und nur diese gespeichert oder weitergegeben werden. Eine spezifische Form der Datensparsamkeit besteht darin, dass erfasste Daten in einer realen oder virtuellen Blackbox oder zumindest nur auf dem Endgerät gespeichert werden.[667]

Für Big Data ist der Grundsatz der Datensparsamkeit **Erkenntnisgift**. Tatsächlich lässt sich der Widerspruch zwischen größtmöglichem mit Big Data verfolgtem Erkenntnisinteresse und Datensparsamkeit nicht völlig reibungs- und verlustfrei auflösen.[668] Ebenso wie es z. B. im Bereich strafrechtlicher Ermittlungen grundrechtlich bedingte Erkenntnisbeschränkungen gibt, gilt dies auch für die Erkenntnissuche mit Big Data.[669]

8.12.1 Anonymisierung

Anders als zuvor das bisherige BDSG (§ 3 Abs. 6 BDSGaF) definiert die DSGVO nicht den Begriff **Anonymisierung**. Bei der Anonymisierung erfolgt eine Veränderung personenbeziehbarer Daten, so dass ein Personenbezug überhaupt nicht mehr hergestellt werden kann, der Gehalt eines Datensatzes zu einer Person aber so weit wie möglich erhalten bleibt (vgl. § 16 Abs. 5 BStatG). Die Verarbeitung wirksam anonymisierter Daten ist datenschutzrechtlich nicht eingeschränkt: „Die Grundsätze des Datenschutzes sollten daher nicht für anonyme Informationen gelten, d. h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. Diese Verordnung betrifft somit nicht die Verarbeitung solcher anonymer Daten, auch für statistische oder für Forschungszwecke" (ErwGr 26 S. 5, 6 DSGVO). Es sind jedoch strenge Anforderungen bei der Frage anzulegen, wann ein Personenbezug (praktisch) nicht mehr hergestellt werden kann. Die verantwortliche Stelle trägt die Beweislast für eine ausreichende Anonymisierung.

Oft wird (juristisch unzutreffend) der Begriff „anonym" schon verwendet, wenn einfach die **Identifizierungsdaten weggelassen** werden. Dies kann im Interesse der Datensparsamkeit geboten sein, ohne dass aber dadurch zumeist eine ausreichende Anonymität entsteht.

667 Schaar in Stiftung Datenschutz (2017) S. 144.

668 Deutscher Ethikrat S. 16; Bergh/Brandner/Kutscha/Heinze/Schreiweis in Stiftung Datenschutz, S. 32 f.; Ladeur DuD 2016, 363.

669 Weichert in Langkafel S. 169 = DuD 2014, 836.

Erfolgt nur eine teilweise Anonymisierung, d. h. die Identifizierung wird erschwert, sie bleibt aber – z. B. für nähere Bekannte oder nur für Personen, die einer Verschwiegenheitspflicht unterliegen – möglich, erfolgt keine Anonymisierung; wohl kann hierin aber ein geringerer Eingriff in das Persönlichkeitsrecht liegen.[670]

Die Löschung der identifizierenden Stammdaten ist also eine notwendige, aber nicht hinreichende Bedingung für die Anonymisierung. Stammdaten können sich auf unterschiedliche Individuen und Institutionen beziehen, nicht nur auf den Betroffenen (Patienten, Probanden), sondern auch z. B. auf Gesundheitshelfer (Arzt, Apotheker, Psychologe) oder einen Dienstleister. Liegen bei einem Gesundheitshelfer die Stammdaten eines Betroffenen vor, so genügt regelmäßig eine Datenabfrage bei diesem, um eine Zuordnung eines scheinbar anonymisierten Datensatzes zur konkreten Person vorzunehmen. Deshalb genügt die Beseitigung der Patienten-Identifikatoren nicht; es bedarf vielmehr zur Anonymisierung auch der Beseitigung der Identifikatoren sämtlicher Helfer, Dienstleister oder sonstiger Dritter, bei denen Zuordnungswissen vorhanden ist.

Für die Wirksamkeit der Anonymisierung kommt es auf die Erkenntnisquellen an, die der speichernden Stelle als Zusatzwissen zur personenbezogenen Zuordnung direkt oder indirekt zur Verfügung stehen. [671] Für die Verfügbarkeit des Zusatzwissens genügt eine theoretische Möglichkeit. Nicht beachtlich ist, dass diese Möglichkeit nicht in Anspruch genommen werden soll oder will. Eine absolute Anonymisierung ist bei hochkomplexen und umfangreichen Datensätzen oft praktisch nicht möglich. Wenn das Zusatzwissen nur unter einem unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskraft beschafft werden kann, genügt dies für die Anonymisierung. Hierbei ist ein objektiver Maßstab anzulegen; nicht beachtlich ist, wenn der Aufwand nur für die speichernde Stelle unverhältnismäßig ist; auch das Interesse der Stelle ist nicht erheblich.[672] Es kommt also grds. nicht darauf an, wo durch wen und für welchen Zweck die Daten vorhanden sind, die eine Zuordnung wieder möglich machen. Es spielt auch grundsätzlich keine Rolle, dass der Zugriff auf diese Daten rechtlich geschützt und damit unzulässig ist.[673] Aufgrund von neuen Zuordnungstechniken können bisher als anonymisiert geltende Daten wieder zu personenbezogenen Daten werden.

Anonymisieren kann dadurch praktisch realisiert werden, dass die Identifikatoren eines Datensatzes gelöscht werden. Voraussetzung für eine wirksame Anonymisierung ist in diesen Fällen, dass die weiteren Merkmalsdaten einschließlich eines Identifikators nicht anderweitig verfügbar sind. Je mehr detaillierte Merkmale also in einem Datensatz

---

670 BVerfG 25.11.1999 – 1 BvR 348/98 u. 1 BvR 755/98, NJW 2000, 1859; BVerfG 29.4.1996 -. 1 BvR 1226/89, RDV 1996, 184 = DuD 1996, 566.

671 Anders noch BFH, NJW 1994, 2247 = RDV 1995, 32, der meinte, dass Reidentifizierbarkeit durch Branchenkenntnisse für eine Behandlung von Daten unschädlich ist.

672 Klar/Kühling in Kühling/Buchner Art. 4 Nr. 1 Rn. 32; a. A. Gola/Schomerus § 3 Rn. 44; Gola in Gola Art. 2 Rn. 11.

673 Weichert DuD 2013, 130; ders. in Langkafel S. 170 = DuD 2014, 836; a. A. EuGH 19.10.2016 – C-582/14, Rn. 49, NVwZ 2017, 213, 215.

verfügbar sind, umso größer ist das Re-Identifizierungsrisiko. Als Technik wird homomorphe Verschlüsselung (homomorphic encryption) eingesetzt, ein kryptografisches Verfahren, welches über Homomorphieeigenschaften verfügt, wodurch sich Berechnungen auf dem Geheimtext durchführen lassen, die mathematischen Operationen auf den entsprechenden Klartexten erfolgen. Mit funktionaler Verschlüsselung werden Daten in unterschiedliche Pakete zerlegt und die Analyse auf unterschiedlichen Ebenen durchgeführt, für die eine Entschlüsselung zugelassen wurde.[674]

Sicherer als die Methode der Anonymisierung eines individuellen Datensatzes ist die Methode der Aggregierung, d. h. des Zusammenführens mehrerer personenbeziehbarer Datensätze zu einem Gruppendatensatz, bei dem nicht mehr festgestellt werden kann, welcher Person in einem Kollektivdatensatz welche Merkmale zugeordnet sind. Bei der Merkmalsaggregierung werden spezifische Angaben zu einer Person (z. B. Alter 16 Jahre) durch Gruppenmerkmale (z. B. minderjährig) ersetzt; dadurch wird der Personenbezug aber nur gelockert, nicht aufgehoben. Entsprechendes gilt für das gezielte Einführen von Merkmalsfehlern (Hinzufügung von Dummy-Datensätzen) oder das Vertauschen von Daten. Um eine effektive Anonymisierung zu erreichen, ist zumeist eine Kombination beider Vorgehensweisen notwendig.[675] Der Einsatz eines Trustcenters genügt nicht für eine Anonymisierung, wenn dem Trustcenter die Re-Identifizierung möglich ist.[676] Aufgrund der verwendeten Technik und der eingesetzten Verfahren darf keine Partei mehr in der Lage sein, eine Person aus dem Datenbestand herauszugreifen, eine Verbindung zwischen zwei Datensätzen eines Datenbestandes oder zwischen zwei unabhängigen Datenbeständen herzustellen oder durch Inferenz Informationen aus einem solchen Datenbestand abzuleiten.[677]

Zur Feststellung hinreichender Aggregierung von Datensätzen wird das Modell der K-Anonymität verwendet. K-Anonymität ist verwirklicht, wenn die identifizierenden Informationen jedes einzelnen Individuums von mindestens k-1 anderen Individuen ununterscheidbar sind, so dass eine korrekte Verknüpfung mit den zugehörigen Attributen erschwert wird. Der Buchstabe „K" ist also ein Parameter, der hinsichtlich einer konkreten Anwendung durch eine natürliche Zahl besetzt wird. Bei einem definierten Datenbestand ist eine Person in einem Datenbestand von mindestens k Personen „versteckt". Je größer K ist, desto sicherer ist die Anonymisierung.[678]

---

674 Ladeur DuD 2016, 363.

675 Ladeur DuD 2016, 363; Schneider S. 22 f.; Weichert in Langkafel S. 170 = DuD 2014, 836; Deutscher Ethikrat S. 66; Thielicke, Big Data in der Medizin: Quadratur des Kreises, www.heise.de 4.10.2017 beschreibt ein vom Start-up Statice entwickeltes Verfahren.

676 Dammann in Simitis, § 3 Rn. 205 ff.; Weichert, DuD 2013, 130; Kühling/Klar, NJW 2013, 3601 kritisieren die Unbestimmtheit des Begriffs.

677 Artikel-29-Datenschutzgruppe, Stellungnahme 5/2014 zu Anonymisierungstechniken.

678 K-Anonymität, de.wikipedia.org, abgerufen am 20.11.2017; Schneider S. 21; 23. TB LDI NRW 2017, Kap.13.2 (S. 100).

8.12.2 Pseudonymisierung

Art. 4 Nr. 5 DSGVO regelt die „Pseudonymisierung“ als „die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden“.

Der mit § 3 Abs. 6a BDSGaF im Jahr 2001 eingeführte Begriff des Pseudonymisierens (vgl. § 15 Abs. 3 TMG) stellte noch darauf ab, dass der Name oder andere Identifikationsmerkmale durch ein Kennzeichen ersetzt werden. Dem gegenüber ist der Begriff in der DSGVO weiter. Es wird nicht mehr unterschieden zwischen Identifikatoren, die ersetzt werden, und Attributen. Jede Veränderung eines Datensatzes genügt, welche die Zuordnung zu einer natürlichen Person erschwert, wenn über zusätzliche Informationen die Zuordnung wieder hergestellt werden kann. Damit kann eine Pseudonymisierung auch über Attribute erfolgen. Letztlich ist auch eine rückholbare Verschlüsselung eines Datensatzes ein Pseudonymisieren i. S. d. DSGVO.

„Einer Pseudonymisierung unterzogene personenbezogene Daten, die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten, sollten als Informationen über eine identifizierbare natürliche Person betrachtet werden“ (ErwGr 26 S. 2 DSGVO). Dies bedeutet, dass bzgl. der pseudonymisierten Daten sämtliche Betroffenenrechte gelten, wenn die Zuordnung tatsächlich möglich ist.[679] Pseudonymisierung dient ebenso wie die Anonymisierung der Datenminimierung (Art. 5 lit. c, 89, ErwGr 156 S. 3 DSGVO) und der datenschutzfreundlichen und sicheren Technikgestaltung (vgl. Art. 25 Abs. 1, 32 Abs. 1 lit. a DSGVO). Dadurch werden Datenschutz durch Technik (data protection by design) und datenschutzfreundliche Voreinstellungen (data protection by default) unterstützt (ErwGr 78 S. 2 DSGVO).

Zuordnungsfunktionen ermöglichen, im Nachhinein Datensätze, die sich auf eine Person beziehen, zusammenzuführen.[680] Pseudonymisierte sind weiterhin personenbezogene Daten, so dass deren Verarbeitung dem Datenschutzrecht unterliegt.[681] Die Pseudonymisierung verfolgt das Ziel, die Kenntnis der Identität der Betroffenen während der Verarbeitung zu verhindern, wenn diese Kenntnis nicht erforderlich ist.

Die Vergabe des Pseudonyms kann durch die betroffene Person selbst erfolgen (selbst generiert), durch einen vertrauenswürdigen Dritten, der über die Zuordnungsregel verfügt (Treuhänder, trusted third party, z. B. pseudonymisierter Signaturschlüssel nach § 7 SignaturG) oder durch die verantwortliche Stelle. In den letzten beiden Fällen wird unterschieden zwischen Referenz-Pseudonymen (Referenzliste) und Einweg-

679 A. A. Wohlgemuth/Gerloff, Datenschutzrecht, 3. Aufl. 2005, S. 30.
680 Roßnagel/Scholz MMR 2000, 721.
681 Karg DuD 2015, 524; Klar/Kühling in Kühling/Buchner Art. 4 Nr. 5 Rn. 11.

Pseudonymen, die mithilfe von (geheimen) mathematischen Algorithmen erstellt werden. Das Erschweren der Identifizierung sollte bei Fehlen der Zuordnungsfunktion zur Anonymisierung führen. Leicht identifizierbare Chiffren (z. B. Namensbestandteile verbunden mit Geburtsdatum) genügen für eine wirksame Pseudonymisierung i. d. R. nicht.

Eine Pseudonymisierung von einzelnen Personen zuordenbaren Stammdaten genügt für den Ausschluss einer Reidentifizierung, also einer wirksamen Anonymisierung, regelmäßig nicht, insbesondere nicht, wenn die Pseudonyme zur Zuordnung von Individualdatensätzen genutzt werden. An diesem Befund ändert sich auch nichts dadurch, dass für diese Pseudonymisierung Hash-Verfahren oder asymmetrische Verschlüsselungsverfahren unter Löschung des zweiten Teils des Schlüsselpaares verwendet werden. Eine Reidentifizierung ist in diesen Fällen z. B. dadurch möglich, dass ursprüngliche Stammdaten gemäß diesem Pseudonymisierungsverfahren verändert werden und die pseudonymisierten Daten mit den angeblich anonymisierten Daten abgeglichen werden. Dabei genügt es bei persistenten Verschlüsselungs- und Hashverfahren auch nicht, dass diese vom Verantwortlichen geheim gehalten werden, da auch eine unzulässige Schlüsselbeschaffung keinen unverhältnismäßigen Aufwand darstellen muss.[682]

Eine Pseudonymisierung führt nicht dazu, dass das Datenschutzrecht nicht mehr anwendbar ist. Wohl aber kann sie dazu führen, dass eine Datenverarbeitung, z. B. im Rahmen von Big Data, datenschutzkonform wird, weil die Bestimmung der Betroffenen derart erschwert wurde, dass deren schutzwürdige Interessen nicht mehr gegenüber den berechtigten Verarbeitungsinteressen überwiegen. Ein derartiger Schutz kann insbesondere dadurch erreicht werden, dass nicht nur eine einmalige Pseudonymisierung erfolgt, sondern, z. B. im Rahmen eines Biobank-Verfahrens, die individualisierenden Daten bei der Speicherung sowie bei den jeweiligen weiteren Verarbeitungsschritten erneut pseudonymisiert werden. Die Zuordnungen zwischen den jeweiligen zu den Personendatensätzen gehörenden Pseudonymen werden in einem geregelten Verfahren einzelfallbezogen ermöglicht, nachdem die Rechtmäßigkeit der jeweiligen Verarbeitungen überprüft und freigegeben wurde. Die Auswertungen müssen dabei in einem geschützten und kontrollierten Raum erfolgen, bei dem insbesondere die Pseudonymzuordnungen und die Ausgabe der Analyseergebnisse einer spezifischen Kontrolle bedürfen. Dabei können komplexe technische Verfahren verwendet werden, über die rollen- und zweckspezifisch definierte Pseudonymverknüpfungen erlaubt, andere aber sicher ausgeschlossen werden.[683]

---

682 Weichert in Langkafel S. 170 = DuD 2014, 836 mit Verweis in Fn. 64 auf den Konflikt über die Pseudonymisierung von Apothekenabrechnungsdaten zwischen dem ULD und dem BayLDA; dazu auch Kauss in Plöse/Fritsche/Kuhn/Lüders, „Worüber reden wir eigentlich?“ Festgabe für Rosemarie Will, 2016, S. 597-602.

683 Weichert in Langkafel S. 171 = DuD 2014, 836 f.; ULD (2009) S. 52 ff.

8.13 Richtigkeit

Gemäß Art. 5 Abs. 1 lit. d DSGVO haben personenbezogene Daten generell „sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein.[684] Es sind angemessene Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden“. Die Regelung deutet darauf hin, dass es keine objektive Richtigkeit gibt, sondern dass diese im Zusammenhang mit dem jeweils verfolgten Zweck gesehen werden muss. So besteht im ärztlichen Bereich eine Dokumentationspflicht, die eine Berichtigung im Sine einer Löschung inhaltlich falscher Daten verbietet, da der Zweck der ärztlichen Dokumentation die Beweissicherung ist. Auch wenn die darin enthaltenen Fakten unzutreffend sind, bleibt es zutreffend, dass sie so vom Arzt dokumentiert wurden.[685] Die Daten in der ärztlichen Dokumentation entsprechen oft nicht denen der für die Abrechnung herangezogenen Codierung gemäß dem International Code of Diseases (ICD). Hierbei sind u. a. von der Gebührenordnung bedingte Pauschalierungen bestimmend.[686]

Eine spezifische Eigenschaft von Big Data besteht darin, dass die Anwendung dieser Technik nicht von formellen oder inhaltlichen Vorgaben, etwa von Formaten, Schnittstellen oder Standards abhängig sein soll. Dessen ungeachtet sind aber solche Vorgaben nützlich und evtl. gar unabdingbar, wenn es auf die Exaktheit und Zuverlässigkeit von Auswertungsergebnissen ankommt.

Bei der Zusammenführung von Gesundheitsdaten über Big Data müssen die jeweiligen Kontexte und Erhebungszwecke berücksichtigt werden, um keine falschen Ergebnisse zu erlangen. Diese Umstände sind oft selbst nicht digital erfasst und müssen daher für valide Big-Data-Analysen digital ergänzt werden. Wegen der hohen Komplexität der Sachverhalte und der gegenseitigen Abhängigkeiten kann ohne eine solche Kontextualisierung Big Data im Gesundheitsbereich keinen Erfolg bringen.

Bei Big Data spielt für die Richtigkeit neben der Datenqualität, also der Richtigkeit der eingeführten Einzeldaten, auch deren Repräsentativität eine zentrale Rolle. Werden dann die (anonymen) Big-Data-Ergebnisse wieder einzelnen Personen zugeordnet, so hat die Repräsentativität nicht nur eine wissenschaftliche, sondern auch in Bezug auf die Richtigkeit datenschutzrechtliche Relevanz (vgl. § 31 Abs. 1 Nr. 2 BDSGnF).

Wegen der Verteiltheit der Verantwortungen bei komplexem Big Data und im Interesse hoher Korrektheit bei medizinischen Anwendungen können quellenübergreifende Qualitätssicherungsmaßnahmen von hoher Bedeutung sein, etwa in Form der Einrichtung

684 Zur Sanktionierbarkeit Hoeren ZD 2016, 462.
685 Däubler in Däubler u. a. § 35 Rn. 9; Brink in Wolff/Brink § 35 Rn. 15.
686 Kamps in Langkafel S. 76.

von Datenprüfern[687] oder der Durchführung von Stichprobenkontrollen, Audits oder Evaluationen.[688]

Gemäß den §§ 136a, 136b SGB V definiert der G-BA, welche Anforderungen an ein einrichtungsinternes Qualitätsmanagement zur Sicherstellung der Richtigkeit von Daten gestellt werden sollen (s. o. 4.2). Er bestimmt auch die Kriterien für die indikationsbezogene Notwendigkeit und Qualität der durchgeführten diagnostischen und therapeutischen Leistungen, insbesondere aufwendiger medizintechnischer Leistungen.

Handelt es sich bei den Gesundheitsdaten um Ergebnisse aus Laboruntersuchungen, so ist deren Richtigkeit davon abhängig, dass diese den wissenschaftlichen und fachlichen Anforderungen genügen. Es gilt die Pflicht zur Qualitätssicherung nach § 135a SGB V. Bei medizinischen Laboruntersuchungen soll die Qualität dadurch hergestellt werden, dass die durchführenden Labore und die eingesetzten Analyseverfahren ein Akkreditierungsverfahren bei der Deutschen Akkreditierungsstelle (DAkkS) durchlaufen müssen. Prüfungsmaßstand ist bei medizinischen Laboratorien DIM EN ISO 15189. Weiterhin anwendbar ist die „Richtlinie der Bundesärztekammer zur Qualitätssicherung laboratoriumsmedizinischer Untersuchungen". Es hat sich gezeigt, dass bei Laboruntersuchungen mit kleinen Fallzahlen gravierende Richtigkeitsdefizite entstehen können.[689]

Die Richtigkeit von Gesundheitsdaten ist eine Grundbedingung für das Vertrauensverhältnis zwischen medizinischen Leistungserbringern und Patienten. Diese bezieht sich zunächst auf die in die Diagnose und Behandlung einfließenden Behandlungsdaten, dann aber auch auf die Diagnose und die Behandlung selbst. Durch die Verfügbarkeit von Gesundheitswissen im Internet kommt es für die Vertrauensbeziehung auf größtmögliche Transparenz und offene Kommunikation an, zumal die Qualität des im Internet verfügbaren Wissens und die korrekte Interpretation oft nicht gewährleistet sind. Insofern sind vertrauenswürdige unabhängige Informationsplattformen von Bedeutung. Hierzu gezählt werden die Angebote von gesundheitsinformation.de, ebm-netzwerk.de, cochrane.de oder igel-monitor.de.[690]

8.14 Gemeinwohlorientierte Privilegierungen

In Art. 89 Abs. 1 DSGVO sind zweckbezogen rechtliche Privilegierungen der personenbezogenen Datenverarbeitung vorgesehen. Vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von der DSGVO zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, gilt dies für die Verarbeitung ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke. Die

687 Deutscher Ethikrat S. 184.
688 Deutscher Ethikrat S. 107.
689 Rili-BÄK, August 2014, Deutsches Ärzteblatt v. 19.9.2014, A 1583; kritisch zur Praxis in einem konkreten Fall Bernd/Braun, Blutsbande, SZ 10.1.2018, 3.
690 Bartens, Google dich gesund, SZ 27./28.1.2018, 33.

Privilegierungen bzw. die Zulassung von Ausnahmen zu Datenschutzgrundsätzen beziehen sich auf den Grundsatz der Speicherbegrenzung (Art. 5 Abs. 1 lit. e DSGVO), auf den Grundsatz der Zweckbindung (Art. 5 Abs. 1 lit. b DSGVO) und auf Schutzvorkehrungen bei der Verarbeitung sensitiver Daten, also z. B. von Gesundheitsdaten (Art. 9 Abs. 2 lit. j DSGVO). Nach Art. 14 Abs. 5 lit. b DSGVO ist der Verantwortliche unter bestimmten Voraussetzungen von Informationspflichten gegenüber den Betroffenen befreit. Entsprechendes gilt für die Löschungspflicht nach Art. 17 Abs. 3 lit. d DSGVO. Art. 89 Abs. 2, 3 DSGVO sieht weitere Ausnahmen in Bezug auf die Betroffenenrechte auf der Grundlage des Unions- oder des mitgliedsstaatlichen Rechts vor.[691] Die §§ 27, 28 BDSGnF greifen diese Öffnungsklausel auf und setzen sie um.

8.15 Weitere nationale Regelungen zur Vertraulichkeit

Das Datenschutzrecht ist für die persönlichkeitsrechtliche Bewertung von Big Data im Gesundheitsbereich von zentraler, aber nicht ausschließlicher Bedeutung. Anwendbar sind vielmehr weitere Regelungen, deren Funktion zumeist darin besteht, das Schutzniveau für die Betroffenen weiter zu erhöhen. Dabei gibt es keine klare Trennung zwischen öffentlichem, Zivil- und Strafrecht, was die Rechtsanwendung nicht einfach macht. Es bedarf oft im Sinne der **Einheit der Rechtsordnung** eines Rückgriffs auf mehrere Rechtsgebiete, um einen Sachverhalt adäquat zu bewerten.

8.15.1 Berufliche Schweigepflicht

Die auf den hippokratischen Eid zurückgehende, verfassungsrechtlich begründete berufliche bzw. ärztliche Schweigepflicht (s. o. 6.8) hat inzwischen in vieler Hinsicht Eingang ins deutsche und ins europäische Recht gefunden. § 203 Abs. 1, 3, StGB stellt die ungerechtfertigte Offenbarung beruflicher Helfer, vom Arzt über den Apotheker bis zum staatlichen Sozialarbeiter, sowie von deren Hilfspersonen unter Strafe. In den Berufsordnungen der Heilberufskammern wird das **Patientengeheimnis** als Standesrecht anerkannt und Verstöße hiergegen mit Sanktionen bedroht. Die rechtliche Bedeutung der beruflichen Schweigepflicht liegt weniger in ihrer strafrechtlichen Sanktionierung. Als Patienten- bzw. Berufsgeheimnis ist die Schweigepflicht Ausdruck einer allgemeinen Wertentscheidung in der deutschen Rechtsordnung, die im Rahmen des Vertraulichkeitsschutzes generell zu beachten ist. Sie wird weltweit anerkannt und hat in die europäische Rechtsordnung umfassend Eingang gefunden (z. B. Art. 9 Abs. 3 DSGVO).

Dieser Hilfeschutz in Kombination mit dem erhöhten Schutz sensitiver Daten (s. o. 2.1) findet seine Konkretisierung in einer Vielzahl von medizinischen Spezialgesetzen, so z. B. in den Krankenhausgesetzen, den Gesundheitsdienstgesetzen, den Krebsregistergesetzen sowie im Gendiagnostikgesetz (GenDG), Infektionsschutzgesetz (InfSchG) und Arzneimittelgesetz (AMG). Dabei ist der Schutz informationeller Selbstbestimmung nur ein Aspekt einer umfassender zu verstehenden **medizinischen Selbstbestimmung**, die nicht nur ein Bestimmungsrecht über die eigenen Gesundheitsdaten begründet, sondern auch über

691 Buchner/Tinnefeld in Kühling/Buchner Art. 89 Rn. 2.

den Umgang mit dem eigenen Körper. Es schließt die medizinische Wahlfreiheit des Patienten mit der freien Arztwahl (vgl. § 76 SGB V) mit ein.[692]

8.15.2 Sozialgeheimnis

Berufsgeheimnis i. S. v. Art. 9 Abs. 3 DSVGO ist auch das **Sozialgeheimnis** nach § 35 SGB I.[693] Dieses verpflichtet alle Sozialleistungsträger bei der Verarbeitung von Sozialdaten nach § 67 Abs. 1 SGB X. Während die klassischen Berufsgeheimnisse an einer personalen Vertrauensbeziehung anknüpfen, wird das Sozialgeheimnis durch die Verarbeitung der sensitiven Sozialdaten bei einem über Gesetz zur Vertraulichkeit verpflichteten Sozialleistungsträger bzw. durch dessen Mitarbeiter begründet. Zusätzlich differenziert das SGB zwischen Sozialdaten generell und „besonders schutzwürdigen Sozialdaten" (z. B. in § 76 SGB X, ähnlich § 65 SGB VIII). Das Sozialgeheimnis will Geheimnisse in vergleichbarem Maße institutionell wie personale Berufsgeheimnisse schützen, wenn sie den personalen Bereich der schweigepflichtigen Geheimnisträger verlassen und z. B. zu Zwecken der Abrechnung von einer Krankenkasse oder einer Kassen(zahn)ärztlichen Vereinigung oder zu Zwecken der behördlichen Aufsicht von einer nicht selbst berufsbedingt schweigepflichtigen Kontrollinstanz verarbeitet werden.[694] Das nach deutschen Recht durchregulierte Sozialgeheimnis erstreckt sich auch auf das bei Leistungsträgern tätige administrative oder technische Hilfspersonal und auf Auftragsverarbeiter (§ 80 SGB X). Die Geheimhaltung muss sich am gesundheitlichen Verarbeitungszweck orientieren. Bei Verstößen sind Sanktionen vorgesehen (§§ 85, 85a SGB X).

8.16 Transparenz

Art. 5 Abs. 1 lit. a DSGVO sieht vor, dass personenbezogene Daten „in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden" müssen. Dieser zentrale Rechtsgrundsatz wird in Erwägungsgrund 39 S. 2-5 DSGVO erläutert: „Für natürliche Personen sollte Transparenz dahingehend bestehen, dass sie betreffende personenbezogene Daten erhoben, verwendet, eingesehen oder anderweitig verarbeitet werden und in welchem Umfang die personenbezogenen Daten verarbeitet werden und künftig noch verarbeitet werden." Der Grundsatz der Transparenz setzt voraus, dass alle Informationen und **Mitteilungen zur Verarbeitung dieser personenbezogenen Daten** leicht zugänglich und verständlich und in klarer und einfacher Sprache abgefasst sind.[695] Der Grundsatz betrifft insbesondere die Informationen über die Identität des Verantwortlichen, die Zwecke der Verarbeitung und sonstige Informationen, die eine faire und nachvollziehbare Verarbeitung im Hinblick auf die betroffenen natürlichen Personen gewährleisten, sowie deren Recht, eine Bestätigung und Auskunft darüber zu erhalten,

692 Weichert in Langkafel S. 163 = DuD 2014, 832.

693 Konferenz der Datenschutzbeauftragten des Bundes und der Länder DANA 2016, 76; unklar Kircher in Kingreen/Kühling, 208 f.; a. A. zu Art. 8 Abs. 3 DSRL Meier Der rechtliche Schutz patientenbezogener Gesundheitsdaten, 2003, S. 66.

694 Rehborn in Prütting MBOÄ § 9 Rn. 1.

695 Zur Verbrauchertransparenz Müller in Stiftung Datenschutz (2017) S. 116 ff.

welche sie betreffende personenbezogene Daten verarbeitet werden. Natürliche Personen sollten über die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten informiert und darüber aufgeklärt werden, wie sie ihre diesbezüglichen Rechte geltend machen können.

Ohne Transparenz darf Big Data mit sensitiven Daten angesichts der individuellen und gesellschaftlichen Risiken nicht realisiert werden. Diese Transparenz muss sich auf **alle wesentlichen Aspekte der Datenverarbeitung** beziehen: Rechtsgrundlagen, Organisation, Verfahrensabläufe, technische Dokumentation, Daten-, Datensicherheits- und Datenschutzmanagement.[696]

Dem Transparenzgebot wird nicht schon dadurch entsprochen, dass relevante Informationen zur Verfügung gestellt werden. Vielmehr verlangt die DSGVO, dass dies „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer **klaren und einfachen Sprache**" erfolgt (Art. 12 Abs. 1 S. 1 DSGVO). Angesichts der Komplexität von informationstechnischen Verfahren setzt dies zum einen eine Reduzierung auf das Wesentliche für den Betroffenen voraus wie auch die Möglichkeit der Hinterfragung und Beratung durch Experten im Auftrag oder im Interesse der Betroffenen. Im Gesundheitsbereich sind insofern nicht nur technische, sondern auch medizinische Experten gefordert.[697]

8.16.1 Transparenzpflichten bei automatisierten Entscheidungen

Die Umsetzung der **Informationspflichten** nach Art. 13 Abs. 2 lit. f, 14 Abs. 2 lit. g DSGVO bei automatisierten Entscheidungen nach Art. 22 DSGVO ist eine unabdingbare Maßnahme zur Wahrung der Rechte der Betroffenen. Die Betroffenen haben einen Anspruch darauf, zu erfahren, dass überhaupt eine automatisierte Entscheidung erfolgt wie auch darauf, Logik, Tragweite und angestrebte Auswirkungen zu kennen. Auch diese Informationen müssen präzise, transparent, verständlich, leicht zugänglich und in klarer einfacher Sprache erteilt werden (Art. 12 Abs. 1 DSGVO). Informations- und Benachrichtigungspflichten stoßen bei Big-Data-Anwendungen an praktische Grenzen, da Zuordnungen und Zwecke oft nicht hinreichend bestimmt bzw. bestimmbar sind.[698] Eine Entbindung von den Transparenzpflichten gegenüber den Betroffenen erlaubt die DSGV nach Art. 11 Abs. 1 aber nur, soweit die für die Identifikation nötigen Informationen nicht verfügbar sind.[699]

Ein zentraler Schwerpunkt von Schutzmaßnahmen liegt in der Herstellung von Verarbeitungs- und Verfahrenstransparenz (Art. 13 Abs. 2 lit. f, 14 Abs. 2 lit. g, 15 Abs. 1 lit. h DSGVO). Die Information über die „involvierte **Logik**" gilt nicht dem Quellcode, fordert

696 Weichert ZD 2013, 257 f.; Münch S. 137 ff.
697 Deutscher Ethikrat S. 94.
698 Werkmeister/Brandt CR 2016, 236.
699 Weichert in Kühling/Buchner Art. 11 Rn. 13-15.

aber eine Offenlegung der relevanten Informationen zu zugrunde liegenden Algorithmen in Bezug auf die individuelle Berechnung.[700]

8.16.2 Begrenzungen der Transparenz

Diesen Transparenzansprüchen wird von Seiten der Verantwortlichen nicht selten entgegengehalten, es müssten Betriebs- und Geschäftsgeheimnisse offenbar werden (s. o. 9.2).[701] Der deutsche Bundesgerichtshof (BGH) hat diese Argumentation gebilligt und mit der Behauptung gestützt, die Interpretation personenbezogener Daten durch Algorithmen, etwa durch ein Scoring-Verfahren, sei durch die Meinungsfreiheit (Art. 5 GG, vgl. Art. 11 GRCh) geschützt.[702] Eine derartige Argumentation ist mit der DSGVO nicht mehr haltbar. Computerentscheidungen genießen keinen Schutz durch die Meinungsfreiheit (s. o. 6.9).[703] Aber auch bei der Abwägung des Eigentumsschutzes des Verantwortlichen mit dem Grundrecht auf Datenschutz muss im Hinblick auf die konkreten personenbezogenen Verarbeitungen und deren Ergebnisse dem Datenschutz generell der Vorrang eingeräumt werden.

Im Erwägungsgrund 63 S. 5 u. 6 DSGVO heißt es zum Transparenzanspruch der Betroffenen: „Dieses Recht sollte die Rechte und Freiheiten anderer Personen, etwa Geschäftsgeheimnisse oder Rechte des geistigen Eigentums und insbesondere das Urheberrecht an Software, nicht beeinträchtigen. Dies darf jedoch nicht dazu führen, dass der betroffenen Person jegliche Auskunft verweigert wird.“ Hieraus kann nicht geschlossen werden, dass Betriebs- und Geschäftsgeheimnisse den Auskunftsanspruch verdrängen können[704], sondern nur, dass insofern eine Abwägung erfolgen muss, bei der die Grundrechte von Betroffenen (insbes. Art. 8 GRCh) und der verarbeitenden Stellen (insbes. Art. 17 GRCh) einfließen müssen. Für die Betroffenenrechte ist nicht der Quellcode relevant, sondern die Merkmalsgewichtung, die wiederum schwerlich zum überwiegenden Geheimnis deklariert werden kann. Rechtswidrige Datenverarbeitung kann in jedem Fall keinen Geheimnisschutz genießen.[705] Die Offenlegungspflichten gegenüber dem Betroffenen müssen so weit gehen, wie dies für die Feststellung der Rechtmäßigkeit der Datenverarbeitung nötig ist (Art. 19 Abs. 4 GG, Art. 47 GRCh).

Transparenz bedeutet Durchschaubarkeit und daraus folgend Verstehbarkeit für alle Beteiligten. Sie muss nicht nur zugunsten des Betroffenen bestehen, sondern auch zugunsten der staatlichen Aufsicht, der gerichtlichen Kontrolle, evtl. der parlamentarischen Kontrolle, bei gesellschaftlich relevanten sensitiven Anwendungen wie Big Data im Gesundheitsbereich zugunsten der Öffentlichkeit bzw. der (wissenschaftlichen) Fachöffentlichkeit.

---

700 Roßnagel/Nebel/Richter ZD 2015, 458; a. A. Martini in Paal/Pauly Art. 22 Rn. 36.

701 Zur Definition Schnabel CR2016, 343 f.

702 BGH 28.1.2014 – VI ZR 156/13, NJW 2014, 1235; Buchner in Kühling/Buchner Art. 22 Rn. 35; dagegen ausführlich zu Recht ULD/GP Forschungsgruppe S. 44 ff.

703 Weichert ZRP 2014, 168 ff.

704 So aber wohl Buchner in Kühling/Buchner Art. 22 Rn. 35.

705 Schnabel CR 2016. 345 f.

Das Erfordernis richtet sich an den **Verantwortlichen** und ist für diesen eine grundlegende Voraussetzung für die Wahrnehmung der eigenen Verantwortlichkeit (Art. 5 Abs. 2 DSGVO). Angesichts der Komplexität von Big Data, insbesondere beim Einsatz von Künstlicher Intelligenz, und der hierbei oft erfolgenden Arbeitsteilung verschiedener Stellen müssen diese ein ureigenes Interesse haben, das Gesamtverfahren und ihren Part dabei zu überschauen und bewusst verantworten zu können.

Eine spezielle Transparenzpflicht besteht in qualifizierten **Kontroll- und Genehmigungsverfahren**, also z. B. gegenüber Ethik-Kommissionen (§ 15 MBOÄ)[706], Datenschutzbeauftragten (Art. 37 ff. DSGVO), den Datenschutzaufsichtsbehörden (Art. 51 ff DSGVO) sowie sonstigen Stellen, die für die Kontrolle, Genehmigung oder für die Zertifizierung bzw. Auditierung von Verfahren oder Produkten zuständig sind.

Transparenzdefizite sind bei der Verarbeitung von Gesundheitsdaten, insbesondere bei Big-Data-Anwendungen weit verbreitet. Eine koordinierte Prüfung der Datenschutzaufsichtsbehörden des Bundes und der Länder im Jahr 2016 bei verschiedenen Anbietern von Gesundheits-Apps zeigte, dass Hersteller, Betreiber und Verkäufer die Nutzenden nicht ausreichend darüber informieren, was mit deren Daten passiert. Die meisten Datenschutzerklärungen erfüllten mangels Verständlichkeit und Bestimmtheit die gesetzlichen Anforderungen nicht. Besonderes Augenmerk muss danach zudem auf die Information über die Datensicherheit und auf die Weitergabe und die Speicherdauer der sensitiven Daten gelegt werden.[707] Die Verbraucherzentrale Nordrhein-Westfalen startete daraufhin eine Abmahnkampagne wegen der ungenügenden Information der Nutzenden durch Anbieter von Fitnessarmbändern, Computeruhren und entsprechender Apps. Betroffene Firmen waren Apple, Garmin, Fitbit, Jawbone, Polar, Runtastic, Striiv, Under Armour und Withings.[708]

8.17 Auskunftsansprüche der Betroffenen

Gemäß Art. 8 Abs. 2 S. 2 GRCh hat jeder Mensch das Recht, Auskunft über die ihn betreffenden erhobenen Daten zu erhalten. Dieser Anspruch ist **einfachgesetzlich** bisher u. a. in den §§ 19, 34 BDSGaF geregelt. Von Mai 2018 an gilt Art. 15 DSGVO. Nach Art. 15 Abs. 1 DSGVO erstreckt sich der Auskunftsanspruch auf die Daten selbst sowie auf die Verarbeitungszwecke (lit. a), die verarbeiteten Datenkategorien (lit. b), die Empfänger bzw. Empfängerkategorien (lit. c), falls möglich die Speicherdauer (lit. d), die Betroffenenrechte (lit. e u. f), die Datenherkunft (lit. g) sowie bei einer Verarbeitung nach Art. 22 DSGVO auf „aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen“ (s. o. 8.16.1) für den Betroffenen.

Dieser Auskunftsanspruch wird oft als die **„Magna Charta“ des Datenschutzes** bezeichnet, weil die Auskunft über die verarbeiteten Daten die Grundlage für die Umsetzung

706 Schneider S. 295 ff.
707 Raum in Stiftung Datenschutz (2017) S. 130 f.
708 Abmahnung wegen Daten, SZ 27.04.2017, 20.

sämtlicher weiterer Betroffenenrechte (Berichtigung, Löschung, Verarbeitungsbeschränkung/Sperrung, Widerspruch usw.) ist.[709]

Gemäß Art. 23 DSGVO haben die Mitgliedstaaten die Möglichkeit, für bestimmte genannte Zwecke im Rahmen einer Interessenabwägung **Beschränkungen des Auskunftsrechts** vorzusehen, sofern dabei der Wesensgehalt der Grundrechte und Grundfreiheiten gewahrt wird. Werden beim Abschluss von Verträgen mit dem Betroffenen Allgemeine Geschäftsbedingungen eingesetzt (AGB, §§ 305 ff. BGB), so kann hierüber nicht, ebenso wenig wie über eine individualvertragliche Regelung, der Auskunftsanspruch abbedungen werden (vgl. § 6 Abs. 1 BDSGaF).

Das Auskunftsrecht im Rahmen von **Big Data im Gesundheitsbereich** ist für den Betroffenen von besonderer Bedeutung wegen der hohen Sensitivität der Daten sowie wegen der besonderen Komplexität dieses Technikeinsatzes und der damit oft verbundenen Undurchsichtigkeit und Unkontrollierbarkeit.

8.17.1 Auskunftsanspruch über Pseudonyme

Auskunft muss auch erteilt werden, wenn personenbezogene Daten unter **Pseudonym** gespeichert werden und dieses Pseudonym der verantwortlichen Stelle bekannt gegeben wird. Hat eine Stelle nur Kenntnis vom Pseudonym und wird dem Verantwortlichen glaubhaft gemacht, dass es sich bei der auskunftssuchenden Person um diejenigen handelt, für die das Pseudonym steht, so muss der Verantwortliche über die personenbezogenen Daten Auskunft geben.[710] Gemäß Art. 11 Abs. 1 DSGVO ist der Verantwortliche aber nicht verpflichtet, nur zum Zweck der Auskunftserteilung Identitätsdaten aufzubewahren oder einzuholen. Die Pflicht zur Glaubhaftmachung der „Betroffenheit" liegt beim Betroffenen, wenn der Verantwortliche nachweist, dass er zu einer Identifikation nicht in der Lage ist (Art. 11 Abs. 2 DSGVO).

8.17.2 Vertragliche Auskunftsansprüche

Neben dem gesetzlichen sind vertragliche Auskunftsansprüche möglich. Diese können sich aus **vertraglichen Nebenpflichten** des Endgeräte-Herstellers, des Applikationsanbieters oder eines sonstigen Vertragspartners ergeben. Für die Abwicklung des jeweiligen Vertrags gemäß Treu und Glauben benötigt ein Betroffener bestimmte zu seinem Endgerät bzw. über ihn gespeicherte Informationen.[711] Die Verweigerung des Zugriffs durch den Betroffenen auf diese personenbezogenen Daten kann einen (Sach-)Mangel darstellen.[712] Bei natürlichen Personen geht die vertragliche zumeist nicht über die datenschutzrechtliche Auskunftspflicht hinaus.

---

709 Wedde in Roßnagel Kap. 4.4 Rn. 2 (S. 547), Dix in Simitis § 34 Rn. 2.

710 Däubler in Däubler u. a. § 34 Rn. 8; Dix in Simitis § 34 Rn. 45; Kamlah in Plath § 34 Rn. 6; ULD (2013) S. 20 f.; zur begrenzten Recherchepflicht bei Nichtvorliegen der Identifizierungsdaten s. o. 2.4. u. Art. 11 DSGVO.

711 So das Beklagtenvorbringen in OLG Hamm 2.7.2015 – 28 U 46/15, Rn. 14; das Gericht geht hierauf nicht ein.

712 Roßnagel in Deutscher Verkehrsgerichtstag S. 276 f.

Eine spezifische zivilrechtliche Auskunftsregelung enthält § 630g BGB bei Vorliegen eines medizinischen Behandlungsvertrags gemäß § 630a BGB. Demnach hat der Behandelnde dem Patienten auf Verlangen unverzüglich Einsicht in die vollständige ihn betreffende Patientenakte zu gewähren, soweit der Einsichtnahme nicht erhebliche therapeutische Gründe oder sonstige erhebliche Rechte Dritter entgegenstehen. Der Patient kann gemäß § 630g Abs. 2 BGB auch elektronische Abschriften verlangen. Er hat die entstandenen Kosten zu erstatten. Hinsichtlich des elektronischen Formats gibt es bisher noch keine Festlegungen.

8.17.3 Auskunftsverweigerung

Betriebs- und Geschäftsgeheimnisse (s. u. 9.2) können nach § 34 Abs. 1 S. 3 bzw. Abs. 3 S. 3 BDSGaF einer Auskunft über Herkunft und Empfänger bei einer Verarbeitung für Zwecke der Übermittlung entgegenstehen, wenn die Geheimhaltungsinteressen die Betroffeneninteressen überwiegen (s. o. 8.16.2). Betriebs- und Geschäftsgeheimnisse können zudem bisher generell auch von Stellen, die Daten für eigene Zwecke verarbeiten, nach § 34 Abs. 7 i. V. m. § 33 Abs. 2 Nr. 3 BDSGaF geltend gemacht werden, wenn die Daten „ihrem Wesen nach, namentlich wegen des überwiegenden rechtlichen Interesses eines Dritten, geheim gehalten werden müssen".

Art. 23 Abs. 1 DSGVO erlaubt auch künftig Ausnahmen. Im nationalen Recht sind Auskunftsausnahmen bei der Datenverarbeitung für wissenschaftliche, statistische und archivarische Zwecke (§ 27 Abs. 2, 28 Abs. 2 BDSGnF) vorgesehen sowie "soweit durch die Auskunft Informationen offenbart würden, die ihrem Wesen nach, insbesondere wegen der überwiegenden Interessen eines Dritten, geheim gehalten werden müssen" (§ 29 Abs. 1 S. 2 BDSGnF). § 34 Abs. 1 BDSGnF ermöglicht künftig zudem eine Auskunftsverweigerung, wenn der Betroffene gemäß § 33 Abs. 1 Nr. 1, 2 BDSGnF nicht zu informieren ist oder die Daten nur aus Satzungsgründen nicht gelöscht werden dürfen bzw. ausschließlich für Zwecke der Datensicherung oder der Datenschutzkontrolle gespeichert werden und ein unverhältnismäßiger Aufwand entstehen würde. § 33 BDSGnF nennt als weitere Gründe für eine Informationsverweigerung Aspekte der Aufgabenerfüllung, der öffentlichen Sicherheit und Ordnung sowie staatlicher Geheimhaltung.

8.17.4 Art der Auskunftserteilung

Hinsichtlich der Art der Auskunftserteilung sieht § 34 Abs. 6, Abs. 8 S. 1 BDSGaF bisher vor, dass auf Verlangen die Auskunft grds. unentgeltlich und in Textform zu erfolgen hat (ähnlich § 19 Abs. 1 S. 4, Abs. 7 BDSGaF für öffentliche Stellen des Bundes). Künftig ist gemäß Art. 15 Abs. 3 S. 1 DSGVO die erste Kopie unentgeltlich; für alle weiteren Kopien kann „ein angemessenes Entgelt auf der Grundlage der Verwaltungskosten" verlangt werden.

Es besteht bisher kein Anspruch darauf, die Daten in einer bestimmten computerlesbaren Form bereitgestellt zu bekommen.[713] Vom Mai 2018 an gilt Art. 15 Abs. 3 DSGVO. Danach besteht der Anspruch auf eine Kopie der personenbezogenen Daten. Bei elektronischem Antrag „sind die Informationen in einem gängigen elektronischen Format zur Verfügung zu stellen" (S. 2). Dies bedeutet, dass bei einem elektronischen Auskunftsersuchen grds. eine digitale Auskunft zu erfolgen hat. Die Regelung dient einer größtmöglichen Praktikabilität. Sie zielt auch darauf ab, dem Betroffenen die Auskunft in einer für ihn weiterverwendbaren Form, z. B. zwecks elektronischer Speicherung, zur Verfügung zu stellen. Will der Verantwortliche einen anderen Weg gehen, so kann er sich dies vom Betroffenen erlauben lassen. Für eine Abweichung vom Regelfall bedarf es künftig einer plausiblen Begründung.

Insofern ist Art. 20 DSGVO interessant, der dem Betroffenen einen Anspruch auf Übertragung seiner Daten zu sich selbst oder zu einem anderen verantwortlichen Dienstleister vorsieht und zwar „in einem strukturierten, gängigen und maschinenlesbaren Format". Für diese Datenübertragbarkeit bestehen aber bisher in Bezug auf Gesundheits- oder Behandlungsdaten keine allgemein akzeptierten Standards. Für Big Data im Gesundheitswesen können solche Standards von Bedeutung sein. Zugleich würde die Selbstbestimmungsmöglichkeit der Betroffenen dadurch gestärkt, dass es sie sind, die darüber entscheiden können, ob und wenn ja welche ihrer Daten in eine Auswertung eingebracht werden.

8.17.5 Bevollmächtigung zur Auskunftseinholung

Der datenschutzrechtliche Anspruch ist höchstpersönlicher Natur[714], muss aber nicht von den Betroffenen höchstpersönlich wahrgenommen werden. Diese können fremde Hilfe in Anspruch nehmen und hierfür z. B. einen Dritten bevollmächtigen. Eine Vollmachterteilung zur Einholung der Auskunft kann z. B. an einen Anwalt oder auch an ein kommerziell tätiges Unternehmen erfolgen.[715] Um zu verhindern, dass wegen unwirksamer Bevollmächtigung eine unzulässige Datenübermittlung vorgenommen wird, kann mit befreiender Wirkung die Auskunft nicht nur gegenüber dem Bevollmächtigten, sondern auch gegenüber dem Betroffenen als Vollmachtgeber erteilt werden.[716]

Hinsichtlich der Ausgestaltung des Verhältnisses zwischen Betroffenem und Bevollmächtigtem gibt es keine spezifischen rechtlichen Vorgaben. Der Bevollmächtigte kann als eigenständige verantwortliche Stelle tätig werden wie auch als Auftragsverarbeiter entsprechend § 11 BDSGaF bzw. Art. 28 DSGVO.[717] Die rechtliche Bewertung richtet sich nach der Form der Bevollmächtigung und dem zwischen den Betroffenen und dem

---

713 Roßnagel in Deutscher Verkehrsgerichtstag S. 277, 283; Dix in Simitis § 34 Rn. 49.

714 Däubler in Däubler u. a. § 6 Rn. 10; Gola/Schomerus § 6 Rn. 3; Schreiber in Plath § 6 Rn. 8.

715 Kamlah in Plath § 34 Rn. 4; Dix in Simitis § 6 Rn. 9; Mallmann in Simitis § 19 Rn. 34; ULD (2013) S. 27 m. w. N.

716 Kamlah in Plath § 34 Rn. 4.

717 Eine direkte Anwendung scheidet aus, weil der Betroffene im datenschutzrechtlichen Sinn nicht verantwortliche Stelle gemäß § 3 Abs. 7 BDSGaF bzgl. seiner eigenen Daten ist.

Bevollmächtigten geschlossenen Vertrag. Auch wenn die bevollmächtigte Stelle als Verantwortlicher i. S. v. Art. 4 Nr. 7 DSGVO (§ 3 Abs. 7 BDSGaF) handelt, gilt grundsätzlich der auf dem Zweckbindungsprinzip (Art. 5 Abs. 1 lit. b DSGVO) basierende Grundsatz der Mandantentrennung. Dies bedeutet, dass über die Auskunftserteilung erlangte Daten zunächst nur zu dem konkreten Zweck der Auskunftserteilung und nicht für andere (z. B. eigene) Zwecke verwendet dürfen; eine Vermischung mit Auskunftsdaten anderer Betroffener ist grundsätzlich unzulässig. Erteilt der Betroffene dem Bevollmächtigten jedoch die Einwilligung zur einer Datenweitergabe oder sonstigen Datenverarbeitung oder erteilt er ihm hierzu evtl. gar einen Auftrag, so ist diese Verarbeitung zulässig.[718]

Dem steht nicht entgegen, dass mit der weiteren Datenverarbeitung andere, z. B. wissenschaftliche oder ökonomische Zwecke verfolgt werden. Es ist inzwischen anerkannt, dass mit persönlichkeitsrechtlichen und insbesondere datenschutzrechtlichen Ansprüchen sowohl durch den Betroffenen wie auch durch Dritte kommerzielle Interessen umgesetzt werden können und dürfen (s. u. 9.3.2).[719]

Zur Durchsetzung von Auskunftsansprüchen kann die Inanspruchnahme professioneller Unterstützung sinnvoll, ja sogar faktisch notwendig sein. Die Bevollmächtigung eines spezialisierten Dienstleisters, der, anders als die meisten Betroffenen, über rechtliche, branchenspezifisch-fachliche und technische Kenntnisse verfügt, erleichtert die Wahrnehmung des Auskunftsrechts. Teilweise wird in Frage gestellt, worin der Mehrwert besteht, auch den Empfang der Auskunft an einen Dritten zu delegieren, zumal die Richtigkeit der Auskunft am besten vom Betroffenen selbst überprüft werden kann.[720] Oft zeigen sich Verantwortliche wenig bereit, ihren Auskunftspflichten gegenüber Betroffenen zu entsprechen. Dies gilt insbesondere dort, wo vom Verantwortlichen mit der Verarbeitung kommerzielle Zwecke verfolgt werden, auch im Gesundheitsbereich. Hier kann oft nur ein professioneller Dienstleister mit Kenntnissen über die Rechtslage wie auch über die Datenverarbeitungspraxis beurteilen, ob und wieweit eine Auskunftserteilung bzw. -verweigerung plausibel und rechtlich korrekt ist.

8.18 Betroffenenrechte generell

Neben dem Auskunftsanspruch und weiteren Transparenzansprüchen (Art. 13, 14 DSGVO) haben Betroffene ein Recht auf Löschung (Art. 17 DSGVO), ein Recht auf Einschränkung der Verarbeitung (bisher „Sperrung“, Art. 18 DSGVO), ein Recht auf Datenübertragbarkeit (Portabilität, Art. 20 DSGVO, s. o. 8.17.4) sowie ein Recht auf Widerspruch (Art. 21 DSGVO). Hinsichtlich dieser weiteren Betroffenenrechte gelten die Ausführungen zur Auskunft im Hinblick auf die Möglichkeit der Bevollmächtigung bzw. Beauftragung (s. o. 8.17.5).

718 Bönninger Deutscher Verkehrsgerichtstag S. 238.

719 Weichert NJW 2001, 1463 ff.; Weichert in Taeger/Wiebe, Informatik-Wirtschaft-Recht, Festschrift für Kilian, 2004, S. 281 ff.; kritisch Simitis in Simitis § 4a Rn. 5 f.; Dix in Simitis § 6 Rn. 6.

720 ULD (2013) S. 28.

Das Recht auf **Berichtigung** kommt bei einer unrichtigen personenbezogenen Datenverarbeitung zum Tragen und dient der Richtigkeit i. S. v. Art. 5 Abs. 1 lit. d DSGVO (s. o. 8.13). Hinsichtlich des Dateninputs bei Big Data dürfte dem Berichtigungsanspruch keine größere Bedeutung zukommen, da die Wahrnehmung dieses individuellen Rechts bei Massendatenverarbeitung äußerst aufwändig ist. Dagegen spielt die Frage der Richtigkeit bei Big-Data-Analyseergebnissen eine große Rolle, insbesondere wenn aus diesen Ergebnissen wichtige individuelle Entscheidungen resultieren. Die Richtigkeitsprüfung kann sich in diesen Fällen sowohl auf die einfließenden Daten, das Auswertungsverfahren und dessen Wissenschaftlichkeit (s. o. 8.9.1) wie auf das Ergebnis selbst beziehen.

8.18.1 Optionsrechte

Neben der Transparenz ist die Wahrung von **Wahlmöglichkeiten** für die informationelle Selbstbestimmung der betroffenen Person ein zentrales Anliegen. Nach Art. 21 Abs. 1 DSGVO hat sie ein Recht, einer konkreten Datenverarbeitung „aus Gründen, die sich aus ihrer besonderen Situation ergeben", zu widersprechen. Dies gilt auch für den Fall des Profiling. Der Verantwortliche ist daraufhin zu einer Prüfung verpflichtet und darf die Verarbeitung nur fortsetzen, wenn er „zwingende schutzwürdige Gründe für die Verarbeitung nachweisen kann", die die Betroffeneninteressen überwiegen. Derartige überwiegende Interessen bestehen nicht bei Werbezwecken (Art. 21 Abs. 2, 3 DSGVO). Bei automatisierten Entscheidungen hat der Betroffene ein Recht auf „Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung" (Art. 22 Abs. 3 DSGVO). Basis dieser Befugnisse ist in jedem Fall ein Widerspruch des Betroffenen, der z. B. durch das Anklicken eines entsprechenden Buttons zum Ausdruck gebracht werden kann. Der Anspruch auf Option einer analogen Alternative muss sich aber nicht zwangsläufig auf den Entscheidungsinhalt auswirken, sondern bezieht sich ausschließlich auf den Entscheidungsprozess.

8.18.2 Kollektive Rechtsverfolgung

Spezifisch vorgesehene Formen einer datenschutzrechtlichen Treuhänderschaft finden sich in Art. 80 DSGVO. Danach sind Betroffene berechtigt, Einrichtungen, Organisationen oder Vereinigungen ohne Gewinnerzielungsabsicht mit der Wahrnehmung ihrer Rechte sowohl im administrativen wie auch im gerichtlichen Verfahren zu beauftragten (Art. 80 Abs. 1 DSGVO). Solche nationalen Regelungen für **Sammelklagen** bestehen bisher im deutschen oder im österreichischen Recht nicht.[721] Wohl aber wird intensiv über die Notwendigkeit der Einführung derartiger Formen kollektiver Rechtsverfolgung diskutiert.[722] Die Verarbeitung von Gesundheitsdaten und Big-Data-Anwendungen sind geeignete

721 Zu Österreich EuGH 25.1.2018 – C-498/16; dazu Janisch, Weg frei für Prozess gegen Facebook, SZ 26.1.2018, 1.

722 Ott, Sammelklagen durch die Hintertür, SZ 28.11.2017, 24; Beise, Auf zur Waffengleichheit, SZ 8.11.2017, 17; Ott, FDP dringt auf Sammelklage, SZ 6.11.2017, 33; Prantl, Munition für David, SZ 1.8.2017; Musterklagen: Union bleibt skeptisch, SZ 1.8.207, 5.

Anwendungsfälle für solche Vorgehensweisen, da hier oft eine Vielzahl von Menschen in gleicher Weise durch Unternehmen in ihren Rechten verletzt sein kann.

Keine direkte Treuhänderschaft für die einzelnen Betroffenen, sondern eine pauschale Vertretung von Kollektivinteressen bzw. der Interessen von allen Betroffenen ist in Art. 80 Abs. 2 DSGVO vorgesehen, wonach bestimmte Organisationen gemäß nationalem Recht ermächtigt werden können, allgemein und ohne konkrete Aufträge die Interessen der Betroffenen zu vertreten. Eine solche nationale Regelung enthält in Deutschland für die Wahrnehmung von Verbraucherinteressen das Unterlassungsklagegesetz (UKlaG), in dem seit 2016 klargestellt ist, dass es auch im Datenschutzbereich anwendbar ist.[723] Im Arbeitsrecht besteht eine entsprechende Klagemöglichkeit noch nicht.[724] Die Nutzung dieses Verbandsklagerechts bei Big Data und Gesundheitsdaten kann – ebenso wie das für Sammelklagen gelten würde – von hoher Relevanz sein.

8.19 Staatliche Aufsicht

Art. 8 Abs. 3 GRCh sieht vor, dass die Einhaltung der Vorschriften zum Datenschutz „von einer unabhängigen Stelle überwacht" wird. Hierfür sind die Datenschutzaufsichtsbehörden eingerichtet. Diese nehmen bisher ihre Aufgaben als „Kontrollstellen" gem. Art. 28 EG-DSRl wahr. In Deutschland ist diese Kontrollstelle die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) für die öffentlichen Stellen des Bundes sowie Telekommunikationsanbieter (§§ 22 ff. BDSGnF, §§ 8 ff. BDSGnF). Die Kontrollstellen der Bundesländer sind die Datenschutzaufsichtsbehörden (§ 38 BDSGaF, § 40 BDSGnF), die für den nicht-öffentlichen Bereich zuständig sind. Die Landesbeauftragten für Datenschutz sind für den öffentlichen Bereich der Länder zuständig und zugleich identisch mit den (für Private zuständigen) Aufsichtsbehörden (außer Bayern).

Für Big Data im Gesundheitsbereich ist die Datenschutzkontrolle von eminenter Bedeutung. Wegen der Kompensationsfunktion der unabhängigen Datenschutzkontrolle für die tatsächlich beschränkten Möglichkeiten der Betroffenen, ihre Rechte geltend zu machen, ergeben sich unter Anwendung des Verhältnismäßigkeitsgrundsatzes Mindestanforderungen an die Frequenz und Tiefe aufsichtlicher Prüfungen: Je weniger eine Kontrolle durch die Betroffenen selbst sichergestellt werden kann, umso wichtiger wird ein hinreichend wirksames aufsichtsrechtliches Kontrollregime. Dies gilt, wie das BVerfG für geheime Sicherheitsdateien festgestellt hat, insbesondere für die hoheitliche Datenverarbeitung, wenn die Verarbeitung für die Betroffenen in hohem Maße intransparent bleibt. Dort dürfen die Abstände aufsichtlicher Regelkontrollen „ein gewisses Höchstmaß, etwa zwei Jahre, nicht überschreiten".[725]

723 Weichert Datenschutz-Berater 04/2017, 79 f., ausführlich ders. DANA 2007, 4-10.

724 Dafür Schuler/Weichert, Die EU-DSGVO und die Zukunft des Beschäftigtendatenschutzes, 8.4.2016, S. 21, https://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2016_dsgvo_beschds.pdf.

725 BVerfG 24.4.2013 – 1 BvR 1215/07, Rn. 217 = NJW 2013, 1517 = DuD 2013, 740 = ZD 2013, 328.

Diese Rechtsprechung lässt sich auf die komplexe Datenverarbeitung in sensitiven Bereichen wie dem Gesundheitswesen übertragen, auch bzw. gerade wenn sie von nicht-öffentlichen Stellen durchgeführt wird. Durch den Einsatz von Big Data sowie Techniken der Künstlichen Intelligenz ist es für die Betroffenen nicht mehr im Ansatz möglich, selbst ihre informationelle Selbstbestimmung auszuüben, da die Betroffenen zumeist allenfalls eine vage Kenntnis über die verarbeiteten Daten und die verarbeitenden Stellen haben Zumeist überhaupt keine Vorstellung haben sie von der Logik und den Verfahren der Speicherung und Auswertung sowie von der Nutzung der jeweiligen Ergebnisse. Praktische Einflussmöglichkeiten bestehen für die Betroffenen i. d. R. überhaupt keine. Dies bedingt, dass Dritte **treuhänderisch ihre Interessen vertreten** müssen.

Es ist an allererster Stelle und grundrechtlich abgesichert die Aufgabe der Datenschutzaufsicht, diese Funktion zu übernehmen. Wegen der Knappheit der vorhandenen Gesamtressourcen und der Unsicherheit, wie diese von der Datenschutzaufsicht in ihrer Unabhängigkeit eingesetzt werden, ist es im Interesse der Betroffenen von Big Data im Gesundheitsbereich nötig, dass, ähnlich wie diese in speziellen Sicherheitsbereichen erfolgt ist[726], einfachgesetzliche **Vorgaben zur Tiefe, Qualität und Frequenz der Datenschutzkontrolle** in diesem Bereich spezifisch festgelegt werden.

8.20 Datenschutz-Folgenabschätzung

Die DSGVO verfolgt bei ihrem Schutzkonzept einen **risikobezogenen Ansatz**. Die Verantwortlichen sollen weniger zur Einhaltung formaler Anforderungen als dazu veranlasst werden, die Risiken ihrer Datenverarbeitung zu bewerten und adäquate Mittel zur Risikovermeidung zu ergreifen. Dem dient in erster Linie die in Art. 35 DSGVO geregelte Datenschutz-Folgenabschätzung. Bei der Datenschutz-Folgenabschätzung geht es nicht nur um die Rechtmäßigkeit der einzelnen Verarbeitungsschritte, sondern darüber hinausgehend um eine prognostische Abschätzung der damit verbundenen Gefahren insbesondere aus der Betroffenenperspektive.[727]

Die **Begründung für Art. 35 DSGVO** liest sich so, als sei sie auf Big Data im Gesundheitsbereich zugeschnitten: „Dies sollte insbesondere für umfangreiche Verarbeitungsvorgänge gelten, die dazu dienen, große Mengen personenbezogener Daten auf regionaler, nationaler oder supranationaler Ebene zu verarbeiten, eine große Zahl von Personen betreffen könnten und — beispielsweise aufgrund ihrer Sensibilität — wahrscheinlich ein hohes Risiko mit sich bringen und bei denen entsprechend dem jeweils aktuellen Stand der Technik in großem Umfang eine neue Technologie eingesetzt wird, sowie für andere Verarbeitungsvorgänge, die ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen mit sich bringen, insbesondere dann, wenn diese

726 § 10 Abs. 2 Antiterrordateigesetz (ATDG), § 11 Abs. 2 Rechtsextremismusdateigesetz (REDG).

727 Datenschutzkonferenz, Kurzpapier Nr. 5, Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO, S. 1; Forum Privatheit (Friedewald/Bieker/Obersteller/Nebel/Martin/Rost/Hansen), White Paper Datenschutz-Folgenabschätzung, Ein Werkzeug für einen besseren Datenschutz, 3. Aufl. 11/2017, S. 5.

Verarbeitungsvorgänge den betroffenen Personen die Ausübung ihrer Rechte erschweren. Eine Datenschutz-Folgenabschätzung sollte auch durchgeführt werden, wenn die personenbezogenen Daten für das Treffen von Entscheidungen in Bezug auf bestimmte natürliche Personen im Anschluss an eine systematische und eingehende Bewertung persönlicher Aspekte natürlicher Personen auf der Grundlage eines Profilings dieser Daten oder im Anschluss an die Verarbeitung besonderer Kategorien von personenbezogenen Daten, biometrischen Daten oder von Daten über strafrechtliche Verurteilungen und Straftaten sowie damit zusammenhängende Sicherungsmaßregeln verarbeitet werden" (ErwGr. 91 S. 1, 2 DSGVO).

Bei Big-Data-Anwendungen im Gesundheitsbereich sind Datenschutz-Folgenabschätzungen Pflicht, da die in Art. 35 Abs. 3 DSGVO genannten Merkmale vorliegen: systematische umfassende Bewertung persönlicher Aspekte (lit. a) und umfangreiche Verarbeitung sensitiver Daten (lit. b). Darunter fallen Krankenhausinformationssysteme wie Datensammlungen aus klinischen Tests, nicht aber die Verarbeitung in einem einzelnen Arztinformationssystem (AIS). Die pseudonyme Zusammenführung von Daten aus AIS muss z. B. dagegen eine Folgenabschätzung durchlaufen.[728]

Gefordert wird dabei gemäß Art. 35 Abs. 7 DSGVO eine systematische Beschreibung der Verarbeitungsvorgänge (lit. a), deren Bewertung hinsichtlich Verhältnismäßigkeit (lit. b, c), sowie die Beschreibung der Maßnahmen zur Bewältigung der Risiken (lit. d). Der Verantwortliche ist gemäß Absatz 9 gehalten, den Standpunkt der betroffenen Personen oder ihrer Vertreter einzuholen. Dies können im Konsumbereich Verbraucherzentralen und Bürgerrechtsverbände oder bei einem Einsatz durch einen Arbeitgeber der Betriebsrat sein.[729] Konkretisierendes europäisches oder nationales Recht ist möglich (Art. 35 Abs. 10 DSGVO).

Die Umsetzung von Art. 35 DSGVO setzt jeweils eine Bewertung voraus, die hinsichtlich Umfang, Aufbau und Detailtiefe von hoher Komplexität ist. Um diesen Anforderungen zu genügen, bedarf es strukturierter Vorgaben für die Verantwortlichen mit allgemeinverständlichen Umsetzungsanleitungen und Handlungsempfehlungen, die an die konkreten Risiken und Schutzmöglichkeiten bei Big Data im Gesundheitsbereich angepasst sind. Es ist wünschenswert und absehbar, dass derartige Hilfen durch die Aufsichtsbehörden zur Verfügung gestellt werden.[730]

---

728 Article 29 Data Protection Working Party, WP 248 v. 4.10.2017, Guidelines in Data Protection Impact Assessment (DPIA) and determining whether processing is „likely to result in a high risk" for the purposes of Regulation 2016/679. S. 9 ff.; Forum Privatheit, White Paper Datenschutz-Folgenabschätzung, 2017, S. 20 f.; Baumgartner in Ehmann/Selmayr Art. 35 Rn. 24-26.

729 Martini in Paal/Pauly Art. 35 Rn. 60; Forum Privatheit, White Paper Datenschutz-Folgenabschätzung, 2017, S. 26.

730 Baumgartner in Ehmann/Selmayr Art. 35 Rn. 39; Jandt in Kühling/Buchner Art. 35 Rn. 35; Hansen DuD 2016, 587 ff.; Article 29 Data Protection Working Party, WP 248 v. 4.10.2017 S. 17.

Gemäß Art. 35 Abs. 10 DSGVO kann auf gesetzlicher Grundlage auf eine Folgenabschätzung in den Fällen der Art. 6 Abs. 1 lit. c od. e DSGVO verzichtet werden, also bei „Erfüllung einer rechtlichen Verpflichtung" sowie, wenn „die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt". In diesen Fällen kann, muss aber nicht, auf eine verfahrensbezogene Folgenabschätzung verzichtet werden, soweit schon gesetzlich die Folgenabschätzung vorgenommen wurde. Bei komplexen Verfahren wie dem Einsatz von Big Data im Gesundheitsbereich dürfte der Gesetzgeber mit einer derartigen Aufgabe überfordert sein.[731] Wohl aber kann über diese Öffnungsklausel mit einer **gesetzlichen Folgenabschätzung** eine Konkretisierung des Art. 35 DSGVO vorgenommen werden.

8.21 Verfahrensrechtliche Schutzmechanismen

Art. 32 Abs. 1 DSGVO fordert, dass Daten verarbeitende Stellen „geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten", zu ergreifen haben. Als solche Maßnahmen werden genannt: Pseudonymisierung und Verschlüsselung (lit. a, s. o. 8.12.2), die Sicherstellung von Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit (lit. b, c) sowie die Evaluierung der Verarbeitung (lit. d). Beim Einsatz von Big Data im Gesundheitsbereich müssen also, wie generell bei jeder personenbezogenen Datenverarbeitung, die technisch-organisatorischen **Schutzziele** optimiert verwirklicht werden. Dabei handelt es sich um die Verwirklichung von Vertraulichkeit, Verfügbarkeit, Nichtverkettbarkeit, Transparenz und Intervenierbarkeit.[732]

Die **Umsetzung dieser Schutzziele** ist Aufgabe der verarbeitenden Stellen, also der Verantwortlichen und der Auftragsverarbeiter, die die Verantwortung für die konkrete Umsetzung haben. Konkretisierungen können aber auch explizit gesetzlich oder untergesetzlich vorgenommen werden. Eine solche Konkretisierung in Bezug auf die Verarbeitung von sensitiven Daten erfolgte – in sehr allgemeiner Form – in § 22 Abs. 2 BDSGnF.[733] Weitere gesetzliche Konkretisierungen werden durch die DSGVO bei sensitiven Daten und bei automatisierten Entscheidungsverfahren erlaubt. Denkbar sind auch Konkretisierungen in der Form von Verhaltensregeln (Art. 40 DSGVO), Zertifizierungsanforderungen (Art. 42 Abs. 5 DSGVO) oder in Festlegungen durch Aufsichtsbehörden für Datenschutz-Folgenabschätzungen (vgl. Art. 35 Abs. 4, 5 DSGVO).

Nichtverkettbarkeit zielt auf die technische Umsetzung des Zweckbindungsgrundsatzes ab (s. o. 8.6). Im Gesundheitsbereich spielt die Zweckbindung in Form des Notlagenschutzes eine zentrale Rolle (s. o. 6.8). Eine strenge Zweckbindung sensitiver Gesundheitsdaten ist für die Betroffenen von größerer Bedeutung als in anderen Lebensbereichen. Während Big Data konzeptionell auf eine Verkettung vorhandener Datenbestände abzielt, stehen dem

731 Ähnlich Baumgartner in Ehmann/Selmayr Art. 35 Rn. 51, Hansen DuD 2016, 589.

732 Grundlegend Rost in Schmidt/Weichert S. 353 ff.; Forum Privatheit, White Paper Datenschutz-Folgenabschätzung, 2017, S. 28 ff.

733 Weichert DuD 2017, 542.

die Ziele der Vertraulichkeit und Nichtverkettbarkeit diametral entgegen. Eine Verkettung durch Übermittlung oder auch durch eine interne Nutzung und eine Zweckänderung muss daher anwendungsbezogen zusätzlich zu technisch-organisatorischen Maßnahmen an materiell-rechtliche wie prozedurale Bedingungen geknüpft werden (s. o. 8.7).

8.21.1 Treuhändermodelle

Datentreuhänderschaft ist im Interesse der Betroffenen möglich (s. o. 8.17.5) wie auch im Auftrag und Interesse von Verantwortlichen: Durch die organisatorische, technische und rechtliche Trennung zwischen Treuhänder und Verantwortlichen bei der Verarbeitung wird eine Compliance-Sicherung für die Verantwortlichen eingerichtet. Diese soll eine mehr oder weniger unabhängige Kontrolle der Verarbeitung sicherstellen. Die etablierteste und gesetzliche ausdrücklich vorgesehene Form einer solchen Treuhänderschaft sind die Vertrauensstellen von Krebsregistern, die Klardaten von Krebspatienten verwalten und eine Pseudonymisierung vornehmen, so dass die Merkmalsdaten nur unter einem Pseudonym im Krebsregister gespeichert und verarbeitet werden. Dem Treuhänder kommt dabei die Funktion zu, sowohl die Interessen des oder der Verantwortlichen wie auch die der der Betroffenen wahrzunehmen.[734] Der Treuhänder pseudonymisiert nicht nur die für ein Register eingehenden Daten, sondern kann nach einer Einzelfallprüfung Datensätze aus dem Register oder Auswertungsergebnisse wieder reidentifizieren, etwa um einen behandelnden Arzt oder den Betroffenen über behandlungsrelevante Auswertungsergebnisse zu informieren.[735]

Eine stelleninterne Treuhänderfunktion war schon in § 30 Abs. 1 BDSGaF für die geschäftsmäßige Verarbeitung zum Zweck der anonymisierten Übermittlung vorgesehen. Danach sind die „Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person zugeordnet werden können. Diese Merkmale dürfen mit den Einzelangaben nur zusammengeführt werden, soweit dies für die Erfüllung des Zwecks der Speicherung oder zu wissenschaftlichen Zwecken erforderlich ist.“ Für eine Wirksamkeit des Schutzes einer sog. „File-Trennung“ ist es erforderlich, dass für Zuordnungsprozesse ein unabhängiges Prüfungsverfahren gewährleistet ist, in dem die Zuordnungen für Kontrollzwecke protokolliert werden.[736]

Praktische Anwendung finden solche Treuhändermodelle insbesondere im Biobankenbereich (s. u. 10.9). Dabei werden Datensätze und Proben mit jeweils unterschiedlichen Pseudonymen abgespeichert. Für bestimmte Verarbeitungsschritte (Erhebung, Speicherung, Herausgabe) können zusätzliche Pseudonymisierungsverfahren vorgesehen werden. Der Treuhänder hat die Aufgabe, die jeweiligen Zuordnungen gemäß

734 Z. B. §§ 11 ff. Bremisches Krebsregistergesetz v. 29.4.2015, Bremisches GBl. 2015, 241; § 11 Bayerisches Krebsregistergesetz v. 7.3.2017 Bayerisches GVBl. S. 26, vgl. § 65c SGB V (Krebsfrüherkennungs- und -registergesetz – KFRG).

735 Deutscher Ethikrat S. 184.

736 Weichert in Däubler u. a. § 30 Rn. 7 f.

den Forschungsfragestellungen zu prüfen, zuzulassen und für diesen Zweck den die Pseudonymzuordnung vorzunehmen.[737]

8.21.2 Sonstige Verfahrenssicherungen

Bei der Verarbeitung sensitiver Daten generell (Art. 9 Abs. 2 DSGVO) und insbesondere auch bei automatisierten Entscheidungen muss der Verantwortliche „angemessene Maßnahmen" ergreifen (Art. 22 Abs. 2 lit. b, Abs. 3, 4 DSGVO).

Als Mindestmaßnahmen werden für automatisierte Entscheidungen generell genannt: „das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung". Dem Betroffenen muss die Möglichkeit eingeräumt werden, eine ausschließlich automatisiert vorgesehene Entscheidung zum Gegenstand einer personalen Entscheidung zu machen, die von einer natürlichen Person verantwortet wird und die individuelle Perspektive des Betroffenen berücksichtigt.[738] Es genügt nicht, dass ein Automat die individuelle Perspektive aufnimmt und dann erneut eine automatisierte Entscheidung getroffen wird. Anders als § 28b BDSGaF zum Scoring enthält Art. 22 DSGVO darüber hinausgehend keine normativ bestimmten Festlegungen hinsichtlich der verwendeten Verfahren und eingesetzten Maßnahmen. Wohl aber werden in Erwägungsgrund 71 einzelne Aspekte angesprochen:

„Um unter Berücksichtigung der besonderen Umstände und Rahmenbedingungen, unter denen die personenbezogenen Daten verarbeitet werden, der betroffenen Person gegenüber eine faire und transparente Verarbeitung zu gewährleisten, sollte der für die Verarbeitung Verantwortliche geeignete mathematische oder statistische Verfahren für das Profiling verwenden, technische und organisatorische Maßnahmen treffen, mit denen in geeigneter Weise insbesondere sichergestellt wird, dass Faktoren, die zu unrichtigen personenbezogenen Daten führen, korrigiert werden und das Risiko von Fehlern minimiert wird, und personenbezogene Daten in einer Weise sichern, dass den potenziellen Bedrohungen für die Interessen und Rechte der betroffenen Person Rechnung getragen wird und mit denen verhindert wird, dass es gegenüber natürlichen Personen aufgrund von Rasse, ethnischer Herkunft, politischer Meinung, Religion oder Weltanschauung, Gewerkschaftszugehörigkeit, genetischer Anlagen oder Gesundheitszustand sowie sexueller Orientierung zu diskriminierenden Wirkungen oder zu Maßnahmen kommt, die eine solche Wirkung haben" (ErwGr 71 S. 6 DSGVO). Das Erfordernis angemessener Maßnahmen ist nicht direkt anwendbar, wenn Rechtsvorschriften der Union oder von Mitgliedstaaten spezifische Regelungen erlassen (Art. 22 Abs. 3 i. V. m. Abs. 2 lit. b DSGVO). So kann u. U. auf Eingriffsmöglichkeiten des Betroffenen bei automatisierten

737 Ausführlich ULD (2009) S. 52 ff.
738 Buchner in Kühling/Buchner Art. 22 Rn. 31.

Entscheidungsverfahren verzichtet werden, wenn in der jeweiligen Regelung andere angemessene Maßnahmen vorgesehen sind.[739]

8.21.3 Melde- und Genehmigungspflichten

Eine prozedurale Sicherungsmaßnahme kann darin bestehen, dass spezifisch beschriebene Formen der Datenverarbeitung davon abhängig gemacht werden, dass sie zuvor einer Revisionsstelle gemeldet oder von dieser genehmigt wurden. Stelleninterne wie externe Lösungen sind denkbar. In jedem Fall sollte gewährleistet sein, dass die jeweilige Stelle die für eine Prüfung nötige fachliche Qualifikation sowie hinsichtlich der konkreten Anwendung eine hinreichende Unabhängigkeit vorweisen kann. Weitere wichtige Rahmenbedingungen für wirksame Melde- und Genehmigungspflichten sind ein möglichst transparentes Verfahren sowie die Sicherstellung einer Verantwortlichkeit der Stelle, gegenüber der die Meldung vorgenommen wird oder die für die Genehmigung zuständig ist. Sowohl für Meldungen wie für Anträge auf Genehmigung sind Anforderungen an Form und Inhalt zu stellen, mit denen sichergestellt wird, dass der Revisionsstelle sämtliche bewertungsrelevanten Umstände bekannt werden. Derartige Revisionsstellen können z. B. für die medizinische Forschung Use-and-Access-Committees sein (s. u. 10.8.4).

Eine Meldepflicht genügt, wenn davon ausgegangen werden kann, dass die geplante Verarbeitung regelmäßig den Vorschriften genügt, dies aber von dritter Seite geprüft werden sollte. Die Meldepflicht führt dazu, dass die verarbeitende Stelle zu einer vertieften eigenen Zulässigkeitsprüfung veranlasst wird und – wegen der zu erwartenden Kontrolle durch eine dritte Stelle – hierbei auch die nötige Sorgfalt walten lässt. Mit der Meldepflicht verbunden sein muss die Möglichkeit der Revisionsstelle, im Zweifel Klärungen herbeizuführen bzw. im Fall von erkennbaren Verstößen gegen zwingende Vorgaben die Umsetzung der gemeldeten Datenverarbeitung zu verhindern. Diese Interventionsmöglichkeit sollte an eine bestimmte Frist gebunden sein, um für die Beteiligten sowohl hinreichende Prüfungsgelegenheit wie auch ab einem bestimmten Zeitpunkt Rechtssicherheit zu gewährleisten.

Eine Genehmigungspflicht ist angezeigt, wenn von einer konkreten Anwendung ein gesteigertes Risiko ausgeht, das in jedem Fall eine unabhängige qualifizierte Überprüfung erfordert. Dies kann damit begründet sein, dass die Selbstbestimmung der von der Verarbeitung Betroffenen nicht möglich ist. Genehmigungspflichten sind auch angezeigt, wenn die Verarbeitung für die Betroffenen hohe Risiken zur Folge hat, dass eine sehr umfangreiche oder eine hochkomplexe Verarbeitung angestrebt wird oder dass die Verarbeitung sich auf viele Stellen oder gar auf verschiedene Rechtsordnungen erstreckt.

8.22 Regulierte Selbstregulierung

Die Sicherstellung von Verantwortung bei der Konzipierung und Umsetzung von Big Data im Gesundheitsbereich kann durch regulierte Selbstregulierung gewährleistet und gefördert werden. Selbstregulierung bedeutet, dass die verantwortlichen Stellen durch

739 Weichert in Reiffenstein/Blaschke S. 257 f.

Vereinbarungen, über Verbände und über gemeinsame Verfahren Compliance-Maßnahmen vorsehen. Dem dienen Codes of Conduct, Verhaltensregeln, verbindliche Selbstverpflichtungen, Standardfestlegungen, Normierungen, Zertifizierungen und Qualitätssiegel. Hierdurch können die Transparenz gegenüber Dritten wie auch das Vertrauen in Organisation, Prozesse und Verfahren gestärkt werden.[740] Der Vorteil von Selbstregulierung liegt darin, dass regelmäßig eine spezifische Fachnähe besteht und die Beteiligten sich mit den selbst gesetzten Anforderungen in einem hohen Maße identifizieren können. Der Nachteil einer Selbstregulierung liegt in einem regelmäßig geringeren Schutzniveau sowie einer eingeschränkten demokratischen Legitimation und evtl. auch einer begrenzten Transparenz und Kontrollierbarkeit.

Regulierte Selbstregulierung (auch Ko-Regulierung) bedeutet, dass diese Maßnahmen der Selbstregulierung hoheitlich vorgegeben und kontrolliert werden bzw. zumindest kontrolliert werden können. Durch die staatliche Festlegung von Kriterien, Verfahren und Organisationen wird eine gewisse Einheitlichkeit und Vergleichbarkeit sowie eine höhere Verbindlichkeit und ein höheres Vertrauen für die Beteiligten erreicht. Die Transparenz der Verfahren wie auch bzgl. der Anforderung an den Regelungsgegenstand kann so verstärkt werden. Bei regulierter Selbstregulierung können die hoheitlichen Aufsichtsverfahren gelockert werden, wenn die Compliance-Anforderungen im Rahmen der Selbstorganisation überprüfbar delegiert werden. Im Konfliktfall sind aber hoheitliche Aufsichtsmaßnahmen vorzusehen.[741]

Ansätze regulierter Selbstregulierung finden sich in verschiedenen Bereichen sowohl des Medizin- wie auch des Informationstechnikrechtes (s. u. 10.3). Vorgaben für Big Data im Gesundheitsbereich bestehen aber bisher nicht. Es kommen unterschiedliche Verfahren und Maßnahmen mit teilweise unterschiedlicher Zielrichtung in Betracht. Mit der DSGVO werden für den Bereich des Datenschutzes erstmals einheitliche verbindliche Vorgaben gemacht, die sich aber auf den Anwendungsbereich der DSGVO beschränken (Art. 40 ff.). Es ist aber nicht ausgeschlossen, dass ergänzend zu diesen Instrumenten weitere Compliance-Anforderungen gestellt werden. Im Interesse schlanker, praktikabler und transparenter Verfahren ist eine Zusammenfassung unterschiedlicher Anforderungen in einem gemeinsamen Prozess wünschenswert.

8.22.1 Verhaltensregeln

Verhaltensregeln fanden in das BDSG im Jahr 2001 in § 38a Eingang (vgl. Art. 27 EG-DSRl). Danach können Berufsverbände und andere Vereinigungen, die bestimmte Gruppen von Stellen vertreten, „Verhaltensregeln zur Förderung von datenschutzrechtlichen Regelungen der zuständigen Aufsichtsbehörde unterbreiten“. Besondere Anreize waren nicht vorgesehen. So verwundert es wenig, dass von diesem Instrument bis heute nur zwei Mal (in den Bereichen Versicherungen und Geodatenwirtschaft) Gebrauch gemacht

740 Deutscher Ethikrat S. 26.
741 Deutscher Ethikrat S. 103 f., 112

wurde.[742] Auf europäischer Ebene liegt im für die vorliegende Studie relevanten Bereich der Entwurf eines „Code of Conduct on privacy for mobile health applications“ vor.[743]

Die Art. 40, 41 DSGVO enthalten nun **ausführliche Regeln zu Verhaltensregeln**, versehen mit einer hoheitlichen Förderpflicht sowie der Pflicht, umfassende Regeln einschließlich Überwachungsmechanismen vorzusehen. Durch die Genehmigung der Regeln erhalten die Stellen, auf welche die Regeln anwendbar sind, mehr Rechtsklarheit und Rechtssicherheit; über die verbandsinternen Verfahren kann die Dichte aufsichtsbehördlicher Kontrolle reduziert werden.

Verhaltensregeln sind geeignet, konkretisierende Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Betroffeneninteressen bei **Big Data im Gesundheitsbereich** festzulegen. Derartige Verhaltensregeln können von relevanten Verbänden erarbeitet werden. Gemäß Art. 40 Abs. 2 DSGVO kommen z. B. folgende Verbände in Betracht: Forschungsgesellschaften, Ärztekammern, medizinische oder informatische Berufsverbände, der Zusammenschluss von (Universitäts-) Kliniken oder von in diesem Bereich tätigen Unternehmen.[744]

Als Inhalte von Verhaltensregeln zu Big Data im Gesundheitsbereich kommen Konkretisierungen der in § 22 Abs. 2 BDSGnF für die Verarbeitung sensitiver Daten vorgesehenen **spezifischen Maßnahmen** in Betracht (technisch-organisatorische Maßnahmen, Dokumentationspflichten, Sensibilisierung, Datenschutzmanagement, Rollenkonzepte, Pseudonymisierung, Verschlüsselung, Backups, Monitoring, Verfahrensvorkehrungen). Vorstellbar sind darüber hinausgehend weitere in 8.21 erörterte Vorkehrungen.

8.22.2 Zertifizierungen

Angesichts des Umstands, dass Algorithmen eine bestimmende Rolle in wichtigen Lebensbereichen haben, ohne die Betroffenen einzubeziehen, wurde vorgeschlagen, bei spezifischen Anwendungen, z. B. bei Online-Angeboten zu Versicherungstarifen, einen „Algorithmen-TÜV“ verpflichtend vorzusehen.[745] Zertifizierungen können zur **Verbesserung des Schutzes** informationeller Selbstbestimmung einen wichtigen Beitrag leisten.[746] Die Wirksamkeit besteht vor allem dort, wo Dritte (Vertragspartner, Kunden) Vertrauen in die Datenschutzkonformität der Verarbeitung einfordern. Dies gilt für Internet-Angebote[747]

742 Weichert in Däubler u. a. § 38a Rn. 2.

743 ec.europa.eu/digital-single-market/en/privacy-code-conduct-mobile-health-apps; dazu Deutscher Ethikrat S. 113 f.

744 Bergt in Kühling/Buchner Art. 40 Rn. 11-14.

745 Verbraucherzentralen fordern „Algorithmen-Tüv“, www.heise.de 23.04.2017; ähnlich Beckedahl in Netzaktivist fordert bessere Kontrolle bei Künstlicher Intelligenz, www.heise.de 27.12.2017.

746 Kritisch Drews/Kranz, DuD 1998, 93; Gola/Schomerus § 9 a Rn. 5: Beschränkung der betrieblichen Selbstkontrolle durch betrieblichen Datenschutzbeauftragten, kostenaufwändige Bürokratie.

747 Hladjk, DuD 2002, 597.

oder auch für die Verarbeitung fremder besonders sensitiver Daten, etwa im Gesundheitsbereich.[748]

Verpflichtende Zulassungs- oder Zertifizierungsverfahren im Gesundheitsbereichs gibt es bisher im Arzneimittel- und im Medizinprodukterecht (s. u. 10.2, 10.3). Zielrichtung ist dabei aber vorrangig die medizinische Sicherheit; informationstechnische oder -rechtliche Aspekte gewinnen erst langsam, ergänzend Relevanz. Im Rahmen des BSI-G zum Schutz kritischer Infrastrukturen, zu denen Gesundheitseinrichtungen gehören, bestehen normative Anforderungen an die IT-Sicherheit (s. o. 4.4). Die vom Bundesamt für die Sicherheit in der Informationstechnik (BSI) angebotenen IT-Sicherheitszertifikate sind bisher nicht verpflichtend. Auch ansonsten gibt es keine obligatorischen vorlaufenden oder nachträglichen Zertifizierungsverfahren bei informationstechnischen Verfahren im Gesundheitsbereich. Mit dem E-Health-Gesetz wurden für Anwendungen in der Telematik-Infrastruktur in § 291f Abs. 3 SGB V für Angebote zur Übermittlung elektronischer Briefe und in § 291g SGB V Vereinbarungen über technische Verfahren zur konsiliarischen Befundbeurteilung und zur Videosprechstunde bestimmte Standardfestlegungen geregelt. Eine unabhängige und transparente Zertifizierung ist dabei aber noch nicht vorgesehen.

In den Art. 42, 43 DSGVO ist nun erstmals ein freiwilliges, aber verbindlich geregeltes Zertifizierungsverfahren zur Gewährleistung des Datenschutzes vorgesehen, das bei Big Data im Gesundheitsbereich Anwendung finden kann. Hierfür können gemäß Art. 42 einheitliche Kriterien festgelegt werden, die von den Datenschutzaufsichtsbehörden und insbesondere auch europaweit vom Europäischen Datenschutzausschuss genehmigt werden können und somit eine hohe Verbindlichkeit erlangen. Die Regelung hindert den nationalen Gesetzgeber nicht, bei sensitiven Anwendungen verpflichtende Zertifizierungen zu normieren.

8.23 Kinderschutz

Der Schutz der Kinder, vor Fremdbestimmung durch Unternehmen und nicht zuletzt vor den eigenen Eltern, wird mit der Digitalisierung der kindlichen Lebensbereiche zunehmend wichtig. Dieser Schutz wird in Art. 6 Abs. 2 S. 2 GG und Art. 24 GRCh ausdrücklich erwähnt und zugesichert. Er findet in einigen Regelungen der DSGVO seinen Ausdruck. Darin werden spezifische Interessenabwägungen gefordert (Art. 6 Abs. 1 lit. f) oder es bestehen besondere Anforderungen an das Einholen einer Einwilligung (Art. 8). Es bedarf, um informationelle Eingriffe bei Kindern zu legitimieren, einer Unabweisbarkeit der Maßnahme. Im kommerziellen Bereich besteht für automatisierte Entscheidungsverfahren zu Kindern keine Notwendigkeit, weshalb der Gesetzgeber zu Recht festgelegt hat: „Diese Maßnahme sollte kein Kind betreffen“ (ErwGr 71 S. 5 DSGVO). Kompensierende Schutzmaßnahmen sollen daran grundsätzlich nichts ändern. Dahinter steckt die Erwägung,

748 Dazu ausführlich Weichert, MedR 2003, 674.

dass die informationelle Selbstbestimmung von Kindern noch eingeschränkt ist. Informationspflichten und Wahlmöglichkeiten würden regelmäßig ins Leere laufen.[749]

9 Weitere Rechtsgebiete

Das Datenschutzrecht hat für die rechtliche Bewertung von Big Data zentrale Bedeutung, wenn die gesundheitsrelevanten Informationen einen Personenbezug haben. Das Datenschutzrecht ist nicht mehr anwendbar, wenn die Informationen vollständig anonymisiert wurden. Dies ist zumeist bei aggregierten Ergebnissen von Big Data gegeben, wenn die Analyse nicht auf eine Person zielt, sondern wenn auf eine allgemeine oder eine organisationsspezifische Fragestellung eine Antwort gegeben wird oder gegeben werden soll. Ein **Bezug zu einer natürlichen Person fehlt** auch regelmäßig bei Angaben zu größeren Organisationen, Strukturen, zu einer Infrastruktur oder zu Technik im Gesundheitsbereich. Wir befinden uns dann nicht in einem rechtsfreien Raum; möglich ist, dass weitere Rechtsgebiete anwendbar sind.

Auch wenn ein Personenbezug besteht, sind im Sinne einer Einheit der Rechtsordnung weitere Rechtsgebiete relevant. Hierbei entstehen oft Wechselbeziehungen. Die **geschützten Rechtsgüter** sind im Rahmen von Abwägungen mit zu berücksichtigen.

9.1 Urheberrecht

Bei der rechtlichen Bewertung von Big Data kann das Urheberrecht relevant sein. Dieses honoriert persönliche geistige Schöpfungen **Werkschaffender** (§ 2 Abs. 2 UrhG) und schützt deren vermögensrechtliche und ideelle Interessen (§ 11 UrhG). Dabei kommt es nicht darauf an, ob das Werk als Auftrag- oder Arbeitnehmer für einen anderen geschaffen wurde. Damit verwandt sind Leistungsschutzrechte, bei denen eine ökonomisch schützenswerte persönliche Leistung erbracht wurde, etwa von Künstlern (§§ 73 ff. UrhG) oder wissenschaftlichen Autoren (§ 70 UrhG). Andere Leistungsschutzrechte honorieren wirtschaftliche, technische oder organisatorische Leistungen (§§ 85 ff. UrhG: Tonträgerhersteller, Sendeunternehmen, Presseverleger). Ein auf die Richtlinie 96/9/EG zurückgehender Schutz für Hersteller von Datenbanken schützt deren Investition in Datenspeicher- und Datenverarbeitungssysteme (§§ 87a ff. UrhG).

Bei Big Data handelt es sich regelmäßig nicht um **persönliche geistige Schöpfungen** (§ 2 Abs. 2 UrhG). Auch ein Schutz als Sammel- bzw. Datenbankwerk (§ 4 UrhG) kommt nicht in Frage, da bei Big Data der kreative Akt fehlt. Ein solcher Schutz ist für die Begriffsauswahl in einem medizinischen Lexikon[750] oder für die Festlegung einer Ordnung in einem Bericht über Umsätze der pharmazeutischen Industrie[751] anerkannt. Die Analyse durch einen Algorithmus ist dagegen kein schöpferischer Akt.

---

749 Weichert in Reiffenstein/Blaschek S. 255.
750 OLG Hamburg 22.2.2001 – 3 U 247/00, GRUR 2001, 831 ff.
751 OLG Frankfurt 17.9.2002 – 11 U 67/00, MMR 2003, 46.

Als schutzfähiges Werk kommt aber wohl Software in Betracht (§§ 69a ff. UrhG). Der Schutz von Programmen nach § 69a Abs. 1 UrhG bezieht sich nicht auf Datenbankstrukturen, auf einzelne Daten oder Schnittstellen. § 69e UrhG soll ermöglichen, dass Hersteller konkurrierender Programme die nötigen Informationen erhalten, um interoperable Anwendungen, wie sie bei Big Data oft erforderlich sind, entwickeln zu können.

Das Leistungsschutzrecht für den Hersteller einer Datenbank nach § 87a Abs. 1 S. 1 UrhG bezieht sich auf Sammlungen von Werken, Daten oder sonstige unabhängige Elemente, die systematisch oder methodisch angeordnet und einzeln zugänglich sind und deren Beschaffung, Überprüfung oder Darstellung eine nach Art bzw. Umfang wesentliche Investition erfordert. Die Rechtsprechung stellt an die Höhe der geschützten Investition keine hohen Anforderungen.[752] Die Anwendung dieser Schutzregelungen auf Big-Data-Applikationen ist regelmäßig nicht gegeben. Wohl aber ist es denkbar, dass Daten aus geschützten Datenbanken in Big-Data-Analysen einfließen. Dadurch erweitert sich aber nicht der Schutzbereich des § 87a UrhG. Das Erzeugen neuer Daten unterfällt hierunter ebenso wenig wie die Analysemethode; allenfalls hinsichtlich der Datenbeschaffung kann die Norm relevant werden.[753] Sind Daten für Big Data lediglich ein Nebenprodukt eines anderen Kerngeschäfts, so kann § 87a UrhG nicht zur Anwendung kommen. Honoriert werden soll mit der Regelung aber wohl die Investition in fortschrittliche Informationssysteme, die Daten zusammenführen und zugänglich machen.

9.2 Betriebs- und Geschäftsgeheimnisse

Grundsätzlich können gesundheitsrelevante Daten Betriebs- und Geschäftsgeheimnisse sein, wenn sie in Big Data eingeführt werden oder das Analyseergebnis von Big Data sind. Betriebs- und Geschäftsgeheimnisse genießen gemäß den §§ 17-19 UWG strafrechtlichen Schutz. Art. 39 Abs. 1 des Übereinkommens über handelsbezogene Aspekte der Rechte des geistigen Eigentums (TRIPS)[754] verlangt einen Mindestschutz. In der EU besteht die Richtlinie 2016/943, die von den Mitgliedstaaten einen angemessenen rechtlichen Schutz von Betriebs- und Geschäftsgeheimnissen einfordert. Als Geschäftsgeheimnis wird angesehen, was nicht offenkundig, sondern nur einem begrenzten Personenkreis bekannt ist und vom Unternehmen nach dem bekundeten, auf wirtschaftlichen Interessen basierenden Erwägungen geheim gehalten werden soll.[755] Es muss ein konkreter Unternehmensbezug bestehen, der fehlt, wenn die Informationen die Sphäre Dritter betreffen.[756] Ein solcher Drittbezug besteht bei der Verarbeitung von personenbezogenen Daten, erst recht bei der Verarbeitung sensitiver Gesundheitsdaten (s. o. 8.16.2, 8.17.3). Generell ist ein Betriebs- und Geschäftsgeheimnis ausgeschlossen, wenn die Daten

752 BGH 1.12.2010 – I ZR 196/08, GRUR 2011, 725.

753 EuGH 9.10.2008 – C-203/02, Rn. 42; EuGH 9.11.2004 – C-444/02 Rn. 45 ff.; BGH 25.3.2010 – I ZR 47/08, GRUR 2010, 1005.

754 Anhang 1C des Übereinkommens zur Errichtung der Welthandelsorganisation (WTO) vom 15.04.1994, BGBl. II 1994 S. 1625.

755 BGH 26.2.2009 – 1 ZR 28/06, NJW 2009, 1420 = GRUR 2009, 604.

756 Köhler in Köhler/Bornkamm, UWG, 34. Aufl. 2016, § 17 Rn. 5.

offenkundig sind. Auch bei rechtswidriger Verarbeitung von Daten kann das Unternehmen regelmäßig keinen Geheimnisschutz für sich in Anspruch nehmen.

9.3 Dateneigentum

Seit wenigen Jahren wird eine politische Diskussion über eine bessere normative Verankerung von „Dateneigentum" geführt.[757] Hierzu äußerten sich politische Parteien im Rahmen des Bundestagswahlkampfs 2017 in ihren Parteiprogrammen teilweise positiv, teilweise kritisch. Die Diskussion, die auch unter dem Stichwort der „Datensouveränität" geführt wird, knüpft an der ökonomischen Verwertbarkeit digitaler Daten an.[758] Datensouveränität bzw. „digitale Souveränität" weckt Assoziationen zum Datenschutzrecht bzw. zum vom BVerfG in der Volkszählungsentscheidung 1983 grundrechtlich begründeten „Recht auf informationelle Selbstbestimmung"[759]. Subjekt dieser informationellen Selbstbestimmung ist ausschließlich der von einer Datenverarbeitung erfasste oder erfassbare Mensch, dem die datenschutzrechtlich Verantwortlichen gegenüberstehen. Das Subjekt der „ökonomischen Datensouveränität" in der politischen Diskussion ist aber weniger der datenschutzrechtlich Betroffene, sondern eher das Daten verarbeitende Unternehmen. Mit einem Eigentumsrecht an Daten erhofft man sich eine klarere Zuschreibung von Verfügungsrechten über Daten und damit eine Förderung von Datenmärkten. Datenschutzansprüche von Betroffenen werden eher als Hindernis der kommerziellen Nutzung von Daten angesehen.[760]

9.3.1 Datenverarbeiter als Dateneigentümer

Schwerpunkte der Diskussion über Dateneigentum liegen in der kommerziellen Nutzung von Daten im Mobilitäts- und im Gesundheitsbereich. Medizinische Forschende oder Behandlungseinrichtungen gehen oft fälschlich davon aus, dass die von ihnen erhobenen oder beschafften Daten auch ihnen gehören, dass es sich hierbei um ihr „digitales Eigentum" handele.[761] Datenschutz wird für die Kommerzialisierung gerade bei der hier bestehenden hohen Sensitivität als „Belastung" wahrgenommen.[762] Big-Data-Analyse-Ergebnissen im Gesundheitsbereich kommt zumeist ein hoher kommerzieller Wert zu. Diensteanbieter versuchen oft mit faktischen (v. a. technischen) Hindernissen, das Teilen von Gesundheitsdaten mit (anderen) Therapeuten, anderen Marktanbietern oder mit den Betroffenen zu bekämpfen.[763] Gerade im Gesundheitsbereich liegt es aber wegen der zumeist bestehenden engen Bindung an die Betroffenen nahe, diesen selbst die Verwaltung ihrer Daten und evtl. auch deren kommerzielle Verwertung zu überlassen.

---

757 Grützmacher CR 2016, 485; Specht CR 2016, 288; Zech CR 2015, 137; Dorner CR 2014, 617; kritisch zur Ökonomisierung aus ethischer und soziologischer Sicht Selke in Stiftung Datenschutz (2017) S. 163 ff.; Deutscher Ethikrat S. 27.

758 BMVI S. 3, 78 ff.; kritisch zum Souveränitätsbegriff Deutscher Ethikrat S. 21, 27 f., 132 ff.

759 BVerfG U. v. 15.12.1983 – 1 BvR 209/83 u. a. , NJW 1984, 419 ff.

760 BMVI S. 3; kritisch dazu vzbv, Verbraucher als „Eigentümer" von Mobilitätsdaten? Stellungnahme v. 3.11.2017.

761 Deutscher Ethikrat S. 66 f., 109 f; Ladeur DuD 2016, 362.

762 BMVI S. 120.

763 Schmundt, Geht euch nix an, Der Spiegel 32/2016, 105.

Das kommerzielle **Verfügungsrecht über Daten** kann aus dem Datenschutzrecht, dem Urheberrecht, dem Strafrecht (vgl. § 303a StGB), dem Lauterkeitsrecht, dem Leistungsschutzrecht oder generell aus dem Zivilrecht abgeleitet werden. Immateriell-rechtlich geschützt sind Werke der Literatur, Wissenschaft und Kunst, Datenbanken, Marken, Patente oder Design, Ideen, Knowhow, Geschäftskonzepte, Entdeckungen, Erfindungen, Software oder Software-Schnittstellen. Rechtliche Zuordnungen erfolgen datenspezifisch unternehmensbezogen (Betriebs- und Geschäftsgeheimnisse), im Hinblick auf die Datenverwertungsrechte (Urheberrecht) und mit Bezug zu der betroffenen Person (Datenschutzrecht), über das Eigentum am Datenträger (§ 903 BGB) sowie handlungsbezogen (geistige Schöpfung, Investition, Skripturakt).[764]

Die Zuordnung zum „**wirtschaftlich Berechtigten**" kann legitim sein, da die Generierung und die Pflege von Daten Kosten und Aufwand auslösen. Dieser Aufwand kann im „Skripturakt", wozu auch u. U. die Entwicklung und Produktion datengenerierender Gegenstände gehören kann, oder bei der Speicherung und weiteren Verarbeitung in der Schaffung eines entsprechend dem Urheberrecht geschützten Werkes gesehen werden.[765] Oft gerät dabei aber aus dem Blick, dass die Generierung nicht originär vom Skribenten finanziert wurde, sondern, z. B. über öffentliche Förderung oder Bereitstellung einer Infrastruktur durch die öffentliche Hand oder durch das Solidarsystem der gesetzlichen Krankenversicherung.[766]

9.3.2 Betroffene als ökonomisch Berechtigte

Die Diskussion, inwieweit **Betroffene als datenschutzrechtlich Berechtigte** ihre Daten (z. B. gegen unentgeltliche Nutzungsmöglichkeit eines Dienstes) kommerziell vermarkten können, wird seit vielen Jahren geführt.[767] Tatsächlich handelt es sich bei den meisten marktgängigen personenbezogenen Daten um die Ergebnisse von Kommunikationsvorgängen, bei denen ein individuelles ökonomisches Ausschließlichkeitsrecht eines Betroffenen nur schwer begründet werden kann. Die Vermarktung von Kommunikationsvorgängen ist nicht unbedingt förderlich für die soziale Interaktion, insbesondere wenn es sich um nicht-kommerzielle Kommunikation handelt.[768] Sozialer Austausch ist eine Grundbedingung für unser Gemeinwesen generell und für dessen demokratische Verfasstheit in Besonderem.

Dessen ungeachtet ist es seit Jahren Realität, dass in personenbezogener Datenverarbeitung (insbesondere bei Telemediendiensten) ein riesiges **Wirtschaftspotenzial** steckt. Sie ist Gegenstand kommerzieller Verträge. Nutzungsrechten an personenbezogenen Daten kommt ein ökonomischer Wert zu. Dies muss für die Betroffenen nicht schädlich sein. Es kann im Interesse des Betroffenen liegen, dass Dritte

764 S. o. 9.1, 9.2.
765 Übersicht zu den jeweiligen Ansätzen mit Eigenschaften und Nachteilen BMVI S. 103 ff.
766 Deutscher Ethikrat S. 67.
767 Dazu grundrechtsdogmatisch Weichert in Taeger/Wiebe, Informatik-Wirtschaft-Recht, Regulierung in der Wissensgesellschaft (Festschrift Kilian), 2004, S. 281-298; BMVI S. 48.
768 Simitis in Simitis § 4a Rn. 5 ff. m. w. N.

ihre Daten kommerziell nutzen. So kann es z. B. im Betroffeneninteresse liegen, dass dadurch eine Qualitätsverbesserung der Produkte erfolgt oder Betroffene – etwa im Rahmen einer Werbemaßnahme – gezielt angesprochen werden.

Die Betroffenen können durch die Kommerzialisierung der Nutzung ihrer eigenen Daten Geld oder geldwerte Leistungen erlangen. Mit der zunehmenden Kommerzialisierung der Gesundheitsdatenverarbeitung, insbesondere über das Internet, wird der „Körper und die Gesundheit in Datenform zur Ware".[769] Die sich daraus ergebenden positiven und negativen Effekte für den Einzelnen wie für die Gemeinschaft hängen zumeist von dem Kontext und dem Zweck sowie oft vom einzelnen Fall ab; eine pauschale Bewertung ist zumeist nicht möglich.

Wegen des Ungleichgewichts in dem Vertragsverhältnis zwischen Verbraucher und Unternehmen ist es aber eine Illusion zu glauben, dass der Verbraucher gerechte „Preise" aushandeln könnte.[770] Der Wert personenbezogener Daten ist extrem volatil und zumeist stark von individuellen Merkmalen wie z. B. der Kaufkraft des Betroffenen im Werbebereich oder der „Datenoriginalität" im Gesundheitsbereich abhängig. Die „Bepreisung" von Datensätzen setzt regelmäßig ein sehr weitgehendes Profiling voraus, so dass das Kommerzialisierungsinteresse des Betroffenen im Widerspruch steht zu dessen Interesse an der Datensparsamkeit (s. o. 8.12).

Für die kommerzielle Nutzung personenbezogener Daten kommt es in vielen Fällen nicht auf den individuellen Personenbezug an. Das Interesse besteht in den meisten Fällen nicht am Menschen als Person, sondern als Merkmalsträger. Zumeist genügt für den wirtschaftlichen Nutzen eine Trefferquote mit einer hinreichenden Wahrscheinlichkeit. Für die Werbeansprache genügen oft Responsequoten von wenigen Prozent. Im Bereich der Sicherheit kann gar ein Einmaltreffer hinsichtlich eines Störers oder Gefährders als ein Erfolg angesehen werden, wenn von diesem Treffer eine große (wirtschaftliche) Gefährdung oder sonstige Wirkung ausgeht. Im Gesundheitsbereich sind zwar zumeist die Besonderheiten des Einzelfalls bis ins Detail von großer Bedeutung. Dessen ungeachtet genügen für die kommerzielle Nutzung zumeist anonymisierte oder pseudonymisierte Datensätze.

Die Grundannahme für die Schaffung des Rechtsinstituts „Dateneigentum", nämlich dass die Datengenerierung einen zu honorierenden Aufwand verursacht, trifft in vielen Fällen nicht zu. Der Anfall von Daten ist oft ein zwangsläufiges Nebenprodukt der Erbringung eines (digitalen) Dienstes. Die Speicherung derart anfallender Daten sowie deren standardisierte Auswertung verursachen zumeist nur noch geringe wirtschaftliche Kosten, die in keinem Verhältnis stehen zu dem durch die Nutzung dieser Daten entstehenden Mehrwert. Die Kosten für den Verarbeitungsaufwand reduzieren sich zumeist im Verhältnis zur verarbeiteten Datenmenge, also je umfangreicher die Daten sowie die Zahl

769 Schramm in Stiftung Datenschutz (2016) S. 107.

770 Ablehnend aus weiteren Gründen auch BMVI S. 49 f., 91 ff., 94, 112 f.: Datenschutz sei vorrangig Abwehr- nicht Verfügungsrecht.

der Datensätze (der Betroffenen) werden. Je größer die Menge der Daten ist, desto komplexere Auswertungsmöglichkeiten eröffnen sich, woraus lukrative Geschäftsmodelle entwickelt werden können.

Wirtschaftliche Nutzungsrechte und „Eigentum" von Daten begründen ökonomische und politische Machtverhältnisse. Eine Anhäufung von ökonomischer (und damit auch politischer) Macht ermöglicht Wettbewerbsverzerrungen. Das Kartellrecht beginnt gerade erst damit, sich den damit verbundenen Angebotsbeschränkungen und Preisnachteilen für die Verbraucher zu befassen (s. u. 11.1.8).

Bei der Beurteilung der Frage, inwieweit Daten bzw. den Ergebnissen von Datenverarbeitung ein eigentumsähnlicher Status zugewiesen werden darf bzw. sollte, darf nicht außer Acht gelassen werden, dass mit dem Umfang der Daten und der Qualität der Datenverarbeitung die gesellschaftlichen Kosten ansteigen, die z. B. für die nötige staatliche Aufsicht, durch Bildungs- oder durch Infrastrukturmaßnahmen entstehen. Es besteht nicht nur eine Sozialpflichtigkeit des Eigentums, sondern auch von Datenverarbeitung, insbesondere bei komplexen und sensitiven Anwendungen. Bevor individuelle Ausschließlichkeitsrechte an Daten begründet werden, sollte deshalb dafür gesorgt werden, dass mit Erträgen der nötige staatliche bzw. gesellschaftliche Aufwand finanziert wird.[771]

9.3.3 Biopatente

Aus der medizinischen Forschung, insbesondere im genetischen Bereich, können unter Einsatz von Big Data patentierbare Erfindungen gemacht werden. Deren ökonomische Nutzung wird durch das Patentrecht geregelt. Grundlage für die Vergabe von Biopatenten in der EU ist die Richtlinie 98/44/EG aus dem Jahr 1998.[772] Die Voraussetzungen für ein Patent im biotechnologischen Bereich unterscheiden sich nicht von denen in anderen Bereichen: Die Erfindung muss neu und gewerblich anwendbar sein und einen erfinderischen Schritt beinhalten. Der menschliche Körper und die Entdeckung einzelner Bestandteile (z. B. Gene) sind von der Patentierung ausgeschlossen. Hingegen kann ein isolierter Bestandteil des menschlichen Körpers oder ein auf andere Weise durch ein technisches Verfahren gewonnener Bestandteil, einschließlich der Sequenz oder Teilsequenz eines Gens, eine patentierbare Erfindung darstellen.

Die menschlichen Gene BRCA1 und BRCA2 stehen im Zusammenhang mit Brust- und Eierstockkrebs. Bei Mutationen steigt die Wahrscheinlichkeit, an diesen Krebsarten zu erkranken, so dass der Feststellung solcher Mutationen eine große Bedeutung zukommt. Die Firma Myriad Genetics Inc. sequenzierte BRCA1 erstmals in Kooperation mit der

771 vzbv, Verbraucher als „Eigentümer" von Mobilitätsdaten, Stellungnahme 27.11.2017, S. 12 f., https://www.vzbv.de/sites/default/files/downloads/2017/11/06/17-11-03_stn_mobilitaetsdaten_final.pdf; vgl. Deutscher Ethikrat S. 177 f.

772 Richtlinie vom 6.7.1998 über den rechtlichen Schutz biotechnologischer Erfindungen, ABl. EG v. 30.7.1998, L 213/13; kritisch zur Patientierung von menschlichen Gensequenzen Weichert, DANA 2/2000, 8.

Universität von Utah. Beide stellten 1994 einen Antrag auf Patentschutz für isolierte DNA und für eine Screeningmethode. Die Diskussion um die damit verbundenen Patentierungen hatten eine ethische, eine ökonomische und eine politische Dimension. Es ging zunächst um die generelle Frage, inwieweit biotechnische, von menschlichen Gesundheitsdaten abgeleitete Erfindungen überhaupt patentierbar sein können. Zudem wurde befürchtet, dass ein Patentschutz die Weiterentwicklung von und den Zugang zu Diagnosemethoden erschweren würde. 2004 wurden diagnostische Methoden in Bezug auf BRCA1 von der Patentierung ausgeschlossen. Mit Urteil vom 13.6.2013 verbot der Supreme Court der Vereinigten Staaten von Amerika (USA) in einer Grundsatzentscheidung Patente auf menschliches Erbgut, das als „Produkt der Natur" nicht patentiert werden könne. Künstlich nachgeahmtes Erbgut, sogenannte cDNA, sei von dem Verbot aber nicht betroffen, „da es nicht von der Natur hergestellt wird". Vorausgegangen war dem Urteil eine Klage von Krebspatienten, Medizinern und Genforschern unter dem Dach der Bürgerrechtsgruppe American Civil Liberties Union (ACLU).[773]

Das europäisches Recht konkretisierende deutsche Patentgesetz (PatG)[774] stellt sicher, dass ein Patent nur für Erfindungen, nicht für Entdeckungen möglich ist. Menschliches Material, das mit einem technischen Verfahren isoliert oder neu hergestellt wird, kann gemäß § 1a Abs. 2 PatG patentiert werden, nicht aber die bloße Entschlüsselung eines Gens oder seiner Teile. 2013 wurde im deutschen Patentgesetz in § 2a Abs. 1 Nr. 1 PatG im Wege einer klarstellenden Konkretisierung festgestellt, dass auch „die ausschließlich durch solche (im Wesentlichen biologischen) Verfahren gewonnenen Tiere und Pflanzen" nicht patentiert werden können. Dies gilt auch für das zu ihrer Erzeugung bestimmte Material wie Saatgut, Sperma, Eizellen und Embryonen.

9.3.4 Konsequenzen für das „Dateneigentum"

Die Analogie zwischen Eigentum und Daten ist vom Grundansatz falsch. Daten haben als Informationen entweder eine persönliche oder eine gesellschaftliche Funktion. Technisch sind Daten beliebig reproduzierbar. Ihre ökonomische Nutzbarkeit ergibt sich aus dem Verarbeitungskontext, nicht aus dem Datum selbst. Für die Regulierung von Datenmärkten kommt es daher nicht auf die Schaffung eines Ausschließlichkeitsrechtes an Daten an, sondern auf die präzise Festlegung von Verfügungs- und Nutzungsrechten. Besteht ein öffentliches Interesse an einer allgemeinen Verfügbarkeit, so muss nicht die Zugangsbeschränkung, vielmehr müssen rechtlich Zugangsrechte begründet werden.

10 Spezifische Anwendungen

Nachdem die grundsätzlichen Aspekte von Big Data im Gesundheitsbereich und die dafür geltenden rechtlichen Regeln behandelt wurden, sollen im Folgenden besondere Aspekte, insbesondere Anwendungsfelder näher beleuchtet werden.

---

773 Welter, Keine Patente auf menschliche Gene in Amerika, www.faz.net 13.6.2013.

774 PatG v. 16.12.1980, BGBl. I 1981, S. 1, zuletzt geändert durch G. v. 12.5.2017, BGBl. I S. 1121.

10.1 Transplantationsmedizin

Die Funktionalität und Gerechtigkeit des Verfahrens der Zuteilung von menschlichen Organen zum Zweck der Transplantation ist von der Verarbeitung einer großen Zahl belastbarer sensitiver Daten abhängig. Die Entnahme von Organen erfolgt entweder auf Basis der Einwilligung des Spenders (§ 3 Transplantationsgesetz – TPG) oder der Zustimmung der Angehörigen (§ 4 TPG). § 9a Abs. 2 Nr. 1 TPG verpflichtet die Entnahmekrankenhäuser, explantationsgeeignete Patienten der Koordinierungsstelle der Deutschen Stiftung Organtransplantation (DSO), zu melden. § 11 Abs. 4 TPG verpflichtet zur Kooperation zwischen den Transplantationszentren, den Entnahmekrankenhäusern und der DSO. Gem. § 11 Abs. 1 lit. 1 S. 2 Nr. 4 TPG erstellt die Koordinierungsstelle geeignete Verfahrensanweisungen zur Sicherstellung der rechtzeitigen Übermittlung der Angaben zur Organ- und Spendercharakterisierung. Die Daten werden verschlüsselt und mit einer die Rückverfolgbarkeit sichernden Kenn-Nummer versehen und an die Vermittlungsstelle Eurotransplant (ET) zur Zuteilungsentscheidung übermittelt. Die Entscheidung von Eurotransplant zum geeignetsten Organempfänger erfolgt auf der Grundlage eines ET-Handbuchs. Zwecks Einschätzung der Eignung der angebotenen Organe für die Transplantationskandidaten und Kontrolle der Vergabeprozesse erhalten die Transplantationszentren über ein Spenderpseudonym elektronisch Einsicht in detaillierte Daten zur Organ- und Spendercharakterisierung.[775] Diese Daten unterliegen einer strengen Zweckbindung (§ 7 Abs. 1 TPG).[776] Bei der Organvergabe kommt Big Data nicht zum Einsatz.

Am 1.11.2016 trat das Gesetz zur Errichtung eines Transplantationsregisters[777] in Kraft, mit dem die Regeln zur Aufnahme der Warteliste, zur Vermittlung, zur Organ- und Spendercharakterisierung, zur Qualitätssicherung, zur Bewertung von Zwischenfällen sowie zur Überwachung von Organspenden und Transplantationen verbessert werden soll (§ 15a TPG). Insofern sind Organtransplantationen ein anschauliches Beispiel dafür, welche hohe Lebensrelevanz die Verarbeitung von Gesundheitsdaten haben kann, welche Bedeutung dabei die Auswertung der Daten hat und welche Zielkonflikte ausgeglichen werden müssen. So steht die Dringlichkeit einer Transplantation in einem Spannungsverhältnis dazu, eine größtmögliche Überlebensdauer von Organen und Empfängern (Erfolgsaussicht) zu erreichen, da die Dringlichkeit und die gesundheitliche Vorschädigung mit der Wartedauer zunehmen.[778] „Objektive“ Vergabekriterien und Diskriminierungsfreiheit sind essenziell, weshalb Vollständigkeit, Integrität und Richtigkeit (Validität) der Daten sowie die Relevanz der Daten von großer Bedeutung sind. Es kommt nicht von ungefähr, dass Datenmanipulationen in diesem Bereich zu einem der größten Medizinskandale der jüngeren Vergangenheit wurden.[779]

775 Augsberg MedR 2016, 701.
776 Schneider S. 60.
777 G. v. 11.10.2016, BGBl. I S. 2233.
778 Augsberg MedR 2016, 704.
779 Rosenau, MedR 2016, 706.

Neben dem gesetzlich festgelegten administrativen Verfahren bestehen bereichsspezifische Datensammlungs- und Datenaustauschprogramme. So diente das von der EU-Kommission finanzierte EFRETOS-Projekt (European Framework for Evaluation on Organ Transplants) der Gewinnung eines Überblicks zu Qualität und Sicherheit von Organtransplantationen durch das Zusammenführen nationaler Daten. Der Arbeitskreis „Nierentransplantation im Kindes- und Jugendalter" der Gesellschaft für Pädiatrische Nephrologie" (GPN) hat ein webbasiertes CERTAIN (Cooperative European Pedriatic Renal Transplant Initiative) Registry[780] aufgebaut, um durch eine flächendeckende Zusammenführung von Daten die Forschung zu unterstützen.[781]

Es ist nachvollziehbar, dass angesichts der Relevanz der Datenauswertung die Unterregulierung im TPG hinsichtlich der Vorgaben für das Allokationsverfahren (Zuweisungs- und Vergabeverfahren), der demokratischen Legitimation der eingebundenen Stellen, etwa der Bundesärztekammer und der Kontroll- und Aufsichtsmöglichkeiten beklagt und kritisiert wird.[782] Analytics mit solchen Gesundheitsdaten bedarf der gesetzlichen Legitimation, in der Vorgaben hinsichtlich der wesentlichen Aspekte einer effektiven Implementierung, der Evaluation und der Kontrolle festgelegt werden.

10.2 Arzneimittelüberwachung

Das erste Arzneimittelgesetz (AMG) in Deutschland stammt aus dem Jahr 1961. Es enthielt keine Verpflichtung der Prüfung von Wirksamkeit und Sicherheit der Medikamente, sondern sah nur eine Registrierung vor. 1964 wurde § 21 AMG um zwei Absätze 1a und 1b ergänzt, die die Prüfung der Arzneimittel durch vorklinische und klinische Studien vorschrieb. Die Hersteller mussten von da an eine bedeutsame schriftliche Versicherung liefern, dass die Arznei entsprechend dem jeweiligen Stand der wissenschaftlichen Erkenntnisse ausreichend und sorgfältig geprüft worden sei. Mit der „Richtlinie über die Prüfung von Arzneimitteln" von 1971 wurden Grundsätze für die pharmakologisch-toxikologische und klinische Prüfung von Arzneimitteln festgelegt. Das Bundesgesundheitsamt wurde angewiesen, nur noch Arzneimittel zu registrieren, die nach der Richtlinie geprüft wurden. Nach dem Conterganskandal und umfassenden Diskussionen über die Arzneimittelsicherheit wurde das AMG mit Datum vom 24.8.1976 neu gefasst.[783] Die Zulassungsverfahren und die Überwachung erfolgt über das Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) mit Sitz in Bonn.[784]

Das AMG schreibt nun ein Zulassungsverfahrens für Arzneimittel vor, bei dem der Nachweis von Qualität, Wirksamkeit und Unbedenklichkeit erbracht werden muss (§§ 21 ff. AMG). Der Arzneimittelverkehr (Vertrieb, Abgabe) wird strenger reguliert und überwacht (§§ 43 ff. AMG). Es wurde ein Informationssystem aufgebaut, um

780 www.certain-registry.eu.
781 Augsberg MedR 2016, 701.
782 Augsberg MedR 2016, 704 f.
783 AMG, neugefasst am 12.12.2005, BGBl. I 3394, zuletzt geändert durch G. v. 18.7.2017, BGBl. I 2757.
784 https://www.bfarm.de.

Arzneimittelrisiken zu sammeln, auszuwerten und Abwehrmaßnahmen ergreifen zu können (Pharmakovigilanz, §§ 62 ff. AMG).

Parallel zur nationalen Gesetzgebung wurden in Europa Vorgaben gemacht, mit denen eine Harmonisierung des Arzneimittelrechts in der Europäischen Union angestrebt wird. Die wesentlichen Regelungen finden sich in Richtlinie 2001/83/EG[785] und in der Verordnung (EG) Nr. 726/2004[786]. Die jüngste Regelung vom 16.4.2014 befasst sich mit der Pharmakovigilanz und dem Schutz vor Arzneimittelfälschungen.[787] Die Europäische Arzneimittel-Agentur (EMA) mit Sitz in London (künftig Amsterdam) hat die Aufgabe, wissenschaftliche Gutachten für die Gemeinschaftsorgane und die EU-Mitgliedstaaten zur Arzneimittel-Bewertung zu erstellen.[788]

Unter Pharmakovigilanz versteht man die laufende systematische Überwachung der Arzneimittelsicherheit im Sinne einer Sammlung und Erfassung von unerwünschten Arzneimittelwirkungen, um gegebenenfalls Maßnahmen zur Risikominimierung ergreifen zu können. Ärzte sind gemäß § 6 MBOÄ verpflichtet, unerwünschte Arzneimittelwirkungen an die „Arzneimittelkommission der deutschen Ärzteschaft“ bzw. an das BfArM zu melden. Auch Patienten können Meldungen vornehmen (§ 62 Abs. 2 S. 1 AMG). Die Pharmaunternehmen sind verpflichtet, sämtliche Informationen wissenschaftlich auszuwerten, die sich auf sie zugelassene Medikamente beziehen, diese zu dokumentieren und Verdachtsfälle über Nebenwirkungen zu melden (§ 63b AMG). Diese Verdachtsfälle schwerwiegender Nebenwirkungen sind innerhalb bestimmter Fristen in einem standardisierten Format an das BfArM zu übermitteln. Das BfArM wertet die Daten aus. Hierfür hat es eine Forschungsabteilung. Zudem speist es die Originaldaten der Meldungen wie auch die Auswertungsergebnisse in eine zentrale Datenbank bei der EMA ein (EudraVigilance).[789] Sämtliche Meldungen erfolgen pseudonymisiert unter präziser Angabe der für die Beurteilung der Wirkung relevanten Parameter.[790]

Meldungen über Arzneimittelwirkungen erfolgen auch in pseudonymisierter Form nach US-amerikanischem Recht gegenüber der dortigen Gesundheitsbehörde FDA. Die FDA sammelt weltweit Meldungen in seinem Center for Drug Evaluation and Research (CDER) und liefert vierteljährlich Berichte aus, in welche die Daten aus wissenschaftlichen Studien,

---

785 Richtlinie v. 6.11.2001, zur Schaffung eines Gemeinschaftskodexes für Humanarzneimittel, ABl. EG v. 28.11.2001, Nr. L 311 v. 28.11.2001 S. 0067 – 0128.

786 Verordnung v. 31.3. 2004 zur Festlegung von Gemeinschaftsverfahren für die Genehmigung und Überwachung von Human- und Tierarzneimitteln und zur Errichtung einer Europäischen Arzneimittel-Agentur, ABl. EG v. 30.4.2004, Nr. L 136 S. 0001 – 0033.

787 Verordnung v. 16.4.2014, über klinische Prüfungen mit Humanarzneimitteln, ABl. EU v. 27.5.2014, L 158/1.

788 Wissenschaftlicher Dienst des Europäischen Parlaments, Arzneimittel in der EU, April 2015 – PE 554.174.

789 § 63e AMG, Art. 107i-107k Richtlinie 2001/83/EG.

790 Meldebogen unter https://www.bfarm.de/SharedDocs/Formulare/DE/Arzneimittel/Pharmakovigilanz/aa-uaw-melde-bogen.pdf?__blob=publicationFile&v=17; https://www.akdae.de/Arzneimittelsicherheit/UAW-Meldung/UAW-Berichtsbogen.pdf

aus Meldungen von Leistungserbringern, Patienten, Verteilern und Pharmaunternehmen sowie aus wissenschaftlichen Veröffentlichungen einfließen. Das vierteljährliche Meldeaufkommen bewegt sich zwischen 300.000 und 400.000 Berichten. Anders als das BfArM und die EMA stellt die FDA ihre Einzeldatensätze allgemein zur weiteren Nutzung und Auswertung zur Verfügung. Diese Daten werden in Deutschland u. a. von OpenVigil der Universität Kiel qualitätsgesichert ausgewertet und in aufbereiteter Form über das Netz zur Verfügung gestellt.[791]

Bei der Durchführung klinischer Studien sind die §§ 40 ff. AMG zu beachten. Gemäß § 40 Abs. 1 Nr. 3 lit. c AMG darf eine klinische Prüfung bei Menschen nur durchgeführt werden, wenn die Betroffenen umfassend informiert wurden und ihre Einwilligung erteilt haben.[792] Bei klinischen Prüfungen, der Pharmakovigilanz und der Bekämpfung von Arzneimittelfälschungen kommt Big Data nach einheitlich festgelegten Standards zur Anwendung. Bei der Klinischen Prüfung gilt die „Verordnung über die Anwendung der Guten Klinischen Praxis bei der Durchführung von klinischen Prüfungen mit Arzneimitteln zur Anwendung am Menschen“ (Good Clinical Practice – GCP-Verordnung).[793] Mit der Einführung der personalisierten Medizin ergibt sich eine teilweise Ablösung von der bisherigen indikationsorientierten Medizin, bei welcher der individuelle Patient in den Mittelpunkt gelangt.[794]

Die Auswertung der Wirksamkeit von Arzneimitteln ist nicht nur eine Frage des Gesundheitsschutzes der Patienten, sondern auch einer der Wirtschaftlichkeit. Mit dem Arzneimittelmarktneuordnungsgesetz (AMNOG)[795], ein Artikelgesetz zur Änderungen u. a. des SGB V und des AMG, wird versucht, die Kosten für die Gemeinschaft an der Wirksamkeit der Arzneimittel auszurichten und dadurch die Ausnutzung der Marktmacht durch Pharmaunternehmen einzuschränken.

10.3 Medizinprodukte

Bei medizinischen, im ärztlichen Bereich eingesetzten IT-Anwendungen handelt es sich um Medizinprodukte, die vor ihrem Einsatz gemäß dem Medizinproduktegesetz (MPG) ein sog. Konformitätsverfahren durchlaufen müssen, in dem der Hersteller nachweist, dass das Produkt sicher ist und die technischen wie medizinischen Anforderungen wie vorgesehen erfüllt.[796] Das MPG setzt drei europäische Richtlinien um und zwar für aktive implantierbare medizinische Geräte[797], für In-vitro-Diagnostika[798] und für sonstige

791 http://openvigil.sourceforge.net/.
792 Schneider S. 68 f.
793 Verordnung über die Anwendung der Guten Klinischen Praxis v. 9.8.2004, BGBl. I S. 2081, zuletzt geändert durch G. v. 19.10.2012, BGBl. I S. 2192.
794 Timm MedR 2016, 684 ff.
795 G. v. 22.12.2010, BGBl. I S. 2262.
796 Deutscher Ethikrat S. 18; Strategy/pwc S. 114 ff.
797 Richtlinie 90/385/EWG v. 20.6.1990, ABl. EG 1990 Nr. L 189/17.
798 Richtlinie 98/79/EG v. 27.10.1998, ABl. EG 1998 Nr. L 331/1.

Medizinprodukte[799]. 2017 traten die Verordnungen für Medizinprodukte[800] und für In-vitro-Diagnostika[801] in Kraft, die nach einer drei- bzw. einer fünfjährigen Übergangszeit verpflichtend anzuwenden sind.

Gemäß § 3 Nr. 1 MPG sind Medizinprodukte zur diagnostischen oder therapeutischen Zwecken bestimmte Instrumente, einschließlich Apparate, Vorrichtungen und Software, zur Anwendung für Menschen zur Erkennung, Verhütung, Überwachung, Behandlung oder Linderung von Krankheiten und Behinderungen. Maßgeblich ist, ob der Hersteller das Produkt „für einen medizinischen Zweck bestimmt" hat.[802] Erwägungsgrund 6 der Richtlinie 2007/47 stellt klar, dass Software für allgemeine Zwecke kein Medizinprodukt ist, auch wenn sie im Zusammenhang mit der Gesundheitspflege genutzt wird. Ein Smartphone ist danach kein Medizinprodukt, wohl aber ein Verfahren oder ein Gegenstand, mit dem ärztliche Feststellungen gemacht werden, z. B. zur medizinischen Bestimmung der Zuckerwerte oder des Herzrhythmus. Das Gesetz sieht ausdrücklich vor, dass auch Software ein Medizinprodukt sein kann.

Die Abgrenzung zwischen Medizinprodukten und gesundheitsbezogenen Lifestyle- und Fitnessprodukten ist nicht immer eindeutig. Auslegungshilfen geben die rechtlich unverbindlichen „Leitlinien der Europäischen Kommission zu Stand-alone-Software"[803] und das durch die EU-Kommission veröffentlichte Handbuch zur Abgrenzung von Medizinprodukten.[804] Für die Einstufung als Medizinprodukt genügt es nicht, dass Gesundheitsdaten erfasst und verarbeitet werden. Voraussetzung ist vielmehr, dass die Verarbeitung der Behandlungsunterstützung dient. Erfasst wird z. B. Software, die Patientendaten erfasst und auswertet, um einen Diagnose- oder Therapievorschlag zu machen, eine Medikationsdosis zu errechnen oder Laborwerte mit Referenzwerten abzugleichen. Wird ein Produkt auch zur Behandlung eingesetzt, ohne dass es hierfür bestimmt ist, so handelt es sich noch nicht um ein Medizinprodukt.[805]

Anders als Arzneimittel bedürfen Medizinprodukte keiner staatlichen Zulassung, sondern lediglich einer Zertifizierung (§ 6 MPG). Vor dem Inverkehrbringen des Medizinprodukts muss dieses einer Risikoklasse zugewiesen werden. Medizinprodukte dürfen nur mit einer CE-Kennzeichnung in den Verkehr gebracht werden.[806] Das Medizinprodukt muss den in Anlage I zur Medizinprodukterichtlinie genannten Anforderungen genügen (§ 7 MPG).

---

799 Richtlinie 93/42/EWG v. 14.6.1993, ABl. EG 1993, Nr. L 169/1, mit Richtlinie 93/42/EWG novelliert über Richtlinie 2007/47/EG v. 5.9.2007, ABl. EU 2007 Nr. L 247/21.

800 Verordnung (EU) 2017/745 v. 5.4.2017, ABl. EU 2017 Nr. L119//1.

801 Verordnung (EU) 2017/746 v. 5.4.2017, ABl. EU 2017 Nr. L 119/176.

802 EuGH U. v. 22.11.2012, C-219/11, Rn. 16, 17, 33; EuZW 2013, 117; Deutscher Ethikrat S. 99.

803 Guidelines on the Qualification and Classification of Stand Alone Software Used in Healthcare within the Regulatory Framework of Medical Devices, 2012.

804 Manual on borderline and classification in the Community Regulatory framework for medical devices, version 1.17, 9/2015.

805 Deutscher Ethikrat S. 100.

806 Raum in Stiftung Datenschutz (2017) S. 129; Rübsamen MedR 2015, 485 ff.; Ortner/Daubenbüchel, NJW 2016, 2919; ULD (2010) S. 132 ff.

Hierfür ist eine produktspezifische Risikobewertung nötig. Zudem muss ein Konformitätsbewertungsverfahren mit der CE-Kennzeichnung durchlaufen werden (§ 6 Abs. 1, 2 MPG), wozu u. U. eine klinische Prüfung durchgeführt werden muss, die der Zustimmung einer Ethikkommission und der Genehmigung einer zuständigen Bundesoberbehörde bedarf. Die Anforderungen und das Verfahren werden nach Risikoklassen differenziert. Je nachdem, in welche Risikoklasse ein Produkt gemäß § 13 MPG eingestuft wird, kann der Hersteller dies in eigener Verantwortung durchführen (Risikoklasse I), oder er muss eine „benannte Stelle" beteiligen. Software sowie Hardware mit integrierter Software können als Medizinprodukte eingestuft werden. So fällt z. B. ein Online-Check zu Rückenschmerzen der Fa. Kaia unter die Kategorie I. Die App stellt Fragen, setzt eine fachärztliche Behandlung voraus und animiert mit kleinen Videos zu Bewegung und Entspannung bzw. vermittelt Wissen. Die Therapievorschläge sind abhängig von den erteilten Antworten. Das Produkt, das Anfang 2017 an den Start gegangen ist, hatte schon nach 8 Monaten über 10.000 Nutzer.[807]

Ergeben sich bei der Nutzung von Medizinprodukten unerwünschte Nebenwirkungen, so sind die Ärzte – ebenso wie bei Arzneimitteln – gemäß § 6 MBOÄ zu einer Meldung an das BfArM verpflichtet. Das BfArM betreibt gemäß § 29 MPG ein umfassendes Medizinprodukte-Beobachtungs- und -Meldesystem, in dem die pseudonymisierten Informationen vergleichbar zu Arzneimitteln ausgewertet, genutzt und veröffentlicht werden.

Gemäß § 2 Abs. 4 MPG bleiben die Rechtsvorschriften über Geheimhaltung und Datenschutz unberührt.[808] Zielsetzung des Medizinprodukterechts ist die Gewährleistung von Sicherheit und Gesundheitsschutz.[809] Bezugspunkte sind nicht die informationstechnische oder die persönlichkeitsrechtliche Sicherheit, sondern die körperliche und psychische Unversehrtheit. Insofern kann nach dem Medizinprodukterecht – bisher – keine umfassende Datenschutzprüfung vorgenommen werden. Wohl aber können datenschutzrechtliche Aspekte einbezogen werden, die Gesundheitsrelevanz haben. Dies trifft insbesondere für Fragen der Datensicherheit zu, da Manipulationen und sonstige Verletzungen der Schutzziele zu Falschdiagnosen und -behandlungen führen können wie auch direkt oder indirekt zu körperlichen und seelischen Schäden. Mit der ab 2018 vorgesehenen förmlichen Datenschutzzertifizierung (Art. 42 DSGVO) können die Zertifikate für Medizinprodukte und für den Datenschutz sich gegenseitig ergänzen.

Wird bei Medizinprodukten Big Data eingesetzt, so setzt dies eine umfassende Prüfung des gesamten informationstechnischen Prozesses von der Erfassung bzw. Eingabe von Daten, deren Speicherung und Analyse bis hin zur Ausgabe eines Ergebnisses oder der Bewirkung eines Vorgangs voraus. Eine Trennung zwischen datenschutzrechtlichen und Sicherheits-

807 Dostert, Downloads gegen den Schmerz, SZ 11.8.2017, 14.
808 Schneider S. 61 f.
809 ErwGr 2 u. 3 RL 93/42; vgl. Raum in Stiftung Datenschutz (2017) S. 129; Ortner/Daubenbüchel NJW 2016, 2919 ff.

Anforderungen ist in der Praxis nicht sinnvoll und zumeist auch gar nicht möglich. Es entspricht daher schon heutiger Rechtslage, dass im Rahmen eines Konformitätsbewertungsverfahrens eine umfassende Überprüfung der Rechtskonformität erfolgen muss, die neben der medizinischen Sicherheit im engeren Sinne auch den Datenschutz sowie die informationstechnische Sicherheit, deren rechtliche Grundlagen im BSI-G geregelt sind, einbezieht.[810]

10.4 Ambient Assisted Living

Ambient Assisted Living (AAL), zu Deutsch etwa „umgebungsunterstütztes Leben", dient der technischen Unterstützung älterer oder behinderter Menschen im Haushalt. Dazu wird die Wohnung des Menschen mit Notruf- und sonstigen Kommunikationseinrichtungen, Assistenzrobotern, Sturzmatten sowie weiteren technischen Angeboten ausgestattet, die es einer Person trotz körperlicher oder geistiger Einschränkungen ermöglicht, weitgehend ein selbständiges Leben zu führen.[811] Um eine möglichst hohe Funktionalität in Form von Assistenz für den Betroffenen zu erlangen und dabei zugleich einen möglichst geringen Aufwand zu verursachen, müssen eine Vielzahl von Vitalitäts- und Umweltdaten zusammengeführt, ausgewertet und assistenzgerecht genutzt werden. Dabei spielen Gesundheitsdaten eine, wenn nicht gar die zentrale Rolle. Hierbei kann es sich zusätzlich auch um Berufsgeheimnisse oder Sozialdaten handeln.[812] Die Sensitivität der Anwendungen wird dadurch weiter erhöht, dass zumeist laufend Daten bei evtl. alltäglichen Verrichtungen erfasst werden und diese Erfassung im räumlichen Schutzbereich der eigenen Wohnung (vgl. Art. 13 GG, Art. 7 GRCh) erfolgt. Hierdurch wird möglicherweise in den Kernbereich privater Lebensgestaltung eingegriffen (s. o. 6.5).

Die hohe Sensitivität der Datenverarbeitung setzt allergrößte **Transparenz und Bestimmungsmöglichkeit** für die Betroffenen voraus. Darüber hinausgehend spielt der Grundsatz der Erforderlichkeit bzw. der Datensparsamkeit eine wichtige Rolle. Frühestmögliche Aggregierung und Datenlöschung sind ebenso angesagt wie die Vermeidung jeder Form von unnötiger Datenübermittlung. Da die Anwendungen und Dienstleistungen beim AAL regelmäßig nicht aus einer Hand erbracht werden können, ist eine präzise Festlegung der Verantwortlichkeiten geboten.[813]

10.5 Telematiktarife bei Versicherungen

Die Belohnung von gesundheitsbewusstem Verhalten durch materielle Vergünstigungen bzw. durch billigere Tarife ist gesellschaftspolitisch wie rechtlich umstritten. **Zugunsten solcher Angebote** wird das Verursacherprinzip bemüht: Diejenigen, die gesund leben, belasten das Gesundheitssystem weniger und verursachen, so die Annahme, weniger Kosten zugunsten der gesamten Versicherungsgemeinschaft. Für ein solches soziales

---

810 Ortner/Daubenbüchel NJW 2016, 2920 f.
811 Münch S. 55 f.; ULD (2010) S. 16 ff.
812 ULD (2010) S. 81 ff.
813 Ausführlich und detailliert ULD (2010) S. 165 ff.

Verhalten soll ein individueller Anreiz geschaffen werden. Big Data ermöglicht eine genaue Segmentierung von Kunden durch zusätzliche Informationen.[814]

Bei der rechtlichen Bewertung des Einsatzes von Telematik ist zwischen **gesetzlichen und privaten Versicherungen** zu unterscheiden. Gesetzliche Versicherungen zielen auf eine existenzielle Grundsicherung ab, die allen Menschen in gleichem Maße zusteht. Durch die Regulierung übernimmt der Staat seine soziale Verantwortung für alle Mitglieder der Gesellschaft (s. o. 6.15). Bei Privatversicherungen ist dagegen die Referenzgruppe für Solidarität die Gemeinschaft der Versicherten eines Unternehmens bzw. einer Unternehmenssparte. Für das Unternehmen ist der Profit ein für die Vertragsbedingungen gestaltungsrelevanter Aspekt, was dazu führt, dass die Prämien risikoadäquat zu bemessen sind.[815]

Im Bereich der GKV werden Krankenkassen nicht nur berechtigt, sondern aufgefordert, „qualitätsgesicherte Angebote zur Förderung eines gesundheitsbewussten Verhaltens" einzurichten, wobei ausdrücklich die Gewährung von Boni vorgesehen ist (§ 65a SGB V). Die Bundesregierung äußerte sich zu **Bonusprogrammen** im Versicherungsbereich wie folgt: „Boni können das Ziel unterstützen, die individuelle Gesundheit zu erhalten und bessern und die Solidargemeinschaft von Ausgaben für Krankenhausbehandlungen entlasten. Eine Aushöhlung des Solidarprinzips, das in der gesetzlichen Krankenversicherung (GKV) insbesondere durch die Einkommensabhängigkeit der Beiträge gekennzeichnet ist, findet durch Boni nicht statt."[816]

10.5.1 Solidaritätsgrundsatz

Kritiker hinterfragen die obige Aussage der Bundesregierung zum **Solidarprinzip** (s. o. 10.5), worauf öffentliche wie private Versicherungen begründet sind. Dieses Prinzip geht davon aus, dass versicherte Beeinträchtigungen individuelle Schicksalsschläge darstellen, vor deren übermäßigen Auswirkungen die kollektive Absicherung bewahren soll. Versicherungsbeiträge, die für alle gleich hoch oder nach sozialen Aspekten gestaffelt sind, sollen die Kosten gemeinsam und diskriminierungsfrei finanzieren. Werden nunmehr die Risiken „eingepreist", so wird dieser Grundsatz mehr oder weniger aufgegeben. Jede Gewährung von Boni bedeutet für die Nichtberücksichtigten einen Malus, also eine Benachteiligung.[817] Bezugsrahmen für die Solidargemeinschaft sind nicht mehr alle Versicherten, sondern kleinere Kollektive. Die Personalisierung von Versicherungsprämien kann im Grunde so weit getrieben werden, wie Daten zur Definition eines Risikomusters vorhanden sind. Der Präsident der Bundesärztekammer Frank Ulrich Montgomery meinte hierzu, Daten aus Gesundheits-Apps dürften nicht zur individuellen Risikoadjustierung von Krankenversicherungstarifen und damit zur Entsolidarisierung eingesetzt werden.[818]

814 Deutscher Ethikrat S. 73.
815 Deutscher Ethikrat S. 23, 102.
816 BT-Drs. 18/9243, zustimmend zit. bei Klose in Stiftung Datenschutz (2017) S. 106.
817 Deutscher Ethikrat S. 74.
818 Pressemitteilung Bundesärztekammer v. 7.6.2016.

Eine Relativierung des Solidarprinzips im Versicherungsbereich ist heute nicht ungewöhnlich. Dies gilt z. B. in den Bereichen der privaten Kranken- und Lebensversicherung, wo das Ausüben von Risikosportarten zu höheren Prämien führen kann. Dies wird für gerechtfertigt angesehen, wenn die Ausübung der bestimmten Aktivitäten tatsächlich ein höheres Schadenrisiko verursacht. Weitere Voraussetzung ist, dass die Entscheidungen für die Aktivitäten individuell getroffen werden und sich auf Exklusives beziehen, also auf Aktivitäten, die vom durchschnittlichen Bürger nicht ausgeübt werden und auch nicht ausgeübt werden müssen (Rauchen, risikogeneigte Sportarten). In diesen Fällen kann es sogar ein Gebot sozialer Gerechtigkeit sein, derartige Risiken nicht von allen Versicherten tragen zu lassen.[819]

Bei der Zurechnung individuellen Verhaltens im Rahmen der Tarifierung von Versicherungen ist zu berücksichtigen, dass es Menschen grds. freisteht, sich gemäß ihren eigenen Vorstellungen und Entscheidungen zu entfalten und zu verhalten. Jede Person ist zunächst für die eigene Gesundheit verantwortlich.[820] Es besteht der Erfahrungssatz, dass Menschen einem natürlichen Drang folgen, ihre Gesundheit zu bewahren. Zugleich ist aber auch anerkannt, dass das Selbstbestimmungsrecht der Menschen diesen auch das Recht zugesteht, sich selbst zu schädigen. Je selbstbestimmter und bewusster eine solche Selbstschädigung erfolgt, desto weniger kann ein Mensch Ansprüche an die Solidargemeinschaft auf Beseitigung der Folgen stellen. Die Frage der Bewusstheit lässt sich jedoch regelmäßig nur sehr begrenzt merkmals- bzw. datenbezogen erfassen, da hierfür eine Vielzahl nicht verfügbarer innerer und äußerer Faktoren ausschlaggebend sind.

Bezieht sich eine versicherungsrechtliche Vergünstigung auf Aktivitäten, die nicht von allen Menschen wahrgenommen werden können, so wird der Grundsatz der Solidarität verletzt. Sportliche Aktivitäten können z. B. nicht von Personen erbracht werden, die hieran wegen gesundheitlichen Beeinträchtigungen gehindert sind. Das Solidarprinzip besteht gerade darin, Menschen, die unverschuldet ein besonders hohes Risiko tragen, durch die Gemeinschaft zu entlasten.[821] Bonusprogramme tendieren im Gegensatz hierzu dahin, ohnehin schon gesunde Menschen in ihrer Gesundheit zu fördern.

Die Telematiktarife basieren auf der Annahme, dass das individuelle Gesundheitsverhalten insbesondere auch individuell determiniert ist, d. h. von den Betroffenen frei bestimmt werden kann. Tatsächlich ist aber das Verhalten von Menschen in vieler Hinsicht sozial bestimmt oder gar festgelegt, so dass es Menschen trotz des Willens hierzu wegen der Lebensumstände nicht möglich ist, das vom Versicherungsunternehmen erwartete Verhalten zu zeigen. Ohne in den Diskurs über den freien Willen von Menschen umfassend einzusteigen, kann festgestellt werden, dass ohnehin sozial benachteiligte Menschen durch ihre Bildung, ihr soziales Umfeld, Werbeeinflüsse usw. diejenigen sind, denen eine freie Entscheidung zugunsten einer gesünderen Lebensführung erschwert

819 Deutscher Ethikrat S. 73, 155.
820 Deutscher Ethikrat S. 155.
821 Deutscher Ethikrat S. 156 f.

wird. Gesundheitsbezogene Telematiktarife führen somit zu einer Verstärkung sozialer Diskriminierung. Zwar gibt es im Hinblick auf die Diskriminierungsverbote in Art. 21 GRCh keine klaren Anwendungsvorgaben. Es ist aber offensichtlich, dass Diskriminierungen hiermit verstärkt werden.

Mit Bonusprogrammen werden gesundheitliche Zustände als vom Individuum zu erstrebende Normen und Normwerte etabliert, die nicht notwendigerweise, schon gar nicht für alle Menschen, gesund sind. Während geförderte Verhaltensweisen für viele Versicherte einen normalen Zustandswert darstellen und so wirkungslose Mitnahmeeffekte bewirken, sind sie für andere selbst bei hohen Anstrengungen nicht zu erreichen. Regelmäßig fehlt es an der Evidenz nach hinreichend langer wissenschaftlicher Beobachtung.[822] Selbst eine Definition normgerechten Verhaltens ist schwer möglich: Kostenminimierung für Versicherungen muss nicht mit verbesserter Gesundheitssituation der Betroffenen korrespondieren. Würde sich eine digitale Selbstvermessung, evtl. in einem gestuften längeren Prozess, zu einer Art Bürgerpflicht entwickelt, so wäre dies nicht verantwortbar.

Die Telematiktarife bei Versicherungen gehen von der Annahme aus, dass das Verhalten der Versicherten mit ausschlaggebend für die Versicherungskosten ist. Es erfolgt eine Reduktion komplexer individueller Merkmalsprofile auf bestimmte Einzelaspekte (Stratifizierung).[823] Diese Vorgehensweise ist plausibel. Es darf aber nicht übersehen werden, dass es sich bei den meisten ausschlaggebenden Faktoren für Versicherungskosten um gesellschaftlich gesetzte Umstände handelt wie z. B. Umweltverschmutzung, gesundheitsschädliche Arbeitsplätze, ungesunde Nahrungsmittel. Telematiktarife bilden allenfalls teilweise risikoadäquates Verhalten ab; eine Berücksichtigung sämtlicher Risikoursachen ist nicht möglich. Durch die Selektion von Faktoren werden Menschen begünstigt, welche sich insofern risikominimierend verhalten und dies auch dokumentieren. Unberücksichtigt bleiben Menschen, die durch andere, nicht prämierte Verhaltensweisen das Risiko minimieren.[824]

10.5.2 Verbraucherpolitische Aspekte

Mit Telematiktarifen erfolgt nicht nur eine gezielte Entsolidarisierung der Versicherungsnehmer, sondern auch eine faktische Interessendifferenzierung, die zu einer Aushöhlung der kollektiven Verbrauchermacht führt. Die Informationsasymmetrie zwischen Unternehmen und Verbraucher wird durch Big Data nicht relativiert, sondern eher ausgebaut: Der Verbraucher wird für das Unternehmen transparenter, ohne dass damit ein Transparenzgewinn für diesen einhergeht.[825]

---

822 Rebitschek/Gigerenzer/Wagner, Kritische Voraussetzungen für ein digitales Gesundheitswesen in Deutschland, ZBW Leibnitz-Informationszentrum Wirtschaft, Wirtschaftsdienst 2017 (10), 702.

823 Deutscher Ethikrat S. 53.

824 Deutscher Ethikrat S. 24, 58.

825 Maas/Milanova Die Volkswirtschaft 5-2014, 25; Deutscher Ethikrat S. 91.

Teilweise wird vorgetragen, verhaltensbasierte Pricing-Modelle im Versicherungsbereich seien eine natürliche Reaktion auf gesellschaftliche Veränderungen, die von einer verstärkten Individualisierung und Vernetzung geprägt seien. Dem Kunden werde in der Kommunikation eine wichtigere Rolle zugewiesen; das Versicherungsprodukt diene nicht nur der Schadensabsicherung und -regulierung, sondern biete einen dauernd stattfindenden „Customer-Journey" und vermittle einen „Customer-Value".[826] Diese Bewertung ist nicht völlig abwegig, ändert aber nichts an der grundsätzlichen Machtasymmetrie zwischen Versicherungsunternehmen und Versicherungsnehmer. Letzterer hat heute zwar regelmäßig mehr Wahlmöglichkeiten als früher, insbesondere wegen eines sich globalisierenden Online-Angebots. Die Telematiktarife sind aber keine Instrumente zur Stärkung der Verbrauchermacht; vielmehr dienen sie der Kundenbindung angesichts des geänderten Wettbewerbs.

10.5.3 Datensparsamkeit

Bonusprogramme von Versicherungen basieren auf der Erwägung, dass die digital erfassten Daten aussagekräftig für das Gesundheitsverhalten des Versicherungsnehmers seien. Dies ist schon wegen der eingesetzten Messmethoden oft äußerst fragwürdig. Die Aussagekraft der erzielten Bonuspunkte kann auch dadurch in Frage gestellt sein, dass der Versicherungsnehmer die Sensoren bewusst täuscht. Dies kann dadurch erfolgen, dass ein Schrittzähler von einem Metronom oder dem Hund des Versicherungsnehmers geschwungen wird. Durch ausgeklügelte Methoden, z. B. die Messung der Körpertemperatur, lassen sich zweifellos bestimmte Manipulationen, nicht aber Manipulationen generell verhindern. In jedem Fall führt jedes Betrugsverhinderungsprogramm zu weiteren, zumeist noch erheblich sensitiveren Datenerhebungen.[827] Gelangen die Vergünstigungen für gesundes Verhalten bei Versicherungen in einen ökonomisch relevanten Bereich, so stellt sich schnell die Frage, weshalb Versicherungsnehmer, die sich aus Gründen ihres Persönlichkeitsschutzes der Teilnahme an solchen Programmen verweigern, für die Wahrung ihres Persönlichkeitsrechts benachteiligt werden. Diese haben keine rechtliche Handhabe gegenüber Versicherungsnehmern, die durch Manipulationen Vergünstigungen für sich in Anspruch nehmen, oder gegenüber den Versicherungen, die diese Vergünstigungen gewähren.

Versicherungsnehmer, die mit ihren Daten im Interesse informationeller Selbstbestimmung sparsam umgehen wollen, werden durch Telematiktarife tendenziell diskriminiert.[828] So heißt es in einem am 8.6.2017 in einem zur Digitalpolitik veröffentlichten gemeinsamen Positionspapier der Bundesministerien für Wirtschaft, Arbeit und Soziales sowie Justiz und Verbraucherschutz: „Wir werden daher prüfen, wie die informationelle Selbstbestimmung hier gestärkt werden kann. Gleiches gilt für die Verarbeitung solcher Daten im Rahmen von hoch individualisierten Versicherungstarifen. Das Prinzip der Risikogemeinschaft, das unser

826 Maas/Milanova Die Volkswirtschaft 5-2014, 25.
827 Moorstedt, Berechne dich selbst, SZ 4.1.2016, 9.
828 Deutcher Ethikrat S. 24, 155.

Versicherungswesen prägt, darf nicht ausgehöhlt werden, indem sich nur noch derjenige günstig versichern kann, der gesund ist und bereit ist, seine Privatsphäre aufzugeben". In der GKV sei die Verwendung dieser Daten weitgehend ausgeschlossen: „Dies muss aber auch für private Versicherungsunternehmen gelten.[829]

Ein Kritikpunkt an den Telematiktarifen von Versicherungen ist, dass auf diese Weise Daten gesammelt werden, die von den Unternehmen zweitverwertet werden. Dieser Kritik könnte dadurch begegnet werden, dass derartige zweckentfremdende Datennutzungen verboten bzw. ausgeschlossen werden. Bisher ist dies in der Praxis zumeist nicht der Fall. Die Programme, über die das gesundheitsbewusste Verhalten nachgewiesen werden, unterliegen keiner besonderen Vertraulichkeit, oft in der Praxis nicht einmal einer wirksamen Durchsetzung des Datenschutzes, z. B. wenn die Dienstleistungen von US-Anbietern erbracht werden, die sich bisher weitgehend einer effektiven Datenschutzkontrolle entziehen. Eine wesentliche Motivation für Telematiktarife besteht für Unternehmen gerade darin, Daten von den Versicherungsnehmern zu erlangen (know your customer) und diese kommerziell (weiter) zu nutzen.

Basiert ein Telematiktarif auf einer umfassenden Datenanalyse, so können Anleihen an die rechtliche Bewertung der Kreditwürdigungsbewertung mit Hilfe des Scoring vorgenommen werden: Voraussetzung für den Anreiz muss sein, dass die von der Versicherung vorgegebenen Verhaltensweisen wissenschaftlich nachweisbar zu einer Reduzierung des versicherten Risikos führen, das in einem Verhältnis zu den Prämienvergünstigungen steht. Eine rein statistische Korrelation genügt nicht, vielmehr muss eine plausible Kausalität zwischen erwartetem Verhalten des Versicherungsnehmers und Risiko- bzw. Kostenreduzierung für die Versichertengemeinschaft bestehen. Während insofern hinsichtlich der Bonitätsprüfung aber aussagekräftige Untersuchungen vorliegen, sind solche konkret auf Versichertenverhalten bezogene Untersuchungen noch nicht bekannt.

10.5.4 Ethische und demokratische Aspekte

Ein weiterer Aspekt der Telematiktarife bei Versicherungen besteht darin, dass die Voraussetzungen für die Erreichung eines günstigen Tarifs einseitig von den Versicherungsunternehmen festgelegt werden. Es erfolgt ein fremdbestimmtes Anleiten zur Selbstoptimierung, die bei ökonomisch engen Verhältnissen zu einem Zwang werden kann. Damit haben diese Unternehmen die Möglichkeit, ihre Versicherungsnehmer zu einem bestimmten Verhalten zu drängen, das nicht auf deren vollen freien Willen basiert. Die vom Unternehmen festgelegten Kriterien geben nicht demokratisch legitimierte Normen vor, die – zumindest bisher – auch nicht demokratisch kontrolliert sind.

Die rechtliche Bewertung eines als Nudging genannten Vorgehens ist noch nicht geklärt. Mit Nudging (übersetzt Anstupsen) wird eine Methode beschrieben, über die staatliche oder private Institutionen gesellschaftlich erwünschtes Verhalten veranlasst.[830] Nudging ist

829 Zit. nach Schärferer Datenschutz für Vitaldaten, www.aerztezeitung.de 08.06.2017.

830 Thaler/Sunstein, Nudge – wie man kluge Entscheidungen anstößt, 2009.

insofern problematisch, dass Menschen im Sinne eines „libertären Paternalismus“ (Thaler) zu einem Verhalten hingeführt, d. h. manipuliert werden, dessen Konsequenzen sie nicht übersehen können.[831]

10.6 Beschäftigtenüberwachung

Beim Einsatz von Big Data im Verhältnis zwischen Arbeitgeber und Arbeitnehmer (s. o. 3.17) sind sowohl das Arbeitsrecht wie auch das Datenschutzrecht in ihrer engen Verbindung zu beachten. Der bisher geltende § 32 BDSGaF wird durch Art. 88 DSGVO und § 26 BDSGnF abgelöst. § 26 Abs. 2 und Abs. 3 S. 2 formulieren spezifische Anforderungen an die Freiwilligkeit der Einwilligung (s. o. 8.8.3). Gemäß § 26 Abs. 3 S. 1 BDSGnF ist die Verarbeitung von Gesundheitsdaten und sonstigen sensitiven Daten „für Zwecke des Beschäftigungsverhältnisses zulässig, wenn sie zur Ausübung von Rechten und zur Erfüllung der sozialen Sicherheit und des Sozialschutzes erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt“. § 22 Abs. 2 BDSGnF mit seinen Anforderungen an besonderen Schutzmaßnahmen ist anwendbar (§ 26 Abs. 3 S. 3 BDSGnF).

Das Fragerecht bzw. Datenerhebungsrecht des Arbeitgebers in Bewerbungsverfahren beschränkt sich auf Angaben, die für das Beschäftigungsverhältnis erforderlich sind. Spezielle Beschränkungen gibt es bzgl. einer evtl. bestehenden Schwangerschaft[832] sowie einer Schwerbehinderung.[833] Fragen zur Gesundheit sind nur zulässig, soweit sich hieraus Auswirkungen auf die Arbeitsfähigkeit ergeben. Alkohol- und sonstige Drogentests bedürfen einer spezifischen arbeitsplatzbezogenen Begründung. Entsprechendes gilt für psychologische Tests.[834] § 19 GenDG verbietet dem Arbeitgeber, vor Begründung eines Beschäftigungsverhältnisses genetische Untersuchungen oder die Vorlage von Analyseergebnissen zu verlangen.

Auch während des Arbeitsverhältnisses ist bei der Erhebung und Verarbeitung von Gesundheitsdaten eine strenge Erforderlichkeitsprüfung durchzuführen. Dabei ist zwischen der Verarbeitung durch den Arbeitgeber und seiner Personalverwaltung und dem Betriebsarzt zu unterscheiden, der gegenüber dem Arbeitgeber wie auch gegenüber Dritten der ärztlichen Schweigepflicht unterliegt (§ 8 Abs. 1 S. 3 ASiG) und dem zugleich spezifische Erhebungs- und Verarbeitungsbefugnisse zukommen.[835] Aber auch innerhalb der Personalverwaltung ist eine Separierung der Gesundheitsdaten z. B. von den Grund-, Stamm- und Statusdaten mit einem spezifischen Zugriffsregime geboten. Die gilt z. B. für die Daten, die im Rahmen eines betrieblichen Eingliederungsmanagements (BEM, § 84 SGB IX) erhoben wurden.[836] Die Pflicht zur getrennten Aufbewahrung hat zur Folge, dass die

831 Piper, Den Menschen anstupsen, SZ 10.10.2017, 17.
832 Däubler Rn. 215.
833 Däubler Rn. 219.
834 Däubler Rn. 229 ff.
835 Däubler Rn. 283 ff., 396 ff.
836 Däubler Rn. 399a ff.

Gesundheitsdaten im Rahmen von Big-Data-Analysen auch nicht mit Stamm- und Sozialdaten zusammengeführt werden dürfen.

Im Beschäftigtenbereich sind automatisierte Entscheidungen bei der Bewerberauswahl schon weit verbreitet. Dabei ist Art. 22 DSGVO anwendbar. Dies gilt z. B. bei einer automatisierten Vorselektion von Bewerbenden, wenn dem keine „harten" Qualifikationsanforderungen, sondern eine komplexe Merkmalsauswertung zugrunde liegt.[837] Ein weiterer Anwendungsfall kann in der sozialen Auswahl nach § 1 Abs. 4 KSchG liegen.[838] Im deutschen Beamtenrecht besteht in § 114 Abs. 4 BBG eine restriktive Regelung: „Beamtenrechtliche Entscheidungen dürfen nicht ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten gestützt werden, die der Bewertung einzelner Persönlichkeitsmerkmale dienen." Konkretisierungen können über Kollektivvereinbarungen (Betriebsvereinbarungen, Tarifverträge) gemäß Art. 88 DSGVO vorgenommen werden.

Bei der Datennutzung sind die Diskriminierungsverbote des AGG zu beachten. Umfassende Persönlichkeitsanalysen, z. B. unter Auswertung der Handschrift oder der Sprache zur Ableitung von Charaktereigenschaften, sind unzulässig.[839] Dies gilt grundsätzlich auch für die Analyse von Stimmungen und von persönlicher Befindlichkeit (z. B. Stress). Die Datenbeschaffung aus öffentlichen Quellen, etwa aus dem Internet, setzt eine Einbeziehung der Betroffenen voraus.[840]

10.7 Statistik

Die amtliche Statistik war mit der Mikrozensusentscheidung des BVerfG schon 1969 Gegenstand verfassungsgerichtlicher Bewertung.[841] Darin stellt das höchste deutsche Gericht fest, dass die statistische Erhebung von Persönlichkeits- und Lebensdaten als Vorbedingung für die Planmäßigkeit staatlichen Handelns von den gemeinschaftsbezogenen und gemeinschaftsgebundenen Bürgern hingenommen werden muss, wenn die Erhebung „an das Verhalten des Menschen in der Außenwelt anknüpft" und die „Angaben durch die Anonymität ihrer Auswertung den Persönlichkeitsbezug verlieren". „Eine Repräsentativumfrage zu statistischen Zwecken, bei der nur der durch ein ´Zufallsverfahren` bestimmte Personenkreis von der Verpflichtung zur Auskunft betroffen wird, verstößt insbesondere nicht gegen den Gleichheitsgrundsatz".[842]

Im Volkszählungsurteil von 1983 wird diese Position bekräftigt und konkretisiert. Danach ist die „strikte Geheimhaltung der zu statistischen Zwecken erhobenen Einzelangaben unverzichtbar, solange ein Personenbezug noch besteht oder herstellbar ist

837 A. A. Franzen DB 2001, 1872.
838 Tinnefeld NJW 2001, 3082; Däubler Rn. 432.
839 Däubler Rn. 428 ff.
840 Dzida NZA 2017, 542 ff.
841 BVerfG 16.7.1969 – 1 BvL 19/63, NJW 1969, 1707.
842 BVerfG 16.7.1969 – 1 BvL 19/63, NJW 1969, 1707.

(Statistikgeheimnis)".[843] Dieses Statistikgeheimnis ist in § 16 BStatG einfachgesetzlich fixiert.

Das BVerfG fordert die Umsetzung „einer möglichst frühzeitigen (faktischen) Anonymisierung, verbunden mit Vorkehrungen gegen eine Deanonymisierung".[844] Hierbei spielt die Unterscheidung zwischen Hilfsmerkmalen und Erhebungsmerkmalen eine zentrale Rolle. Während die Erhebungsmerkmale zur statistischen Auswertung herangezogen werden, sind die der Identifizierung dienenden Hilfsmerkmale zum frühestmöglichen Zeitpunkt zu löschen und bis dahin von den übrigen Angaben getrennt und unter Verschluss zu halten (§§ 10, 12 BStatG).[845]

Voraussetzung für die Weitergabe von Statistikdaten an Dritte, etwa zur Weiterverwendung im Kontext von Big-Data-Analysen, ist entweder ein förmliches Gesetz mit entsprechenden grundrechtssichernden Organisations- und Verfahrensregelungen, oder die vollständige Anonymisierung der Einzelangaben.[846] Die Statistikämter haben sicherzustellen, dass selbst bei der Übermittlung und bei der Veröffentlichung von Ergebnissen zumindest eine Dreier-Aggregation erfolgt, d. h. ein Datenfeld die Angaben von mindestens drei Betroffenen aufweist (§ 16 Abs. 1 Nr. 3 BStatG).[847] Angesichts der Reidentifizierungsmöglichkeiten mit Hilfe von Big Data scheint bei Veröffentlichungen und der fehlenden Kontrollierbarkeit ein Aufgeben der Dreier-Vorgabe notwendig. Diese sollte durch ein flexibles System (K-Anonymität) ersetzt werden (s. o. 8.12.1). Bei den Empfängern ist durch weitere Vorkehrungen sicherzustellen, dass diese keine Reidentifizierung vornehmen.

Das bisherige amtliche Statistikrecht ist noch nicht an die heute bestehenden technischen Möglichkeiten von Big Data angepasst. Anlass für eine solche Anpassung besteht durch die Neuregelung in der DSGVO, die in den Art. 5 Abs. 1 lit. b, 89 bei hinreichenden Garantien einen privilegierten Zugang zu für einen anderen Zweck erhobenen Daten vorsieht.

Dieses Privileg besteht aber nur für Statistiken, an denen ein öffentliches Interesse besteht. Ein solches besteht i. d. R., wenn amtliche Statistiken auf der Basis einer gesetzlichen Regelung erstellt werden. Private Statistiken ohne gesetzliche Sicherung von Garantien genießen die Privilegierung der DSGVO nicht.[848]

---

843 BVerfG 15.12.1983 – 1 BvR 209/83 u. a., NJW 1984, 423.
844 BVerfG 15.12.1983 – 1 BvR 209/83 u. a., NJW 1984, 423.
845 BVerfG 24.9.1987 – 1 BvR 970/87, NJW 1987, 2805 ff.
846 BVerfG 15.12.1983 – 1 BvR 209/83 u. a., NJW 1984, 424; Poppenhäger in Roßnagel S. 1629 ff.
847 Poppenhäger in Roßnagel S. 1632 f.
848 So wohl auch Grages in Plath, Art. 89 Rn. 7; Hense in Sydow, Europäische Datenschutzgrundverordnung, 2017, Art. 89 Rn. 16; Laue/Nink/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis, 2016, § 1 Rn. 119 (S. 72 f.); die darüber hinausgehend eine vollständige Aggregierung fordern.

10.8 Medizinische Forschung

10.8.1 Rechtsrahmen

Der rechtliche Rahmen zur Nutzung von Gesundheitsdaten für Forschungszwecke ist auf nationaler Ebene stark fragmentiert und zugleich antiquiert. Regelungen finden sich bisher in den allgemeinen Datenschutzgesetzen des Bundes und der Länder (vgl. §§ 40, 28 Abs. 6 Nr. 4, 14 Abs. 2 Nr. 9, 4a Abs. 3 BDSGaF, § 22 LDSG SH), die auf die Spezifik von Gesundheitsdaten als besonders sensitive Kategorie (vgl. § 3 Abs. 9 BDSGaF) nur bedingt eingehen. In verstreuten Forschungsklauseln werden die allgemeinen Regelungen durch spezifische Festlegungen in Spezialgesetzen ergänzt, was die Rechtslage unüberschaubar und ihre praktische Umsetzung schwierig macht.[849] Forschungsklauseln mit explizitem Gesundheitsbezug sind z. B. § 273 SGB V, der Forschungsvorhaben der gesetzlichen Krankenversicherung regelt[850], sowie die §§ 303 ff. SGB V, die darauf abzielen, die Versorgungsforschung sowie die Forschung zur Steuerung des Gesundheitssystems zu unterstützen.[851]

Je nach anzuwendenden Forschungsregelungen wird

- externe Forschung nicht oder nur anderen Fachabteilungen derselben juristischen Person erlaubt,
- der Einsatz externen Personals vor Ort vorausgesetzt,
- die Datennutzung auf das jeweilige konkrete Forschungsprojekt beschränkt,
- die Formulierung von Aufklärung und Einwilligung spezifischen Anforderungen unterworfen,
- die Nutzung für andere Projekte an eine umfassende Anonymisierung geknüpft, oder
- die Einbeziehung von Datenschutzbehörden oder anderen Stellen gefordert. [852]

Mit der DSGVO besteht nun ein Rechtsrahmen, in dem Gesundheitsdaten weiterhin einen hohen Schutz genießen (Art. 9 DSGVO). Deren Weiterverarbeitung zu Forschungszwecken wird aber als von hohem öffentlichem Interesse und nicht länger unvereinbar mit dem ursprünglichen Erhebungszweck eingestuft (Art. 5 Abs. 1 lit. b DSGVO). Eine wissenschaftliche Verarbeitung personenbezogener Gesundheitsdaten soll demnach zulässig sein, wenn „angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person“ vorgesehen sind (Art. 9 Abs. 2 lit. j,

849 Schneider S. 309 ff., 344.

850 Torbohm in Kingreen/Kühling S. 361 f.; Spindler MedR 2016, 698.

851 Torbohm in Kingreen/Kühling S. 363 f.; Spindler MedR 2016, 698.

852 Ausführlich zu den für Kliniken geltenden Regelungen Schneider S. 82 ff., 244 f., 247 f., 310 ff., 323; vgl. auch die unterschiedlichen Anforderungen im Sozialrecht § 75 SGB X, § 287 SGB V, § 98 SGB XI, § 119 SGB XII; dazu Heckmann/Paschke in Stiftung Datenschutz (2017) S. 78; zur Regelungsnotwendigkeit auch Stellungnahmen zum Entwurf DSAnpUG-EU der Bundesärztekammer v. 21.03.2017, Deutscher Bundestag, Innenausschuss Ausschussdrucksache 18(4)826, S. 6 f. sowie Deutscher Wissenschaftseinrichtungen, u. a. Deutsche Forschungsgemeinschaft v. 16.02.2017, Ausschussdrucksache 18(4)779 neu S. 3 ff.

89 DSGVO).[853] Die DSGVO betont in ErwGr 159 S. 4 die besondere Bedeutung der Gesundheitsforschung: „Die wissenschaftlichen Forschungszwecke sollten auch Studien umfassen, die im öffentlichen Interesse im Bereich der öffentlichen Gesundheit durchgeführt werden."

Das vom 25.5.2018 an geltende neue **Bundesdatenschutzgesetz** (BDSGnF) enthält zwar in § 27 Abs. 1 die Erlaubnis zur Verarbeitung sensitiver Daten für Forschungszwecke, wenn „die Verarbeitung zu diesen Zwecken erforderlich ist und die Interessen des Verantwortlichen an der Verarbeitung die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung erheblich überwiegen" (Satz 1) und „angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person" (Satz 2) gemäß § 22 Abs. 2 S. 2 BDSG-neu ergriffen werden. Allerdings ist laut § 27 Abs. 3 BDSGnF weiterhin eine frühestmögliche Anonymisierung gefordert, und Merkmale, „mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person zugeordnet werden können", sind bis zur Anonymisierung gesondert zu speichern. Damit greift diese Regelung Art. 89 Abs. 1 DSGVO auf, der „geeignete Garantien für die Rechte und Freiheiten der betroffenen Person" einfordert: „Mit diesen Garantien wird sichergestellt, dass technische und organisatorische Maßnahmen bestehen, mit denen insbesondere die Achtung des Grundsatzes der Datenminimierung gewährleistet wird. Zu diesen Maßnahmen kann die Pseudonymisierung gehören, sofern es möglich ist, diese Zwecke auf diese Weise zu erfüllen" (Art. 89 Abs. 1 S. 2, 3 DSGVO).

10.8.2 Regulatorische Unzulänglichkeiten

Medizinische Forschung basiert zunehmend auf einrichtungs- und länderübergreifenden Kooperationen, die den Austausch personenbezogener Daten erfordern. Die bereichsspezifischen Regelungen, die für die jeweiligen Datenquellen gelten, knüpfen oft für die Datennutzung bzw. -weitergabe an eine Genehmigung oder zumindest Kenntnisnahme durch Ministerien, Ethik-Kommissionen oder Datenschutzbehörden an. Die daraus resultierenden administrativen Anforderungen bedeuten einen hohen Aufwand für die Forscher und führen wegen **rechtlicher Unwägbarkeiten** leicht zu Verunsicherungen. Bisweilen können sich einschlägige Regelungen auf unterschiedlichen Ebenen sogar widersprechen (z. B. bei Forschungsprojekten, für die zugleich Bundes- und Landesgesetze anwendbar sind), was Forscher schlimmstenfalls der Gefahr aussetzt, unabsichtlich und unwissentlich gegen rechtliche Vorgaben zu verstoßen.[854]

Zusätzlich zu den datenschutzrechtlichen Anforderungen müssen bei vielen medizinischen Forschungsvorhaben analog § 15 MBOÄ auch **Ethik-Kommissionen** einbezogen werden. Dauer und Ergebnis der damit verbundenen Beratungs- und Genehmigungsprozesse sind oft schwer einschätzbar.[855] Es kommt in vielen Belangen zur Doppelung von Aufgaben und Infrastrukturen, da ethische und datenschutzrechtliche Erwägungen teilweise identische

853 Dierks, EHEALTHCom 02_03/16, 42.
854 Weichert in Stiftung Datenschutz (2017) S. 189.
855 Rehborn in Prütting § 15 MBOÄ.

Schutzziele verfolgen (Würdeschutz, Persönlichkeitsschutz, sonstiger Grundrechtsschutz). Beide Verfahren fordern letztlich eine Abwägung zwischen Forschungsinteressen und Betroffeneninteressen; sie unterscheiden sich lediglich in der Zusammensetzung des „Spruchkörpers" und der dort präsenten Expertise.

Den Regelungen zur (medizinischen) Forschung ist gemein, dass eine Datennutzung **ohne Einwilligung** der Betroffenen nur im Ausnahmefall und auf der Grundlage einer Güterabwägung erlaubt ist. Vorrang hat die Legitimation durch eine Einwilligung. Dieser Grundsatz folgt dem Kernprinzip der informationellen Selbstbestimmung[856], dass der Betroffene idealerweise selbst bestimmen soll, wer worüber mit seinen Daten forschen darf. Allerdings kann dieser Grundsatz in der medizinischen Forschung nicht uneingeschränkt realisiert werden. In diesen Fällen sind organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, die einer Verletzung von Persönlichkeitsrechten effektiv vorbeugen.[857]

Wirksame Einwilligungen bzw. Schweigepflichtentbindungen setzen voraus, dass sie **informiert erfolgen**, d. h. auf hinreichend präzisen Informationen darüber basieren, welche Stelle für welche Zwecke mit welchen Daten forschen können soll (s. o. 8.8.2). Diesen Anforderungen kann bei der Forschung aus folgenden Gründen oft nicht entsprochen werden:

1. Medizinische Daten bilden ebenso wie Biomaterialien eine **dauerhafte Erkenntnisquelle** für die Forschung. Viele wissenschaftliche Fragestellungen, die sich mit Daten und Biomaterial bearbeiten lassen, sind zum Erhebungs- bzw. Gewinnungszeitpunkt noch gar nicht genau bekannt. Im Laufe der Forschungsarbeiten können sich neue Fragestellungen ergeben, die ursprünglich ebenso wenig absehbar waren wie die Identität der Einrichtungen, die für die Bearbeitung dieser Fragestellungen am besten qualifiziert und geeignet wären.[858]

2. Wegen der Offenheit der teilweise bestehenden Fragestellungen werden im Kontext der medizinischen Forschung zunehmend Einwilligungen erbeten, die sehr **umfassend und allgemein formuliert** sind. Daher werden wiederholt Zweifel laut, ob derartige Einwilligungen (sog. broad consent)[859] noch als „informiert" gelten können und die Funktion einer wirksamen Erlaubnis zur Verarbeitung persönlicher Daten erfüllen (s. o. 8.8.2, 8.8.3). Dies gilt insbesondere für Einwilligungen, die sich in ihrer Unbestimmtheit auch auf ethische „Randzonen" (z.B. militärische Forschung) erstrecken könnten.

3. Die Unsicherheit in Bezug auf die Verarbeitungszwecke wird teilweise dadurch kompensiert, dass die Betroffenen während der Nutzung ihrer Daten regelmäßig oder auf Nachfrage über **aktuelle und geplante Forschungsprojekte informiert** werden (dynamic

856 BVerfG 15.12.1983 – 1 BvR 209/93 u. a., NJW 1984, 419, 422.
857 BVerfG 15.12.1983 – 1 BvR 209/93 u. a., NJW 1984, 419, 422.
858 Schneider S. 117 ff.
859 RfII (2016) S. 10.

consent).[860] Ein solches Vorgehen ist aber nicht umsetzbar, wenn sich die Erreichbarkeit der Betroffenen ändert, die Mitteilung der Informationen das Recht auf Nichtwissen der Betroffenen verletzt (s. o. 6.5) oder ein laufender Kontakt mit Forschenden zu aufwändig oder aus fachlicher Sicht abträglich ist. Diese Unzulänglichkeiten lassen sich nur teilweise dadurch ausgleichen, dass statt des Einzelnen die Öffentlichkeit als Ganzes informiert wird, oder die Spender ihr Widerrufsrecht für spezielle Forschungsfragen geltend machen.

4. Einer Anonymisierung und einer Beseitigung des Personenbezugs stehen in vielen Fällen Forschungsinteressen entgegen: Langzeitstudien erfordern eine fortlaufende Zuordnung neuer Daten zu bereits vorhandenen Daten. Solche Studien sind für die medizinische Forschung unerlässlich, da die Wirksamkeit von Therapien und Umweltfaktoren oft erst nach Jahren feststeht.[861]

5. Die in Gewebeproben enthaltenen Erbinformationen mit ihrem inhärenten Personenbezug bewirken bei Biomaterialien und genetischen Daten, dass eine unumkehrbare Anonymisierung unmöglich ist. Wohl lassen sich aber die persönlichkeitsrechtlichen Risiken beim Umgang mit genetischen Daten durch den geschickten Einsatz von Pseudonymen und die abgeschottete und kontrollierte Verarbeitung der Daten maßgeblich reduzieren.

6. Das wissenschaftliche Potenzial von Gesundheitsdaten lässt sich oft, etwa bei der Erforschung seltener Erkrankungen, nur durch eine einrichtungsübergreifende (möglicherweise weltweite) Zusammenführung der Daten ausschöpfen. Eine solche Zusammenführung erfolgt heute über Forschungsnetzwerke oder Krankheitsregister. Allerdings gibt es hierfür, abgesehen vom Spezialfall der Krebsregistergesetze, bisher keine explizite gesetzliche Grundlage. Die Rechtmäßigkeit der Datennutzung gründet vielmehr allein auf der informierten Einwilligung der Betroffenen mit dem Vorbehalt, dass Art und Umfang der Datenzusammenführung zum Zeitpunkt der Einwilligung meist völlig unbekannt sind.

10.8.3 Grundsatzerwägungen

Bei dem Bestreben, den Vertraulichkeits- und Persönlichkeitsschutz von Patienten und Probanden in der medizinischen Forschung zu gewährleisten und zugleich das wissenschaftliche Potenzial existierender Datenbestände so weit wie möglich auszuschöpfen sind folgende grundsätzliche Erwägungen von Bedeutung: Moderne Forschungsansätze zielen immer häufiger darauf ab, räumlich und zeitlich auseinanderliegende Datenquellen unterschiedlicher Zweckbindung für eine gemeinsame Analyse zusammenzuführen. Zur Sicherung der guten wissenschaftlichen Praxis müssen Forschungsergebnisse unabhängig nachvollziehbar sein, was wiederum die Aufbewahrung der diesen Ergebnissen zugrunde liegenden Daten in möglichst unverändertem Zustand voraussetzt. Heute sind technische Möglichkeiten (asymmetrische Kryptografie,

860 RfII (2016) S. 11.

861 RfII (2016) S. 3; RfII (2017) S. 4.

homomorphe Verschlüsselung) verfügbar, um die Verarbeitung von Forschungsdaten auf bestimmte Stellen und Zwecke zu begrenzen.

Folgende Regelungsaspekte **bestehender Forschungsklauseln** haben sich weitgehend bewährt:[862]

1. Im Interesse der Datenminimierung sind Daten für Forschungszwecke zu anonymisieren; ansonsten ist eine Pseudonymisierung vorzunehmen.[863]

2. Die Verarbeitung personenbeziehbarer Forschungsdaten setzt die Umsetzung technisch-organisatorischer Maßnahmen zur Erreichung der Schutzziele Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Intervenierbarkeit, Nichtverkettbarkeit voraus.[864]

3. Die ausdrückliche, informierte, freiwillige und widerrufbare Einwilligung[865] kann im Kontext der medizinischen Forschung konkretisiert werden.[866]

4. Überwiegt das öffentliche Interesse am jeweiligen Forschungsvorhaben die schutzwürdigen Belange der Betroffenen, so kann eine Verarbeitung auch ohne Einwilligung der Betroffenen zulässig sein, wenn der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.[867]

5. Eine Veröffentlichung personenbezogener Daten ist nur zulässig, wenn die betroffene Person eingewilligt hat oder dies für die Darstellung der Forschungsergebnisse unerlässlich ist und die Betroffenenbelange hinreichend berücksichtigt wurden.[868]

Bei Forschung mit Gesundheitsdaten, die zugleich einem Berufsgeheimnis, z. B. dem Patientengeheimnis unterliegen (s. o. 6.8), ist es wegen des **Zwei-Schranken-Prinzips**[869] erforderlich, dass neben den allgemeinen Datenschutzregelungen auch die Anforderungen an die Verarbeitung von Berufsgeheimnissen beachtet werden. Für die arbeitsteilige medizinische Forschung hat dies zur Folge, dass sämtliche Personen, denen Patientengeheimnisse offenbart werden, arbeitsrechtlich der ärztlichen Leitung der Forschungseinrichtung unterstellt werden müssten.[870] Da dies faktisch oft nicht möglich ist, sehen Aufsichtsbehörden in solchen Fällen contra legem über das Fehlen von

862 Weichert in Stiftung Datenschutz (2017) S. 192; Spindler MedR 2016, 693.
863 Vgl. § 40 Abs. 1 BDSG-alt; § 22 Abs. 1, 2, 5 LDSG SH; Art. 5 Abs. 1 lit. c u. e, 89 Abs. 1 DSGVO.
864 Art. 25, 32 DSGVO; Rost in Schmidt/Weichert S 353 ff.
865 Weichert, Big Data, Gesundheit und der Datenschutz, DuD 2014, 835.
866 Ein „broad consent", also eine weit formulierte Einwilligung kann im Forschungsbereich hinreichend Selbstbestimmung gewährleisten; dazu Richter/Krawczak/Lieb/Wolff/Schreiber/Buyx, Genetics in Medicine 7/2017; Deutscher Ethikrat S. 121 f.
867 Vgl. z. B. § 28 Abs. 6 Nr. 4 BDSGaF, § 22 Abs. 4 S. 1 LDSG SH; Art. 7, 9 Abs. 2 lit. a DSGVO.
868 Vgl. § 40 Abs. 3 BDSGaF; § 22 Abs. 6 LDSG SH.
869 Schneider S. 76 f.; Dochow GesR 2016, 408; Hauser/Haag S. 13; Kircher in Kingreen/Kühling S. 204, zum Sozialdatenschutz S. 212 f.; Dix in Simitis § 1 Rn. 176 ff.; a. A. Uwer in Wolff/Brink Syst. F Rn. 14 f.; Lippert in Ratzel/Lippert MBO-Ä, 5. Aufl. 2010, § 9 Rn. 68, wonach Berufsgeheimnisse dem Datenschutzrecht vorgehen sollen.
870 Als Gehilfen i. S. v. § 203 Abs. Abs. 3 S. 2 StGB.

Offenbarungsbefugnissen hinweg oder interpretieren eine Offenbarungsbefugnis in die allgemeinen Forschungsklauseln hinein, ohne dass die Forschenden den Offenbarungsschutz der Berufsgeheimnisse für sich in Anspruch nehmen können.[871] Dem kann durch eine normative Fixierung eines Forschungsgeheimnisses entgegengewirkt werden, das als Berufsgeheimnis anerkannt wird. Dafür gesetzlich festlegbare Bedingungen können in Genehmigungen oder dem Erfordernis von Zertifikaten bestehen.[872]

Besteht bei einem Forschungsergebnis eine Nützlichkeit für den Betroffenen, so dürfen diese hierfür verwendet werden. Die Zweckbeschränkung der Forschungsdatenverarbeitung soll, so ErwGr. 159 S. 6 DSGVO nicht gelten, wenn der Betroffene selbst profitieren kann: „Geben die Ergebnisse wissenschaftlicher Forschung insbesondere im Gesundheitsbereich Anlass zu weiteren Maßnahmen im Interesse der betroffenen Person, sollten die allgemeinen Vorschriften dieser Verordnung für diese Maßnahmen gelten." Dies darf aber nicht dazu führen, dass der Anspruch des Betroffenen auf Nichtwissen ignoriert wird (s. o. 6.5).

10.8.4 Regelungsvorschlag

Die voranstehend beschriebene Situation wird schon lange insbesondere von Forschenden und Datenschützern als unbefriedigend angesehen. Eine Auflösung des Konfliktes zwischen Forschungsinteressen und der Wahrung des Persönlichkeitsschutzes der Betroffenen kann in einer gesetzlichen Regelung liegen, in der die Einrichtung unabhängiger „Use and Access-Committees" (UACs) für medizinische Forschungsdaten vorgesehen wird, mit denen Doppelentwicklungen und Parallelstrukturen vermieden werden.[873] Dabei soll es sich um unabhängige, lokal agierende Gremien handeln, die in ihre Entscheidungen sämtliche technisch-organisatorischen, datenschutzrechtlichen, ethischen und fachlichen Erwägungen einfließen lassen. [874] Diesen UACs werden in Abhängigkeit von der Sensitivität des jeweiligen Forschungsvorhabens Genehmigungs- bzw. Vetorechte für die Nutzung personenbezogener Gesundheitsdaten per Gesetz übertragen, erhalten also eine hoheitliche Funktion. In den UACs müssen fachlicher, ethischer und datenschutzrechtlicher Sachverstand vertreten sein. Das Verhältnis der UACs zu den Ethik-Kommissionen und Datenschutzaufsichtsbehörden sollte unter Einräumung eines gegenseitigen Konsultationsrechts so geregelt werden, dass eine Kollision ihrer datenschutz- und berufsrechtlichen Compliance-, Kontroll- und Beratungspflichten weitestgehend vermieden und eine spürbare Entlastung aller Beteiligten erreicht wird. Die Zuständigkeit eines UAC für ein bestimmtes Forschungsprojekt könnte sich aus der geographischen oder organisatorischen Zugehörigkeit der jeweils Projektverantwortlichen ergeben. Vorbild hierfür könnte die in der DSGVO verankerte Regelung zur Zuständigkeit

871 Haag/Hauser S. 22, 254 ff.; Torbohm u. Kingreen/Kühling in Kingreen/Kühling S. 369 f., 446 f.
872 RfII (2017) S. 19, 23.
873 Ebenso von Kalle/Ücker/Eils/Winkler/Schickhardt in Stiftung Datenschutz (2017) S. 94.
874 Ähnlich RfII (2017) S. 13 ff.; siehe auch die Vorschläge zu einem Bund-Länder-Forschungsgremium bei Weichert in Stiftung Datenschutz (2017). S. 194 ff.

der Aufsichtsbehörden sein, die sich an der Hauptniederlassung eines Verantwortlichen orientiert (Art. 56 Abs. 1).

Während die organisatorischen und administrativen Verfahren der UACs gesetzlich zu regeln sind, sollten die Kriterien für die Bewertung von Forschungsvorhaben im Rahmen einer „regulierten Selbstregulierung" (s. o. 8.22) durch Einrichtungen wie z.B. die Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V. (TMF) entwickelt werden. Die resultierenden Standards könnten im Konsens der betroffenen Fach-Communities auch als verbindlicher und ggf. sogar rechtssicherer Rahmen für die Konzipierung und Zulassung von Forschungsvorhaben dienen.[875]

Derzeit gibt es im Kontext der personenbezogenen Verarbeitung von Daten für medizinische Forschungszwecke keine demokratische Kontrolle; den entsprechenden Verfahren fehlt systematische Transparenz.[876] Bei einer (teilweisen) Bündelung der bisherigen Aufgaben von Ministerien, Aufsichtsbehörden und Ethik-Kommissionen in eigens dafür eingerichteten und untereinander vernetzten UACs ließe sich dieser Missstand durch den Betrieb eines öffentlich einsehbaren Forschungsregisters beheben, an das die UACs wesentliche Informationen zu den von ihnen freigegebenen Forschungsprojekten weitergeben. Dieses Register würde insbesondere den Datenspendern einen Überblick über die Forschung mit ihren Daten, die dafür jeweils Verantwortlichen, ihre Ziele und Fragestellungen sowie die in der Forschung ergriffenen grundrechtsschützenden Maßnahmen erlauben. Nicht zuletzt könnte damit auch der immer wieder erhobenen Forderung nach stärkerer Teilhabe der Patienten und Probanden Rechnung getragen werden.

Durch eine bundesweit einheitliche Regelung in einem Bund-Länder-Staatsvertrag könnten die bisherigen, teilweise verstreuten und widersprüchlichen Bundes- und Länderregelungen zur medizinischen Forschung ersatzlos wegfallen.[877] In besagtem Staatsvertrag würden die materiell-rechtlichen und prozeduralen Voraussetzungen für die Zulässigkeit medizinischer Forschungsvorhaben normiert - einschließlich eventueller Einwilligungserfordernisse, der Verfahren der UACs, der Einbindung von Ethik-Kommissionen und Datenschutzaufsicht sowie der Transparenzverpflichtungen gegenüber der Öffentlichkeit.

Welche Forschungsprojekte unabhängig vom Datenzugang melde- bzw. genehmigungspflichtig sein sollen bzw. können, bedarf der weiteren fachlichen Erörterung. Maßgebliches Kriterium muss dabei die Sensitivität des jeweiligen Projektes sein.

---

875 Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V. (TMF), http://www.tmf-ev.de/, wahr; vgl. Pommerening/Drepper/Helbing/Ganslandt, Leitfaden zum Datenschutz in medizinischen Forschungsprojekten, 2014; der RfII (2016) S. 20 verfolgt ein ähnliches Konzept mit mehreren interdisziplinären Gremien.

876 Weichert DuD 2014, 837.

877 Wagner RDV 2017, 75 ff.

- Auf eine **Meldung und Registrierung kann verzichtet** werden, wenn klassische Eigenforschung erfolgt oder die Forschungsdatenverarbeitung auf einer informierten Einwilligung der Betroffenen basiert.
- **Melde- und registrierungspflichtig** sollten Projekte sein, bei denen eine Interessenabwägung die Betroffeneneinwilligung ersetzen soll, was impliziert, dass die UACs bei solchen Projekten neben Aufklärungs- auch Untersagungsrechte haben müssen.
- Zusätzlich zur bestehenden Meldepflicht sollten Projekte **genehmigungspflichtig** sein, wenn in ihnen hochsensitive Daten verarbeitet werden, wie dies z. B. bei umfangreichen Gensequenzierungen der Fall ist, oder wenn weiterreichende Zweckänderungen beabsichtigt sind. Auch zeitlich unbegrenzte Studien[878] bzw. Forschungsdatenbanken sollten unter Genehmigungsvorbehalt gestellt werden.

Für ethisch oder technisch besonders anspruchsvolle Projekte wie z. B. internationale Studien, Forschungsnetzwerke, Krankheitsregister oder Biomaterialdatenbanken[879] könnten vom zuständigen UAC bei Bedarf zusätzliche **Anforderungen** festgelegt und zur Genehmigungsgrundlage gemacht werden.

10.9 Biobanken

Modelle für Big Data im Gesundheitsbereich wurden in der jüngeren Vergangenheit insbesondere für Biobanken entwickelt und realisiert. Dabei wird regelmäßig versucht, einen Kompromiss zwischen personaler Selbstbestimmung, etwa durch Einwilligungen und Widerrufsmöglichkeiten, und umfassender Auswert- und Nutzbarkeit zu finden.[880] Biobanken sind **Sammlungen menschlicher Körpersubstanzen** wie Blut, Gewebe, Zellen oder DNA als Träger von Gesundheitsinformationen, die mit personenbezogenen Daten ihrer Spender verknüpft werden bzw. verknüpfbar sind. Zu den verknüpfbaren Daten gehören z. B. Angaben über Krankheiten, Behandlungsverläufe, Medikamenteneinnahmen, Dispositionen, Umweltdaten, Verwandtschaftsbeziehungen, familiäre und soziale Situation und Lebensstil. Biobanken umfassen regelmäßig sowohl eine Proben- wie auch eine Datensammlung, die intern oder für den externen Gebrauch, insbesondere für Forschungsprojekte zur Verfügung gestellt werden. Wesensmerkmal einer Biobank ist die beabsichtigte oder erfolgte genetische Analyse des Materials sowie dessen langfristige Lagerung. Hauptanwendungsfelder sind die medizinische und die pharmazeutische Forschung.[881] In Deutschland gibt es gemäß dem Biobankenregister derzeit über 120 Biobanken.[882]

878 Leopoldina/acatech/Union der Akademien der Wissenschaften, Wissenschaftliche und gesellschaftliche Bedeutung von Längsschnittstudien, Mai 2016.
879 ULD, Datentreuhänderschaft in der Biobank-Forschung, 2009.
880 Deutscher Ethikrat S. 20.
881 ULD (2009) S. 10.
882 www.biobanken.de.

In Deutschland wird seit einigen Jahren über die **Regulierung von Biobanken** diskutiert.[883] Im Frühjahr 2015 wurde von Rechtswissenschaftlern aus Augsburg und München ein Entwurf eines Biobankgesetzes vorgelegt, der aber von der Politik nicht aufgegriffen wurde.[884] Vorgesehen sind darin Regelungen zur informationellen Selbstbestimmung der Proben spendenden Personen über einen informed consent, die Festschreibung eines Biobankgeheimnisses, verfahrens- und organisationsrechtliche Anforderungen mit Qualitätssicherungs-, Dokumentations- und Transparenzpflichten, einer Treuhändernorm und einer Anzeigepflicht gegenüber der Datenschutzaufsicht sowie Zugangsvoraussetzungen für Forschende.

10.10 Open Data

Die **öffentliche Bereitstellung von Daten** durch staatliche Stellen ist eine generelle Zukunftsaufgabe in der Informationsgesellschaft, die sich auch für den Gesundheitsbereich stellt. Der Zweitverwertung von Gesundheitsdaten durch Aufbereitung und Veröffentlichung kann eine wichtige Funktion zukommen für die Hebung des Gesundheitsbewusstseins in der Bevölkerung und insbesondere für deren Kompetenz zu gesundheitsbewusstem Verhalten und zum Ergreifen präventiver Maßnahmen. Insofern kann ein Gemeinwohlinteresse daran bestehen, dass Ergebnisse von Big Data staatlichen Stellen bereitgestellt und von diesen, evtl. in aufbereiteter Form, öffentlich gemacht werden. Entsprechende Ansprüche sind auf verfassungsrechtlicher Ebene in Deutschland bisher nicht anerkannt (s. o. 6.10). Wohl aber steht es dem Gesetzgeber frei und liegt in dessen politischer Entscheidung, den Umfang der Informationsfreiheit zu erweitern.[885] Von diesen Möglichkeiten wird insbesondere durch die Veröffentlichungen von DIMDI im Gesundheitsbereich schon sehr weitgehend Gebrauch gemacht (s. o. 3.8).

Die Entwicklung der Informationsfreiheit, also der Bereitstellung von Informationen der öffentlichen Verwaltung für die Bevölkerung, geht insbesondere von der Landespolitik aus. Am weitesten geht insofern bisher der Landesgesetzgeber Hamburgs mit seinem **Transparenzgesetz**.[886] Soweit keine gesetzlichen Regelungen bestehen und angestrebt werden, steht es der öffentlichen Hand frei, durch Anreize und Förderung den öffentlichen Zugang zu Gesundheitsdaten zu verbessern. Dies gilt unter bestimmten Voraussetzungen auch für die Bereitstellung von Informationen durch Private (Private Open Data). Durch Standards und positive Marktbedingungen können die Voraussetzungen und Bedingungen für ein freiwilliges Zurverfügungstellen von Big-Data-Erkenntnissen im Gesundheitsbereich und zu deren Nutzung verbessert werden. Im kommerziellen Bereich ist auch die

---

883 Deutscher Ethikrat, Humanbiobanken für die Forschung, 2010; Albers MedR 2013, 483 ff.; Herbst DuD 2016, 371 ff.; Pigeot/Hummel Bundesgesundheitsblatt 2016, 301 ff.; Taupitz/Schreiber, Bundesgesundheitsblatt 2016, 3014 ff.

884 Gassner/Kersten/Lindemann/Lindner/Rosenau/Schmidt am Busch/Schroth/Wollenschläger, Biobankgesetz – Augsburg-Münchner-Entwurf, 2015; dazu Gassner/Schmidt am Busch/Wollenschläger DuD 2016, 365 ff.

885 BVerfG 20.6.2017 – 1 BvR 1978/13, Rn. 20 ff., EuGRZ 2017, 477 f.

886 Hamburgisches Transparenzgesetz (HmbTG) v. 19.6.2012, Hamburgisches Gesetz- und Verordnungsblatt I S. 271.

Schaffung von Lizenzierungsmodellen vorstellbar, die zur Grundlage für die Bereitstellung von Daten gemacht werden.

Open-Data-Initiativen müssen nicht von hoheitlicher Seite ausgehen. So gibt es über das Internet eine Vielzahl von privaten Open-Data-Projekten, die darauf beruhen, dass eine große Zahl von Nutzenden ihre Erkenntnisse oder Daten einbringen, z. B. Open Street Map. Derartige Initiativen bestehen auch im Gesundheitsbereich, bei denen Menschen mit dem Ziel der Erforschung von Gesundheitsrisiken ihre individuellen Gesundheitsangaben zur Verfügung stellen. Beispiele hierfür sind die US-amerikanische Open-Science-Organisation Sage Bionetworks, die Schweizer Kooperative MIDATA oder Open Targets.[887] Im wissenschaftlichen und im kommerziellen Bereich gibt es eine Vielzahl von Angeboten, über die seriöse Gesundheitsinformationen vermittelt werden.

10.11 Sicherheit und Strafverfolgung

Big Data hat schon seit längerem bei Sicherheitsbehörden in der Gefahrenvorsorge, der Gefahrenabwehr und der Strafverfolgung Einzug gehalten. Die Technik wird dazu verwendet, auf der Basis gesammelter Erfahrungen Gefahrenprognosen für die Zukunft zu erstellen und hierauf Präventionsprogramme oder Polizeipräsenz auszurichten. Im Bereich der Straftatenbekämpfung wird versucht, bestimmte kriminelle Vorgehensweisen zu erkennen, zu ermitteln und einer Bestrafung zuzuführen.

Von Kriminellen wird Big Data eingesetzt, z. B. um über das sog. Darknet Werkzeuge zur Begehung von Straftaten oder strafbare Inhalte anonym zu vertreiben. Über derartige Crime-as-a-Service-Kriminalität werden z. B. gefälschte Arzneimittel, sog. Fake-Medikamente, auf den Markt gebracht.[888] Mit Hilfe der Ransomware (Erpressungssoftware) WannaCry wurde insbesondere in Großbritannien (London, Blackpool, Hertfortshire und Derbyshire), aber auch in Deutschland (Neuss) die Funktionsfähigkeit einiger Krankenhäuser kurzfristig praktisch vollständig stillgelegt. In Reaktion hierauf streben die Sicherheitsbehörden, was den Technikeinsatz angeht, „Waffengleichheit“ an. Die Aufklärung solcher Kriminalität setzt regelmäßig das Zusammenführen großer Datenmengen durch zentrale Stellen, evtl. aus verschiedenen Staaten voraus.[889] Eine Koordinierungsfunktion innerhalb der Europäischen Union nimmt insofern Europol in Den Haag in den Niederlanden ein.

Big Data mit Gesundheitsdaten kann auch zur Aufklärung eines Verdachts gegenüber einem konkreten Beschuldigten beitragen. Ein Beispiel hierfür ist der seit Jahrzehnten in den USA im Einsatz befindliche, und technisch immer weiter entwickelte „Lügendetektor“ (s. o. 2.1.3). Im „Kampf gegen den Terrorismus“ testete man dort schon im Jahr 2011 eine Art Lügendetektor aus der Entfernung, der über spezielle Sensoren Atemgeschwindigkeit,

887 Deutscher Ethikrat S. 68.

888 Tripmaker, Die guten Hacker, Kieler Nachrichten 11./12.11.2017, Sonntag S. 4.

889 Tripmaker, Erpressungem im Internet nehmen zu, Kieler Nachrichten, 11./12.11.2017, Sonntag S. 5; Ludwig, Das Comeback des Klemmbretts, SZ 18.3.2016, 2.

Herzschlag und Mimik an Sicherheitskontrollstellen erfasst, um dann mit einer Psychosoftware abzuleiten, ob die überprüfte Person „böse Absichten“ verfolgt.[890]

Einen wichtigen Beitrag für die Kriminalitätsbekämpfung können Daten von Gesundheitseinrichtungen für Sicherheitsbehörden darstellen. Ein rechtliches Hindernis stellt insofern das Patientengeheimnis dar (s. o. 6.8).[891] Während Gesundheitsdaten bei Berufsgeheimnisträgern durch einen Offenbarungsschutz (§ 203 StGB) und durch Beschlagnahmeverbote (§ 97 StPO) geschützt sind, existiert ein vergleichbarer Schutz für Daten, die aus der Sphäre der Berufsgeheimnisträger zu Dritten gelangten oder dort noch nicht angekommen sind, nicht. Dies gilt z. B. für die Datenerfassung durch Wearable-Sensoren auf den Geräten der Betroffenen.[892] Dies gilt auch für mit Berufsgeheimnissen Forschende, soweit diese nicht selbst z. B. als Arzt der Schweigepflicht unterliegen, da – entgegen langjährigen Forderungen – bisher kein gesetzliches Forschungsgeheimnis besteht.[893] Zwar wurden zum Ende der 18. Legislaturperiode des Deutschen Bundestags die berufliche Schweigepflicht und der Beschlagnahmeschutz für IT-Dienstleister von Schweigepflichtigen eingeführt.[894] Doch beschränkt sich die Ausweitung des Schutzbereichs auf Personen, die direkt an der „beruflichen oder dienstlichen Tätigkeit mitwirken“ (§ 203 Abs. 3 S. 2, Abs. 4 Nr. 1, 2 StGB; § 53a Abs. 1 StPO). Dies ist bei Big-Data-Auswertungen, die über die Berufsausübung hinausgehende Ziele verfolgen, regelmäßig nicht der Fall.

10.12 Auslandsbezüge

Big Data muss sich nicht auf die Analyse im Inland erhobener Daten beschränken. Für die Verarbeitung von personenbezogenen Daten generell besteht mit Wirksamwerden der DSGVO ein rechtlich harmonisierter europäischer Binnenmarkt, so dass ein grenzüberschreitender Austausch innerhalb der EU keinen spezifischen Einschränkungen unterliegt (Art. 1 Abs. 3 DSGVO, zuvor schon Art. 1 Abs. 2 EG-DSRl). Keine weiteren Beschränkungen bestehen auch, wenn die EU-Kommission festgestellt hat, dass im Drittland, wo europäische Daten verarbeitet werden sollen, ein angemessenes Datenschutzniveau besteht (Art. 45 DSGVO, Art. 25 Abs. 1, 2 EG-DSRl).

Wurde nicht förmlich die Angemessenheit des Datenschutzes im Empfängerland der Daten festgestellt ist, so kann eine Datenübermittlung – auch für Zwecke von Big Data – durch entsprechende Garantien, evtl. auf der Grundlage von Standardvertragsklauseln oder sog.

890 Distanz-Lügendetektor bei Kontrollstellen, DANA 2011, 129; Der Spiegel 23/2011, 124.
891 Ausführlich dazu Hauser/Haag S. 116 ff.
892 Theißen S. 391.
893 Kritisch Weichert in Däubler u. a., BDSG, § 40 Rn. 7; Simitis in Simitis § 40 Rn. 14.
894 Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter bei der Berufsausübung schweigepflichtiger Personen v. 30.10.2017, BGBl. I S. 3618; dazu Dierlamm/Ihwas BB 2017, 1097 ff.; Hartung/Steinweg, DB 2017, 2081 ff.; Ruppert K&R 2017, 609 ff.; Wronka RDV 2017, 129; ULD 36. TB 2017 Kap. 4.6.2 (S. 48).

Binding Corporate Rules legitimiert werden (Art. 46, 47 DSGVO, bisher Art. 25, 26 EG-DSRl, §§ 4b, 4c DSGaF).[895]

Bei der nationenübergreifenden Zusammenführung und Auswertung von Gesundheitsdaten spielt die Weltgesundheitsorganisation (World Health Organization – WHO) eine wichtige Rolle. Es besteht ein globales Interesse an der Verbesserung des Wissens über Gesundheit und über medizinische Zusammenhänge. Zur Gewinnung dieses Wissens ist ein weltweiter Austausch über Grunddaten wie über Auswertungsergebnisse erforderlich. Mit Hilfe von Big Data können Ursachen und Verlauf von Krankheitsepidemien erkannt und analysiert werden.[896] Die WHO engagiert sich schon heute bei Informations- und Forschungskampagnen zu Gesundheitsfragen.[897]

11 Schlussfolgerungen

Die Darstellung von Big Data im Gesundheitsbereich und der rechtlichen Einstufung zeigt, dass Bewertungen von konkreten Anwendungen jeweils stark von den Akteuren, deren Interessen, den bestehenden Regelungen und dem konkreten gesellschaftlichen Kontext abhängen.[898] Nutzen und Risiken bzw. Schäden liegen oft nahe beieinander.[899] Die Aufgabe für die Politik, die Anwendenden sowie alle sonstigen Beteiligten besteht darin, die technischen Möglichkeiten von Big Data im Gesundheitsbereich so weit wie möglich auszuschöpfen und dabei die damit verbundenen Risiken zu vermeiden.

Die Schaffung bzw. Bereitstellung einer einheitlichen Infrastruktur ist angesichts der Vielzahl von Beteiligten mit teilweise sehr unterschiedlichen Interessen eine grundlegende Voraussetzung für die Kommunikation über Big Data sowie für einen gemeinsamen Einsatz und für gesellschaftlichen Nutzen. Interoperabilität setzt informationstechnische Vernetzung und die Anerkennung gemeinsamer Standards voraus.[900] Dabei muss verhindert werden, dass Partikularinteressen eine dominante oder eine innovationsbehindernde Rolle erhalten.

11.1 Normierungsbedarf

Bei der Regulierung von Big Data im Gesundheitsbereich muss der verfassungsrechtliche Rahmen leitend sein, der die kulturellen Werte unserer freiheitlichen demokratischen Gesellschaften sowie ethische Gemeinsamkeiten in gültige und beachtete Normen umsetzt. Es kann und darf nicht darum gehen, Erkenntnis- und Wertschöpfungsmöglichkeiten zulasten des Gemeinwohls und der individuellen Grundrechte zu eröffnen (s. o. 9.3.4). Leitkonzept bei der Regulierung sollte die

895 Deutscher Ethikrat S. 110 ff.; Schröder in Kühling/Buchner Art. 44 ff.
896 Häußermann, Mit Big Data in den Kampf gegen Ebola, www.bigdata-insider.de 31.10.2014.
897 Kupferschmidt, Hauptsache gesund, SZ 12.1.2018, 14.
898 Zu bestehenden Zielasymmetrien Strategy/pwc S. 119 ff.
899 Deutscher Ethikrat S. 81.
900 Wallenfels, Spielregeln für Big Data fehlen, www.aerztezeitung.de 15.12.2017.

informationelle, medizinische und sonstige Selbstbestimmung der Menschen sein.[901] Marktmechanismen sollten aber dort freie Entwicklungsmöglichkeiten eröffnen, wo die damit einhergehenden Risiken beherrschbar sind und der Wettbewerb ein pluralistisches Informations-, Produkt- und Dienstleistungsangebot hervorbringt.

Die Potenziale von Big Data im Gesundheitsbereich lassen sich nur realisieren, wenn den Beteiligten ein klarer Rechtsrahmen bereitsteht, der technische und ökonomische Innovation und Entfaltung ermöglicht.[902] Deregulierung ist dort angebracht, wo sich überkommene Rechtsinstrumente für die neue technische Herausforderung als inadäquat erweisen. Rechtsunsicherheit durch fehlende Regelungen ist für eine freie gemeinschaftsförderliche Entfaltung der sich entwickelnden Potenziale ein großes Hindernis.

Angesichts der Unsicherheit bei der Regulierung von Big Data bietet sich generell das Instrument der Evaluierung an: Regelungen sind nach Ablauf einer definierten Periode auf ihre technischen, ökonomischen, demokratischen und sozialen Wirkungen hin zu überprüfen verbunden mit der Frage, inwieweit aus den Evaluierungserkenntnissen neue normative Schlussfolgerungen zu ziehen sind.[903] Um diesen Prozess verbindlicher zu machen, können in Regelungen Verfallsklauseln vorgesehen werden, wonach die Erlaubnisse zu bestimmten (Big-Data-) Verarbeitungen von einem bestimmten Zeitpunkt aufgehoben werden, wenn nicht zuvor eine ausdrückliche Bestätigung durch den Normgeber erfolgt.[904]

11.1.1 Verfassungsrecht

Der Einsatz von Big Data im Gesundheitsbereich ist von hoher verfassungsrechtlicher und insbesondere grundrechtlicher Relevanz. Zwar gibt die Europäische Grundrechte-Charta (GRCh) gegenüber dem deutschen Grundgesetz präzisere und technikadäquatere Antworten auf die neuen technischen Herausforderungen.

Doch bedarf es auf verfassungsrechtlicher Ebene einer Diskussion über die Notwendigkeit einer weitergehenden verfassungsrechtlichen Regulierung zum Thema Big Data sowie den damit verbundenen Möglichkeiten. Mit dem Entwurf für eine digitale Grundrechte-Charta (dGRCh-E, s. o. 6.2) werden insofern wertvolle Anregungen gegeben. Dieser Entwurf enthält u. a. Aussagen zum Profiling (Art. 6 dGRCh-E), zu Algorithmen, zur künstlichen Intelligenz (Art. 7 dGRCh-E), zur Transparenz (Art. 9 dGRCh-E), zur Datensouveränität (Art. 11 dGRCh-E), zum Zugang zu Diensten (Art. 15 dGRCh-E) oder zum Immaterialgüterschutz (Art. 22 dGRCh-E). Die Vorschläge sind bisher eher programmatischer Natur und genügen noch nicht den Anforderungen an rechtliche Klarheit und Logik. Sie benennen aber die relevanten Stichworte und thematisieren den Regulierungsbedarf.

---

901 Der Deutsche Ethikrat S. 173 ff. verwendet hierfür den missverständlichen Begriff der „Datensouveränität".

902 Strategy/pwc S. 181 ff.

903 Eine allgemeine Evaluierungsklausel enthält Art. 97 DSGVO; vgl. § 48 BDSGaF.

904 Weichert in Däubler u. a. Einl. Rn. 24.

Die Diskussion über digitale Grundrechte darf sich nicht auf die europäische Ebene beschränken. Angesichts des jungen Alters der GRCh und eines engeren Diskussionszusammenhangs auf nationaler Ebene besteht eine größere Chance innovativer Ansätze im nationalen Verfassungsrecht, die für die europäische wie die internationale Ebene inspirierend sein können.

11.1.2 Völkerrecht

Die Vereinten Nationen (United Nations Organization- UNO), deren Unterorganisationen sowie sonstige völkerrechtliche Institutionen, insbesondere im vorliegenden Bereich die Weltgesundheitsorganisation (World Health Organization – WHO), können sich dem globalen Digitalisierungsdruck nicht entziehen, der von der Vernetzung und dem Einsatz von Big Data und KI ausgeht. Angesichts der teilweise sehr unterschiedlichen Kulturen, den verschiedenen politischen Systemen sowie dem unterschiedlichen technischen Entwicklungsstand bei der Digitalisierung des Gesundheitswesens ist eine Verständigung auf dieser Ebene nicht einfach. Da aber Big Data gerade bei der Bewältigung der großen Überlebensfragen der Menschheit in bisher weniger entwickelten Ländern ein möglicher Lösungsansatz sein kann, können sich Verständigungen durch pragmatischen Handlungsdruck ergeben (s. o. 10.12).

Abgeleitet aus den allgemeinen Menschenrechten bedarf es eines globalen Diskurses über deren Konkretisierung angesichts neuer technischer Möglichkeiten und gesundheitspolitischer Herausforderungen. Die Bundesregierung sollte in der UNO sowie in zugeordneten Organisationen darauf hinwirken, dass möglichst verbindliche Regelwerke auf internationaler Ebene geschaffen werden, in denen grundrechtliche oder grundrechtsähnliche Schutzvorkehrungen bei der und Standards für die Digitalisierung im Gesundheitsbereich geschaffen werden. Parallel dazu sind Projekte zu fördern, in denen globale gesundheitsnützliche Datensammlungen und -auswertungen vorangebracht werden.

11.1.3 Europäische Regulierung

Zwar ist die Europäisierung der Gesundheitspolitik, anders als die Politik zum digitalen Binnenmarkt, noch nicht weit fortgeschritten (vgl. aber Art. 168 AEUV). Angesichts des Umstands, dass Gesundheitsrisiken an nationalen Grenzen keinen Halt machen, gemeinsame Anstrengungen zu deren Bewältigung förderlich sind und schon vielfältige Verflechtungen und gegenseitige Abhängigkeiten bestehen, ist eine Trendwende in der EU absehbar, die durch die informationstechnische und wissenschaftliche Vernetzung befördert wird. Dabei wird es auf einer übergeordneten Ebene auch darum gehen, angesichts der Digitalisierung aller Lebensbereiche grundrechtliche Standards festzulegen (s. o. 11.1.1).[905] Parallel dazu sind die konkreten Anwendungen daraufhin zu überprüfen, inwieweit sie europäische Relevanz haben und sich daraus ein Normierungsbedarf ergibt. Dabei sollten Ansätze, wie sie z. B. im Arzneimittel- (s. o. 10.2), im

[905] Vgl. Charta der Digitalen Grundrechte der Europäischen Union, https://digitalcharta.eu/; abgedruckt z. B. in SZ 1.12.2016, 25.

Medizinproduktesicherheitsbereich (s. o. 10.3) und im Datenschutz (s. o. 7.2) bestehen, weiterentwickelt werden. Neue Herstelleranforderungen oder Zertifizierungsmöglichkeiten können in weiteren Marktsegmenten erarbeitet werden. Dies gilt beispielhaft für die Erhebung und Auswertung von Gesundheitsdaten in Lebensbereichen, die bisher von der medizinischen Regulierung nicht erfasst sind.

Das bisherige europäische Datenschutzrecht im Gesundheitsbereich ist gekennzeichnet von einer Parallelität eines in der EU teilweise vereinheitlichten Datenschutzrechts und einem weitgehend nationalen medizinischen Berufsrecht mit Regelungen zur beruflichen Schweigepflicht bzw. zum Patientengeheimnis. Durch eine Harmonisierung des medizinischen Berufsrechtes würde nicht nur der Binnenmarkt im Gesundheitswesen gestärkt. Es könnte zugleich ein gemeinsames hohes Schutzniveau für die Patienten geschaffen werden. Dies käme insbesondere grenzüberschreitendem Big Data zugute, für das nationale medizinische Sondervorschriften oft ein Hindernis darstellen.

In der EU findet eine Diskussion darüber statt, verbraucherrechtliche Sammelklagen zuzulassen, um die kollektive Durchsetzung von Verbraucherrechten zu verbessern.[906] Da bei Big Data im Verbraucherbereich regelmäßig viele Betroffene mit wenig individueller Rechtsdurchsetzungskraft tangiert sind, wäre eine derartige Rechtsänderung positiv zu bewerten.[907]

Im Bereich der Forschung und der informationellen wissenschaftlichen Kooperation finden schon ein reger Austausch und Aktivitäten der Harmonisierung und Standardisierung – auch im Gesundheitsbereich – statt (s. o. 10.8, s. u. 11.6). Dies hat hier bisher aber nur eingeschränkt zu einer rechtlichen Harmonisierung geführt. Durch einheitliche Regelungen zu Gesundheitsdaten im Datenschutzrecht sollten die bisher bestehenden Öffnungsklauseln zugunsten gemeinsamer oder harmonisierter Regelungen zurückgedrängt werden (s. o. 10.8.1).

11.1.4 Nationales Recht generell

Die Regulierung von Big Data im Gesundheitsbereich durch den nationalen Gesetzgeber blieb mit den Krebsregistergesetzen bisher die Ausnahme. Ein Grund hierfür mag darin liegen, dass der Regulierungsbedarf bisher noch nicht hinreichend erkannt wurde. Ein weiterer Grund dürfte sein, dass sich die Gesetzgeber angesichts der Komplexität der Regelungsmaterien und der rasanten technischen, sozialen und wissenschaftlichen Entwicklung (noch) nicht in der Lage sah, verbindliche Festlegungen vorzunehmen. Dies zeigte sich z. B. bei dem Bestreben einer generellen Regulierung von Big Data in der DSGVO.[908]

---

906 Hülsen/Müller, „Gute Absichten machen skeptisch“, Der Spiegel 4/2018, 69; vgl. EuGH 25.1.2018 – C-498/16.

907 Martini JZ 2017, 1024.

908 Albrecht/Jotzo Kap. 3 Rn. 6, 66.

Die Bereitstellung von Gesundheitsdaten für die Versorgungsplanung, die Verbesserung der medizinischen Versorgung und die Herstellung demokratischer Transparenz im Gesundheitswesen ist eine Aufgabe, die in Deutschland dem Bund wie auch den Ländern obliegt. Die Erfüllung dieser Aufgaben wird – den Gesetzgebungskompetenzen folgend – bisher über einen Flickenteppich unterschiedlicher Bundes- und Landesgesetze geregelt, die inhaltlich voneinander abweichen und teilweise sogar zueinander im Widerspruch stehen können. Dies gilt insbesondere dort, wo Bundes- und Landesregelungen parallel zur Anwendung kommen, evtl. ergänzt durch Vorschriften des Standesrechts sowie untergesetzliche Standards, Leitlinien oder Verhaltensregeln.[909] Ein Beispiel hierfür ist die Gesundheitsforschung, für die Big Data eine wichtige Methode ist. Für die Beteiligten ist die aktuelle unübersichtliche und teilweise widersprüchliche Regulierung nicht wünschenswert. Angesichts dessen ist zu erwägen, dass **Bund und Länder über Staatsverträge** einheitliche transparente Regelungen anstreben, mit denen sowohl eine größtmögliche Funktionalität wie auch ein größtmöglicher Schutz vor unerwünschten Wirkungen durch materielle, technische, organisatorische und prozedurale Maßnahmen sichergestellt werden (s. o. 10.8.4). Solche E-Health-Staatsverträge sollten auf eine weitgehende Zustimmung der betroffenen Interessengruppen stoßen. Die europäischen Regelungen, etwa die DSGVO, geben hierfür sowohl den nötigen Spielraum wie auch einen validen übergeordneten normativen Rahmen.[910]

Der **Gesetzgeber** sollte sich bei der Regulierung von Big Data im Gesundheitsbereich auf das Wesentliche beschränken; dies bedarf aber wegen der hohen Grundrechtsrelevanz einer umfassenden parlamentarischen demokratischen Debatte und der normativen Festlegung.[911] Der parlamentarische Gesetzgeber ist mit der Bewältigung der Aufgabe der Normierung wegen der Innovationsgeschwindigkeit sowie des hohen Komplexitäts- und Spezialisierungsgrads schnell überfordert. Diese Erkenntnis darf nicht dazu führen, dass hinsichtlich der demokratischen Legitimation der Lösungen Abstriche gemacht werden. Durch maximale Transparenz sowie die Einbindung von möglichst weitgehend demokratisch legitimierten Fachgremien, etwa Aufsichtsbehörden, Beiräten, Ethikkommissionen oder Fachbeauftragten, kann dem entsprochen werden. Der Gesetzgeber sollte sich aber auf die Vorgabe von Zwecken und Zielen sowie die Festlegung verbindlicher Verfahren zur Aushandlung der materiellen oder auch technischen Vorgaben beschränken.

Die **normativen Konkretisierungen** können durch Verwaltungsregeln sowie im Rahmen regulierter Selbstregulierung erfolgen (s. o. 8.22). Dank ihrer größeren Fachnähe und der Flexibilität können die staatliche Aufsicht und die verbandlich organisierten wirtschaftlichen und gesellschaftlichen Interessen die nötigen Präzisierungen vornehmen. Dabei ist darauf zu achten, dass größtmögliche Transparenz wie eine umfassende

909 Deutscher Ethikrat S. 184, kritisch Fischer in Deutscher Ethikrat S. 187 f.

910 Weichert DuD 2014, 837 f.

911 BVerfG 9.5.1972 – 1 BvR 518/62 u. 308/64 (Facharzt), BVerfGE 33, 125; BVerfG 8.8.19978 – 2 BvL 8/77 (Technikrecht, Kalkar), BVerfGE 49, 89.

Vertretung aller relevanten Interessen gesichert sind. Die in der DSGVO für den Datenschutz entwickelten Instrumente von Verhaltensregeln und Zertifizierungen lassen sich auf andere Regelungsbereiche des Gesundheits-Big-Data übertragen und in einheitlichen Regelungen zusammenfassen.

Bei den normativen Lösungen ist regelmäßig ein **Mix von materiell-rechtlichen, prozeduralen sowie technisch-organisatorischen Vorkehrungen** sinnvoll. Wichtige prozedurale Maßnahmen sind Zertifizierungen sowie regelmäßige Evaluationen bzw. unabhängige Audits. Bei der Festlegung dieses Mixes gibt es keine allgemeingültigen Antworten; dessen Zusammensetzung muss sich bzgl. der jeweiligen Anwendungen an den bestehenden Rechten und Interessen orientieren.

Während es für andere Branchen (Nahrungsmittel, Kfz) teilweise detaillierte gesetzgeberische Vorgaben für und Anforderungen an Produkte gibt, werden die **Hersteller für IT-Produkte** bisher zumeist weder prozedural noch qualitativ-inhaltlich in die Pflicht genommen. Soweit solche Pflichten bestehen (z. B. für Arzneimittel, Medizinprodukte, s. o. 10.2, 10.3) zielen die Anforderungen noch nicht hinreichend auf die informationstechnisch bedingten Risiken. Das Datenschutzrecht berücksichtigt die Hersteller nur indirekt bei der Regulierung zur Zertifizierung (Art. 42 DSGVO). Eine spezifische Kontrolle von riskanten Algorithmen ist bisher nicht gewährleistet. Insofern bedarf einer umfassenden Bestandsaufnahme des Regelungsbedarfs und der Umsetzung der daraus erlangten Erkenntnisse. Dabei sollte nicht erst bei der Auslieferung von Produkten im Markt angesetzt werden, sondern schon in den Bereichen Forschung, Entwicklung und Testung.

Der Staat selbst kann seinen Schutzpflichten angesichts der rasanten Entwicklung bei der Digitalisierung aller Lebensbereiche nicht mehr hinreichend nachkommen. Angesichts dessen muss geprüft werden, inwieweit durch gesetzliche Pflichten den privaten Anbietern digitaler Angebote auferlegt wird, die Nutzer zu schützen und ihnen **Hilfsangebote** zu machen. Dabei ist aber darauf zu achten, dass mit diesem Schutz und mit diesen Hilfen nicht noch weitergehend in Grundrechte eingegriffen wird (s. o. 7.4).

11.1.5 Datenschutzrecht

Die grundlegende Herausforderung besteht darin, die allgemeinen Regeln der Europäischen Datenschutz-Grundverordnung (DSGVO), insbesondere deren Regelung zum Profiling und zu automatisierten Entscheidungen in Art. 22 DSGVO, für konkrete Anwendungen zu präzisieren. Dabei geht es nicht nur um Anwendungsfälle (sog. Use Cases) und die Festlegung von für diese nötigen rechtlichen Rahmenbedingungen, z. B. die Formulierung von Einwilligungstexten und die Gestaltung von Transparenz- und Optionsverfahren, die Wahl guter Verarbeitungskonzepte und der richtigen Pseudonymisierungs- und Auswertungsstrategien. Es geht vielmehr auf einer abstrakteren Ebene um die Festlegung eines spezifischen **materiellen, prozeduralen sowie technisch-organisatorischen Rahmens**, der sich zwischen den Vorgaben der DSGVO und den Use Cases bewegt. Eine Reduzierung der Komplexität wird dadurch erreicht, dass die Normierung auf die wesentlichen abgrenzbaren Aspekte beschränkt wird. Dabei sollte im

Interesse der Entwicklungsoffenheit und der Technikneutralität ein hinreichendes Abstraktionsniveau gewahrt bleiben. In der Regel bietet sich insofern eine regulierte Selbstregulierung an (s. o. 8.22).

Bei der Festlegung neuer datenschutzrechtlicher Regeln kann auf die bestehenden Regelungskonzepte zurückgegriffen werden. Als trügerisch erweist sich aber bei hohem Sozialbezug, hoher Sensitivität und hoher Komplexität die Vorstellung, dass die Einwilligung der Goldweg zur Verwirklichung informationeller Selbstbestimmung sei (s. o. 10.8.2). Einerseits gibt es Formen der Datenverarbeitung, die – z. B. wegen der Verletzung der menschlichen Würde – nicht einwilligungsfähig sind.[912] Zum anderen bestehen an personenbezogener Datenverarbeitung Gemeinwohlinteressen, deren Wahrnehmung nicht von einer individuellen Zulassung abhängig gemacht werden können. Diese Umstände dürfen aber nicht zum Entzug von Transparenz und Wahlfreiheit für die Betroffenen führen. Hierzu, zur Umsetzung des „Privacy by Default", sind technische Lösungen denkbar, etwa kaskadisch strukturierte Einwilligungsmodelle (s. o. 8.8.1 u. 8.8.2).[913] Soweit bisher für Einwilligungen ausschließlich ein analoges Vorgehen erlaubt ist (Schriftform), sollten auch digitale Erklärungen ermöglicht werden (s. o. 3.5.1) Das Vorliegen von wirksamen Betroffeneneinwilligungen entbindet den Staat nicht von seiner staatlichen Fürsorgepflicht, der er dadurch nachkommen kann und muss, dass die Rahmenbedingungen für zulässige Datenverarbeitung präzise festgelegt werden. Diese Schutzpflicht ist dort besonders wichtig, wo im gesellschaftlichen Interesse einwilligungsfrei Verarbeitungen erlaubt werden.

Neben der bisher freiwilligen Zertifizierung von riskanten Verfahren sollten bei präzise zu beschreibenden hochriskanten Verfahren, wie sie im Gesundheitsbereich vorkommen, obligatorische Zertifizierungen gesetzlich vorgesehen werden (s. o. 8.22.1).

Hinsichtlich der aufsichtlichen Kontrolle hochsensitiver Verarbeitungen des Big Data im Gesundheitssystem sollten gesetzliche Festlegungen in Bezug auf die Prüffrequenz und die Prüftiefe erfolgen (8.19).

Ein Bereich, in dem sowohl ein hoher Novellierungsbedarf wie auch die Möglichkeiten hierfür bestehen, ist die medizinische Forschung. Durch eine bundesweite einheitliche Regulierung der Nutzung von Behandlungsdaten für Forschungszwecke, mit Melde- und Genehmigungspflichten für Biobanken, Krankheitsregister und Forschungsnetzwerke, die Normierung eines Transparenz-, Einwilligungs- und Widerspruchsmanagements und die Etablierung von untereinander vernetzten Use-and-Access-Committees zur Prüfung und Zulassung von Datenzugängen können Forschungsstandards weiterentwickelt und die Voraussetzungen für die Entwicklung einer einheitlichen medizinischen

912 Weichert in Kühling/Buchner Art. 9 Rn. 48; a. A. wohl Fischer in Deutscher Ethikrat S. 186.
913 Deutscher Ethikrat S. 178.

Forschungsinfrastruktur geschaffen werden (s. o. 10.8.4).[914] Ein Forschungsgeheimnis sollte als Berufsgeheimnis etabliert werden, um sicherzustellen, dass Patientengeheimnisse, die für Forschungszwecke verwendet werden, einen Offenbarungs- und einen Beschlagnahmeschutz genießen (s. o. 10.11).

Auf einige neue Fragen hat die Rechtsordnung noch keine Antworten gefunden. Dies gilt für die Bewertung von Sensorik, die in den Kernbereich privater Lebensgestaltung eingreift, indem sie Gedanken, Gefühle und Stimmungen erfasst, speichert und auswertet. Für die Schnittstellen zwischen Computer und Mensch, die sich mit Biotechnologie und Robotik innovativ weiterentwickeln, müssen anwendungsspezifische Anforderungen definiert, umgesetzt, erprobt und normiert werden (s. o. 2.1.3). Dabei muss beachtet werden, dass in jedem Bereich, ja oft bei jeder konkreten Anwendung angepasste Antworten gefunden werden müssen.

Entsprechendes für den Einsatz sog. künstlicher Intelligenz (s. o. 2.9, 8.5).

Das Statistikrecht sollte angesichts der modernen Erkenntnismöglichkeiten der Nutzung von Big Data und den Möglichkeiten der Re-Identifizierung auf die Höhe der Zeit gebracht werden (s. o. 10.7). Anlass genug hierfür ist die Privilegierung der Statistik und der Normierung eines europäischen Rahmens durch die DSGVO.

11.1.6 Haftungsrecht

Angesichts der mit Big Data insbesondere im Gesundheitsbereich verbundenen Risiken ist es angemessen und notwendig, neue Haftungsmodelle zu entwickeln. Diese können in einer Klarstellung der (haftungsrechtlichen) Verantwortlichkeiten, der Festlegung von gemeinsamer Haftung, in Haftungserleichterungen und einer Beweislastumkehr[915] oder in einer Ausweitung der Produkt- bzw. Gefährdungshaftung liegen.[916]

11.1.7 Versicherungsrecht

Der Einsatz von Künstlicher Intelligenz und Big Data im Versicherungswesen führt dazu, dass die Transparenz und die Einflussmöglichkeiten für die Verbraucher abgebaut werden. Dem sollte durch Transparenzregeln entgegengewirkt werden (s. o. 3.5, 10.5.2-10.5.4).

Die Zulässigkeit von Telematiktarifen oder von Bonusprogrammen, die auf Datenerhebungen beim Versicherten während des Versicherungsverhältnisses erfolgen, sollten gesetzlich so beschränkt werden, dass Diskriminierungen vermieden und das Solidarprinzip gewahrt bleiben (s. o. 10.5.1). Dies kann dadurch erfolgen, dass näher zu definierende Tarifgestaltungen gesetzlich verboten werden. Zumindest sollten Gesetze erlassen werden, die telematikbasierte Prämienberechnungen einer Genehmigungspflicht unterwerfen (s. o. 10.5.4).

---

914 Krawczak/Weichert, DANA 2017, 193 ff.; diess. http://www.uni-kiel.de/medinfo/documents/TWMK%20Vorschlag%20DInfMedForsch%20v1.9%20170927.pdf; vgl. Deutscher Ethikrat S. 174 f.

915 Theißen S. 446 ff.

916 Theißen S. 452 ff.; Deutscher Ethikrat S. 181 f.; BMVI S. 77, 122, 128.

11.1.8 Verbraucherrecht

Das Verbraucherrecht kennt bisher keine adäquaten Antworten auf die Herausforderungen von Big Data. Dies gilt auch für den ansonsten engmaschigen Verbraucherschutz bei Gesundheitsdienstleistungen. Lediglich hinsichtlich der gemeinsamen **Schnittmenge zum Datenschutz** bestehen Regelungen, die jedoch weiterentwickelt werden sollten.

Den Verbrauchern sollten rechtliche und technische Möglichkeiten gegeben werden, die Verarbeitung ihrer Daten gegenüber digitalen Anbietern zu steuern und zu verwalten. Hierzu können normative Vorgaben für **Datenagenten** sowie die Entwicklung von entsprechenden Angeboten sinnvoll sein, mit denen die Nutzer ihre voreingestellten Präferenzen z. B. im Hinblick auf Nutzungseinwilligungen gegenüber Online-Anbietern kommunizieren können (s. o. 8.8.1).[917]

Das **Medizinprodukterecht** ist dahingehend weiterzuentwickeln, dass die Datenschutzkonformität zu den selbstverständlichen Anforderungen von digitalen Produkten wird (s. o. 10.3).

Das Medizinprodukterecht schafft keinen Verbraucherschutz für den Lifestyle- und Wellnessbereich, in dem massenhaft Gesundheitsdaten erfasst werden, die Big-Data-Anwendungen zugeführt werden. In diesem Bereich sollten **Qualitätsgütesiegel** geschaffen werden, bei denen neben dem Datenschutz auch weitere Verbraucheranforderungen (Transparenz, Anwendungsfreundlichkeit, Portabilität) geprüft werden.[918] Das Qualitätsgütesiegel sollte für den Marktzugang nicht zur Pflicht gemacht werden, sondern als vertrauensförderndes Marktinstrument entwickelt und etabliert werden (s. o. 8.22.2).

Ein zentrales Problem bei der Durchsetzung von Verbraucherrechten besteht darin, dass dem einzelnen Verbraucher für die gerichtliche Durchsetzung seiner Rechte die nötigen finanziellen Ressourcen sowie das rechtliche und technische Know-how fehlen. Dieses Defizit lässt sich über kollektive Rechtsbehelfe und Klagemöglichkeiten kompensieren, wie sie mit der Verbandsklage nach dem UKlaG bestehen (vgl. Art. 80 Abs. 2 DSGVO). In Deutschland bisher nicht möglich ist die **verbraucherrechtliche Sammelklage**, die gemäß Art. 80 Abs. 1 DSGVO datenschutzrechtlich möglich ist (s. o. 8.18.2, 11.1.3).

Das **Kartell- und Wettbewerbsrecht** spielte lange Zeit bei der Diskussion um die Regulierung der Digitalisierung keine wichtige Rolle.[919] Dies hat sich in den letzten Jahren geändert, nachdem allgemein bewusst wurde, wie informationstechnische Konzerne ihre Marktmacht nutzen, um einen pluralen Wettbewerb und damit die Wahl- und Einflussmöglichkeiten von Verbrauchern zu beschränken. Wettbewerbsschädigende Konzentrationen bestehen insbesondere im Internet, wo wenige Oligopolisten den Markt beherrschen und in Marktsegmenten (z. B. bei Internetsuche Google, beim Onlinehandel

---

917 Deutscher Ethikrat S. 177; Theißen S. 426 ff.
918 Deutscher Ethikrat S. 175, 184.
919 Kritisch schon früh Weichert DuD 2007, 724.

Amazon) Quasimonopole herrschen. Auch im Bereich des Medizinmarketings bestehen wettbewerbsschädliche Konzentrationen (s. o. 3.2, 4.8). Diese Konzentrationen haben Auswirkungen auf den Einsatz von Big Data im Gesundheitsbereich, etwa, wenn Algorithmen eine neutrale Suche im Gesundheitsbereich verhindern oder wenn im Netz über eine Personalisierung individualisierte Preise für Gesundheitsleistungen verlangt werden. Der Monopolisierung der Verfügung über Big Data muss begegnet werden.[920] Das Kartell- und Wettbewerbsrechts ist an die Spezifika digitaler Märkte weiter anzupassen, um wettbewerbsschädigende Konzentrationen zu verhindern.

11.1.9 Arbeitsrecht

Big Data mit Gesundheitsdaten eröffnet gewaltige Überwachungs- und Diskriminierungsmöglichkeiten im Beschäftigungsbereich. Dem kann mit **arbeitsrechtlichen Verarbeitungsverboten** gegengesteuert werden (vgl. §§ 19 ff. GenDG), durch die übermäßige Verhaltens- und Leistungskontrollen und spezifische Benachteiligungen unterbunden werden.

Ähnlich wie im Verbraucherrecht sollten die Möglichkeiten des **Kollektivrechtsschutzes** ausgeweitet werden. Dies kann durch zusätzliche Klagemöglichkeiten von Betriebsräten oder von Gewerkschaften vorgesehen werden und zwar sowohl als materiell-rechtliche Rechtskontrolle in Form der Verbandsklage wie auch als vermögensrechtliche Sammelklage.[921]

11.1.10 Open Daten - Informationsfreiheit

Generell gilt wegen der mit Big Data im Gesundheitsbereich verbundenen Risiken, dass Geheimhaltungsregelungen zurückgefahren und **Open-Data**-Anforderungen – auch im Bereich der privaten Wirtschaft – gesetzlich zu normieren sind. Hier besteht eine gesellschaftliche Relevanz, weshalb, egal ob von privaten oder öffentlichen Stellen praktiziert, öffentliche Mitbestimmung und Kontrolle notwendig sind (s. o. 10.10). Dem stehen immaterielle Ausschließlichkeitsrechte, wie sie aktuell immer wieder im Interesse einer verstärkten Ökonomisierung der Digitalisierung teilweise gefordert werden, entgegen (s. o. 9.3). Letztlich profitiert die Gesamtwirtschaft vom adäquaten Teilen und von den staatlich zu finanzierenden Regulierungs- und Aufsichtsstrukturen. Ebenso behindert Deregulierung, wie sie z. B. in den USA praktiziert wird, plurales öffentliches Marktgeschehen und damit Kreativität und Gemeinsinn.

Durch die Etablierung und Fortentwicklung von **Wissensdatenbanken** im Gesundheitsbereich sowohl für die Forschergemeinde (Krankheitsregister) sowie für die Allgemeinheit (z. B. bei DIMDI, s. o. 3.8) kann der Wissenstransfer verlässlich und diskriminierungsfrei im Medizinbereich organisiert werden.

---

920 Ladeur DuD 2016, 362.

921 Schuler/Weichert, Die EU-DSGVO und die Zukunft des Beschäftigtendatenschutzes, 8.4.2016, https://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2016_dsgvo_beschds.pdf, S. 21.

Eine noch nicht hinreichend erörterte Aufgabe besteht darin, gesellschaftlich wie individuell relevante **Algorithmen transparent** und damit allgemein bewert- und kontrollierbar zu machen. Dabei geht es sowohl um die Offenlegung der einfließenden Daten, der Zwecke, der handelnden bzw. verantwortlichen Stelle wie auch der Ableitungen, Schlüsse und Entscheidungen.[922] Hierfür könnte die Infrastruktur der Datenschutz- und Informationsfreiheitsbeauftragten genutzt werden.

11.2 Administrative Ebene

Die Schaffung einer **Informations- und Wissensstruktur** ist eine zentrale Grundbedingung für den gemeinwohlförderlichen Einsatz von Big Data im Gesundheitsbereich. Dabei dürfen die Fehler, die bei der Etablierung der Telematik-Infrastruktur gemacht wurden, nicht wiederholt werden. Diese bestanden darin, dass potenziellen oder eingebildeten Innovations-Verlierern faktische Veto- bzw. Verhinderungsmöglichkeiten eingeräumt wurden.

Eine leistungsfähige und zugleich vertrauenswürdige und verlässige **Kommunikationsinfrastruktur** ist für den für Big Data notwendigen Datenaustausch unerlässlich. Dies bedingt eine hinreichende Bandbreite und Geschwindigkeit der Kommunikationsnetze sowie den diskriminierungsfreien Zugang hierzu (Stichwort Netzneutralität). Eine wünschenswerte Maßnahme wäre insofern die Etablierung verlässlicher, preiswerter oder unentgeltlicher Signierungs- und Verschlüsselungsangebote für Endverbraucher wie für an Big-Data-Kommunikationen beteiligten Stellen.

Eine Grundvoraussetzung für eine gemeinschaftsförderliche Digitalisierung der Gesellschaft generell wie auch eines verantwortlichen Einsatzes von Big Data im Gesundheitsbereich ist der Aufbau einer handlungsfähigen und effektiven **staatlichen Aufsicht**. Als Grundlage hierfür sind die Datenschutz- und Informationsfreiheitsbehörden geeignet.[923] Deren bisher eingeschränkte gesetzliche Kompetenz (informationelle Selbstbestimmung, teilweise Informationsfreiheit) wie das damit einhergehende Selbstverständnis müssen erweitert werden auf den gesamten Bereich des Schutzes digitaler Grundrechte und der damit verbundenen öffentlichen Belange. Der Schutz vor Diskriminierung und Stigmatisierung, der Schutz von Minderheiten[924] sowie die Verwirklichung digitaler Teilhaberechte (Informationsfreiheit, Meinungsfreiheit, Forschung) sind gemäß einem modernen Verständnis von Datenschutz und Informationsfreiheit integrale Aufgabe, ohne dass sich dies bisher in der Praxis oder in der Normierung durchgesetzt hat. Auch die Funktion einer (gesetzlich zu regulierenden) Algorithmenkontrolle könnte auf unabhängige Datenschutzbehörden übertragen werden (s. o. 11.1.10). Mit der DSGVO wurde ein erster Schritt in Richtung eines allgemeinen digitalen Grundrechtsschutzes gegangen. Um diesen Weg weiterzugehen, bedarf es – zunächst auf nationaler Ebene – weiterer Aufgaben- und Befugniszuweisungen.

---

922 Deutscher Ethikrat S. 178 f.
923 Deutscher Ethikrat S. 183.
924 Deutscher Ethikrat S. 180 f.

Um die Aufgaben einer staatlichen Aufsicht wirksam wahrnehmen zu können, müssen die zuständigen Behörden massiv ausgebaut werden (vgl. Art. 52 Abs. 4 DSGVO). Die bestehenden Vollzugsdefizite im Datenschutzrecht sind insbesondere auf die katastrophale Ausstattung der Aufsichtsbehörden zurückzuführen.[925] Wenn es zutrifft, dass Daten das Öl des 21. Jahrhunderts sind, dass bedarf es einer verbesserten personellen, technischen und finanziellen Ausstattung, um zu verhindern, dass sich einzelne Player in einem Ölrausch verlieren.[926] Orientierungsmaßstab sollte auf längere Sicht die bestehende Finanzverwaltung sein, zumal das finanzielle (steuerrelevante) Gebaren von Unternehmen und Einzelpersonen von ähnlicher Gesellschaftsrelevanz ist wie das digitale Wirtschaften und Leben.[927]

11.3 Anforderungen an Verbände/Kammern

Angesichts der Ungleichzeitigkeit von technischer Entwicklung und politischem Bewusstsein sind nicht nur die Gesetzgeber und die Verwaltung, sondern auch die sonstigen Beteiligten gefordert. Dies gilt insbesondere für die in diesem Bereich professionell fachlich Tätigen.[928] Diese haben über das Instrument von Zertifizierungen (Art. 42 DSGVO) und Verhaltensregeln (Art. 40, 41 DSGVO) die Möglichkeit selbst Normen und Standards zu setzen. Durch die hoheitliche Aufsicht über diese Verfahren und die damit erfolgende regulierte Selbstregulierung kann gewährleistet werden, dass Gemeinwohlbelange adäquat berücksichtigt werden (s. o. 8.22).

Auch unterhalb einer verbindlichen Normierungsebene besteht die Möglichkeit der Entwicklung und Festlegung von Standard Operation Procedures, Best Practices, Verhaltensregeln und freiwilligen Audits.[929] Derartige fachliche Festlegungen können, wenn sie sich inhaltlich als valide erweisen, auf eine höhere Ebene der Verbindlichkeit gehoben werden.

Normierungs- und Standardisierungsmöglichkeiten bestehen über die Festlegung durch nationale oder internationale Normungsgremien, also DIN sowie ISO/IEC. Die Interoperabilität von Daten kann auf dieser Grundlage festgelegt und eingeführt werden. Angesichts der hohen gesellschaftlichen und praktischen Relevanz von Standards sollte erwogen werden, weitere Stakeholder, z. B. Verbraucher, oder staatliche Aufsichtsbehörden, verstärkt in Standardisierungs- und Normungsprozesse mit einzubinden.

---

925 Fischer in Deutscher Ethikrat S. 187; Roßnagel, ZD 2015, 109; Lüdemann/Wenzel, RDV 2015, 287 ff.; Böhm in Kühling/Buchner, Art. 52 Rn. 24; Hamburgischer Beauftragter für Datenschutz und Informationsfreiheit TB 2014/2015, S. 12 f. 268 ff.

926 Konferenz der deutschen Datenschutzbehörden, 25.5.2016, EU-Datenschutz-Grundverordnung erfordert zusätzliche Ressourcen für Datenschutzbehörden; Roßnagel, Aufwand der Datenschutzbehörden, 2017, insbes. S. 144 ff.

927 Schulzki-Haddouti, Datensouveränität wiederherstellen! mmm.verdi.de 27.1.2017.

928 Weichert in Langkafel S. 172 f. = DuD 2014, 838.

929 Thießen S. 429 ff.; Weichert in Langkafel S. 173 = DuD 2014, 838; kritisch Fischer in Deutscher Ethikrat S. 187 f.

Eine bisher im Hinblick auf Big Data ungenutzte Möglichkeit der Regulierung von Big Data besteht über das heilberufliche Standesrecht. Die Heilberufskammern können hier rechtsetzend tätig werden. Dabei ist aber zu berücksichtigen, dass Big Data im Gesundheitsbereich sich oft auf Sachverhalte bezieht, die sich nicht auf einen Heilberuf und damit auf eine Kammerzuständigkeit beschränken lassen. Insofern kommt ein koordiniertes oder gar ein gemeinsames Vorgehen in Betracht.

11.4 Anforderungen an Unternehmen

Unternehmen, die Big Data im Gesundheitsbereich einsetzen, haben gegenüber ihren Beschäftigten, ihren Kunden wie generell gegenüber der Gesellschaft eine hohe Verantwortung. Dieser können sie – jenseits der bzw. in Ergänzung zur Beachtung formellen Rechts – durch ein rationales complianceorientiertes Management entsprechen. Hierzu gehören inhaltliche Zielvorgaben, Ethikstandards, eine entsprechende Unternehmensphilosophie und organisatorische Strukturen, die es dem jeweiligen Unternehmen ermöglichen, ihrer Verantwortung gerecht zu werden (corporate data governance). Vor dem Beschluss von Leitlinien für Wirtschaft und Menschenrechte durch die Vereinten Nationen im Jahr 2011 (s. o. 7.1) gab es, soweit ersichtlich, kein großes Unternehmen, das ein System zur Überwachung von Menschenrechten in der Unternehmenspraxis installiert hatte.[930] Dies kann und soll sich mit diesen Leitlinien ändern. Dafür ist es nötig, eine Kommunikations- und Informationsinfrastruktur, ein Beschwerdemanagement und klare Vorgaben für Forschung, Entwicklung, Erprobung, Einführung und Vertrieb von Produkten zu etablieren. Datenschutzbeauftragte wie auch Betriebsräte können hierbei über ihre gesetzlichen Aufgaben hinaus intern wichtige Funktionen übernehmen.[931]

11.5 Bildungsbedarf und öffentlicher Diskurs

In unserer Informationsgesellschaft muss der Vermittlung von Medienkompetenz noch eine erheblich größere Bedeutung zugewiesen werden. Dies gilt für die Vermittlung der informationstechnischen Kompetenz wie auch des Verständnisses für die damit verbundenen sozialen Prozesse. Die pädagogische Aufgabe beginnt spätestens in der Grundschule und endet nicht bei der beruflichen Aus- und Weiterbildung. Insbesondere der Vermittlung von Allgemeinbildung muss durch neue Angebote, Lehr- und Lerninhalte mehr Augenmerk gewidmet werden, um den öffentlichen demokratischen Diskurs über die Digitalisierung der Gesellschaft und das Verständnis hierzu zu stärken.[932]

Zu Big Data wird inzwischen weltweit wie auch in Europa und in Deutschland umfangreich geforscht. Erlangte Erkenntnisse finden aber oft nicht adäquat Eingang in die Praxis. Hierfür bedarf es wohl nicht eines allgemeinen Kompetenzzentrums für Big Data.[933] Wohl aber kann und sollte es eine öffentliche Aufgabe sein, die vorhandenen Erkenntnisse in

930 Willmroth, Botschafter des Wandels, SZ 4.1.2018, 17.
931 Deutscher Ethikrat S. 183.
932 Deutscher Ethikrat S. 179.
933 So Zimmermann-Rittereiser/Schaper in Langkafel S. 158.

spezifischen Bereichen über Anwendungen sowie damit gesammelten Erfahrungen öffentlich aufzuarbeiten, zu verbreiten bzw. über Open Data (s. o. 10.10, 11.1.10) bereitzustellen und hierüber den gesellschaftlichen Diskurs voranzubringen.[934] Ergebnisse sollten zeitnah in politische Entscheidungen, insbesondere in gesetzliche und infrastrukturelle Maßnahmen münden. Für eine Organisation dieses Diskurses kann angesichts der vielen Beteiligten und der vielfältigen oft gegenläufigen Interessen spezifisch für den Gesundheitssektor die Zuweisung bzw. die Einrichtung eines im öffentlichen Interesse handelnden Kompetenzzentrums sinnvoll sein.

Die Gefahr, dass aus kommerziellem Interesse gesundheitsrelevante Informationen verbreitet und genutzt werden, die keine positive oder gar eine schädliche Wirkung haben, ist groß. Daher sind die bestehenden Bestrebungen zu verstärken, den Menschen wie auch den im Gesundheitsbereich tätigen Einrichtungen und Stellen zu helfen, verlässliche Quellen für Gesundheitsinformationen zu finden. Dabei geht es nicht nur um die Verhinderung gezielter Falschinformationen (sog. Fake-News), sondern auch um die Verifizierung umstrittener Thesen oder Forschungsergebnisse. Durch eine Bündelung solcher Aktivitäten soll nicht die gesundheitsrelevante Meinungsbildung eingeschränkt werden, sondern es sollte eine fachkundige und durch die Unabhängigkeit vertrauenswürdige Instanz etabliert werden, die als Wegweiser im Dschungel der Gesundheitsinformationen wirkt. Vorbilder hierfür könnten die im Patient Protection und Affordable Care Act (2019), dem sog. Obamacare, vorgesehenen oder die in Deutschland von der AOK unter aok.de/faktenboxen angebotenen Informationsangebote sein.[935]

11.6 Forschungsbedarf

Die Qualitätsevidenz digitaler Maßnahmen zur Verbesserung des Gesundheitswesens wird zwar in allen Bereichen behauptet, muss aber in vielen Fällen hinterfragt und sollte mit empirischen Studien untersucht und bewiesen werden. Big Data nutzt in der Regel wissenschaftliche Methoden. Die hieraus abgeleiteten Schlussfolgerungen sind aber oft wissenschaftlich (noch) nicht (hinreichend) belegt. Nur durch regelmäßige Evaluation kann angesichts der sozialen wie der wissenschaftlichen und technischen Dynamik nachhaltig Qualität gesichert werden.

Dabei sind differenzierte Forschungsansätze zu verfolgen: Was für viele Menschen (gesundheits-) förderlich ist, kann bei anderen das genaue Gegenteil bewirken. Die Untersuchungen dürfen sich nicht auf den direkten Nutzen spezifischer Maßnahmen beschränken. Erfasst und berücksichtigt werden müssen auch die sozialen und freiheitlichen Fernwirkungen der Maßnahmen auf das Solidarsystem, die gesundheitliche

934 Strategy/pwc S. 178 ff.

935 Rebitschek/Gigerenzer/Wagner, Kritische Voraussetzungen für ein digitales Gesundheitswesen in Deutschland, ZBW Leibnitz-Informationszentrum Wirtschaft, Wirtschaftsdienst 2017 (10), 701.

und informationelle Selbstbestimmung und die ökonomischen Konsequenzen (s. o. 10.8.4).[936]

Forschungsbedarf besteht in Bezug auf Anonymisierung und Pseudonymisierung. Bei Big Data im Gesundheitsbereich wird regelmäßig Anonymität als Rechtmäßigkeitsvoraussetzung für die Verarbeitung behauptet und angenommen, obwohl allenfalls eine Pseudonymisierung vorliegt. Die technischen Möglichkeiten zur Anonymisierung sind weiterzuentwickeln und Pseudonymisierungsmodelle sind zu entwerfen und zu etablieren (s. o. 8.12.1., 8.12.2).

Es besteht große Verunsicherung bzgl. der Frage, wie bei langfristig angelegten und komplexen Datenverarbeitungsprozessen die Selbstbestimmung der Betroffenen optimiert werden kann. Hierzu müssen Angebote zur Sicherung der Transparenz und der Eingriffs- und Wahlmöglichkeit, etwa durch technische Einwilligungshilfen, entwickelt und etabliert werden. Entsprechende Forschungsprojekte bedürfen der praktischen Erprobung, um die Erfassungs- und Handlungsfähigkeit und -bereitschaft von Betroffenen zu erkunden und die Maßnahmen hieran auszurichten (s. o. 8.8.2)

936 Rebitschek/Gigerenzer/Wagner, Kritische Voraussetzungen für ein digitales Gesundheitswesen in Deutschland, ZBW Leibnitz-Informationszentrum Wirtschaft, Wirtschaftsdienst 2017 (10), 703.

Literatur

Albrecht, Jan Philipp/Jotzo, Florian, Das neue Datenschutzrecht der EU, 2017.

Auernhammer, Hrsg. von Eßer, Martin/Kramer, Philipp/von Lewinski, Kai, DSGVO, BDSG – Kommentar, 5. Aufl. 2017.

Bergmann, Lutz (früherer Autor u. Hrsg.)/Möhrle, Roland/Herb, Armin, Datenschutzrecht – Kommentar, Loseblatt Stand September 2016.

Buchner, Benedikt (Hrsg.), Datenschutz im Gesundheitswesen, Loseblatt Stand 7/2017.

Bundesministerium für Verkehr und digitale Infrastruktur (BMVI, Hrsg.), „Eigentumsordnung" für Mobilitätsdaten? – Eine Studie aus technischer, ökonomischer und rechtlicher Perspektive, verfasst durch Partnerschaft Deutschland/ Lorenz-von-Stein-Institut für Verwaltungswissenschaften an der Christian-Albrechts-Universität zu Kiel/Universität Kassel/Fraunhofer FOKUS, 2.8.2017, https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/eigentumsordnung-mobilitaetsdaten.pdf?__blob=publicationFile

Callies, Christian/Ruffert, Matthias, EUV/AEUV – Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta, 5. Aufl. 2016.

Däubler, Wolfgang, Gläserne Belegschaften? 7. Aufl. 2017.

Däubler, Wolfgang/Klebe, Thomas/Wedde, Peter/Weichert, Thilo (Däubler u. a.), Bundesdatenschutzgesetz – Kompaktkommentar, 5. Aufl. 2016.

Deutscher Ethikrat, Big Data und Gesundheit – Datensouveränität als informationelle Freiheitsgestaltung, Stellungnahme, 30.11.2017; http://www.ethikrat.org/dateien/pdf/stellungnahme-big-data-und-gesundheit.pdf.

Deutscher Verkehrsgerichtstag, 52. Deutscher Verkehrsgerichtstag (52. VGT 2014), 2014.

Ehmann, Eugen/Selmayr, Martin (Hrsg.), Datenschutz-Grundverordnung, 2017.

Fraunhofer-Zentrum für Internationales Management und Wissensökonomie (IMW)/Gesundheitsforen Leipzig/ Universität Leipzig, Big Data im Krankenversicherungsmarkt, 2016.

Gola, Peter/Schomerus, Rudolf (Hrsg. bis 9. Aufl.), bearbeitet von Gola, Peter/Klug, Christoph, Körffer, Barbara, BDSG – Bundesdatenschutzgesetz, Kommentar, 12. Aufl. 2015.

Gola, Peter (Hrsg.), DS-GVO Datenschutz-Grundverordnung VO (EU) 2016/679, 2017.

Härting, Niko, Datenschutz-Grundverordnung, 2016.

Hauser, Andrea/Haag, Ina, Datenschutz im Krankenhaus, 4. Aufl. 2012.

Hoffmann, Christian/Luch, Anika D./ Schulz, Sönke E./ Borchers, Kim Corinna (Hoffmann u. a.), Die digitale Dimension der Grundrechte, 2015.

Kingreen, Thorsten/Kühling, Jürgen (Hrsg.), Gesundheitsdatenschutzrecht, 2015.

Kühling, Jürgen/Buchner, Benedikt (Hrsg.), Datenschutz-Grundverordnung, Kommentar, 2017.

Langkafel, Peter (Hrsg.), Big Data in Medizin und Gesundheitswirtschaft, 2014.

Meyer, Jürgen (Hrsg.), Charta der Grundrechte der Europäischen Union, 4. Aufl. 2014.

Münch, Florian, Autonome Systeme im Krankenhaus, 2017.

Paal, Boris P./Pauly, Daniel A. (Hrsg.), Datenschutz-Grundverordnung, Kompakt-Kommentar, 2017.

Plath, Kai-Uwe (Hrsg.), BDSG DSGVO Kommentar, 2. Aufl. 2016.

Pommerening, Klaus/Drepper, Johannes/Helbing, Krister/Ganslandt, Thomas, Leitfaden zum Datenschutz in medizinischen Forschungsprojekten, Generische Lösungen der TMF 2.0, September 2014.

Prütting, Dorothea (Hrsg.), Fachanwaltskommentar Medizinrecht, 3. Aufl. 2014.

Rat für InformationsInfrastrukturen (RfII), Datenschutz und Forschungsdaten, Diskussionspapier für den RfII-Workshop am 27. Oktober 2016.

Rat für InformationsInfrastrukturen (RfII), Datenschutz und Forschungsdaten, Aktuelle Empfehlungen, März 2017, http://www.rfii.de/?wpdmdl=2249.

Reiffenstein, Maria/Blaschek, Beate (Hrsg.), Konsumentenpolitisches Jahrbuch 2017, 2017.

Roßnagel, Alexander (Hrsg.), Handbuch Datenschutzrecht, 2003.

Schantz, Peter/Wolff, Heinrich/Amadeus, Das neue Datenschutzrecht, 2017.

Schmidt, Jan-Hinrik/Weichert, Thilo (Hrsg.), Datenschutz – Grundlagen, Entwicklungen und Kontroversen, 2012.

Schneider, Uwe K., Sekundärnutzung klinischer Daten – Rechtliche Rahmenbedingungen, 2015.

Schwarze, Jürgen (Hrsg.), EU-Kommentar, 3. Aufl. 2012.

Simitis, Spiros (Hrsg.), Bundesdatenschutzgesetz, 8. Aufl. 2014.

Stiftung Datenschutz (Hrsg.), Zukunft der informationelle Selbstbestimmung, 2016.

Stiftung Datenschutz (Hrsg.), Big Data und E-Health, 2017.

Strategy/PricewaterhouseCoopers (pwc), Weiterentwicklung der eHealth-Strategie, Studie im Auftrag des Bundesministeriums für Gesundheit, 2016, https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/E/eHealth/BMG-Weiterentwicklung_der_eHealth-Strategie-Abschlussfassung.pdf.

Theißen, Sascha, Risiken informations- und kommunikationstechnischer (IKT-) Implantate im Hinblick auf Datenschutz und Datensicherheit, 2009.

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), Scoringsysteme zur Beurteilung der Kreditwürdigkeit – Chancen und Risiken für Verbraucher, 2005, https://www.datenschutzzentrum.de/uploads/projekte/scoring/2005-studie-scoringsysteme-uld-bmvel.pdf.

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), Datentreuhänderschaft in der Biobank-Forschung, Schlussbericht, 2009, https://www.datenschutzzentrum.de/biobank/20090630-datentreuhaender-biobankenforschung-endbericht.pdf.

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), Juristische Fragen im Bereich Altersgerechter Assistenzsysteme, 2010, https://www.datenschutzzentrum.de/uploads/projekte/aal/2011-ULD-JuristischeFragenAltersgerechteAssistenzsysteme.pdf.

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), Datenschutz-Auskunftsportal – Datenschutzrechtliche Aspekte, 2013, https://www.datenschutzzentrum.de/uploads/projekte/auskunftsportal/DatenschutzAuskunftsportal.pdf.

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)/GP Forschungsgruppe, Scoring nach der Datenschutz-Novelle 2009 und neue Entwicklungen, 2014, https://www.bmjv.de/SharedDocs/Downloads/DE/PDF/Scoring-Studie.pdf?__blob=publicationFile&v=3.

Wolff, Heinrich Amadeus/Brink, Stefan (Hrsg.), Datenschutzrecht in Bund und Ländern, Kommentar, 2013.

Abkürzungen

a. A.	andere Ansicht
AAL	Ambient Assisted Living
ABIDA	Assessing Big Data (Projekt)
ABl.	Amtsblatt
Abs.	Absatz
AEMR	Allgemeine Erklärung der Menschenrechte
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AfP	Archiv für Presserecht (Zeitschrift)
AG	Aktiengesellschaft
AGG	Allgemeines Gleichbehandlungsgesetz
AMG	Arzneimittelgesetz
AOK	Allgemeine Ortskrankenkasse
App	Applikation, Anwendung
Art.	Artikel
Aufl.	Auflage
AuR	Arbeit und Recht (Zeitschrift)
ASiG	Arbeitssicherheitsgesetz
BayLDA	Bayerisches Landesamt für Datenschutzaufsicht
BB	Betriebsberater (Zeitschrift)
BBG	Bundesbeamtengesetz
BDSGaF/nF	Bundesdatenschutzgesetz alte Fassung/neue Fassung
Bek.	Bekanntmachung
BfArM	Bundesinstitut für Arzneimittel und Medizinprodukte
BfDI	Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
BFH	Bundesfinanzhof
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BMBF	Bundesministerium für Bildung und Forschung
BMVI	Bundesministerium für Verkehr und Infrastruktur
BR-Drs.	Bundesrats-Drucksache
BSG	Bundessozialgericht
BSI-G	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
bspw.	beispielsweise
BStatG	Bundesstatistikgesetz
BT-Drs.	Bundestags-Drucksache
BVerfG/E	Bundesverfassungsgericht/Entscheidungssammlung
BVerwG	Bundesverwaltungsgericht
bzw.	beziehungsweise
ca.	circa
Chr.	Christus
CR	Computer und Recht (Zeitschrift)
CRM	Customer Relation Management
DB	Der Betrieb (Zeitschrift)
DANA	DatenschutzNachrichten (Zeitschrift)
ders.	derselbe
d. h.	das heißt

dGRCh-E	Entwurf einer digitalen Grundrechte-Charta
DIVSI	Deutsches Institut für Vertrauen und Sicherheit im Internet
DNA	(auch DNS) Desoxyribonukleinsäure
DÖV	Die Öffentliche Verwaltung (Zeitschrift)
DRG	Disease Related Groups
DSB	Datenschutzberater (Zeitschrift) od. Datenschutzbeauftragte
DSGVO	Europäische Datenschutz-Grundverordnung
DSRI-JI	Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr
DuD	Datenschutz und Datensicherheit (Zeitschrift)
DVBl	Deutsches Verwaltungsblatt
EG	Europäische Gemeinschaften
EG-DSRI	Europäische Datenschutzrichtlinie
EGMR	Europäischer Gerichtshof für Menschenrechte
EMA	Europäische Arzneimittel-Agentur / European Medicines Agency
EMRK	Europäische Menschenrechtskonvention
EPA	elektronische Patientenakte
ERP	Enterprise Ressource Planing
ErwGr	Erwägungsgrund
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EuGRZ	Europäische Grundrechtezeitschrift
f/f.	fort-/folgende
Fa.	Firma
FDA	Food&Drug Administration (US-Behörde)
Fn.	Fußnote
G.	Gesetz
G-BA	Gemeinsamer Bundesausschuss
GBl.	Gesetzesblatt
Gematik	Gesellschaft für Telematikanwendungen der Gesundheitskarte
GenDG	Gendiagnostikgesetz
GesR	Gesundheitsrecht (Zeitschrift)
GG	Grundgesetz
GKV	Gesetzliche Krankenversicherung
GRCh/GRC	Europäische Grundrechte-Charta
grds.	grundsätzlich
GRUR	Zeitschrift für Gewerblichen Rechtsschutz und Urheberrecht
GVBl.	Gesetz- und Verordnungsblatt
Hrsg.	Herausgeber
ICD	International Code of Diseases
i. d. R.	in der Regel
IMW	Zentrum für Internationales Management und Wissensökonomie/Gesundheitsforen
insbes.	insbesondere

i. V. m.	in Verbindung mit
IT	Informationstechnik od. informationstechnisch
JZ	Juristenzeitung
Kap.	Kapitel
Kcal	Kilokalorien
KG	Kammergericht
KI	Künstliche Intelligenz
K&R	Kommunikation und Recht (Zeitschrift)
KSchG	Kündigungsschutzgesetz
LDI NRW	Landesbeauftragte für den Datenschutz Nordrhein-Westfalen
LDSG SH	Landesdatenschutzgesetz Schleswig-Holstein
LfD Nds.	Landesbeauftragte/r für Datenschutz Niedersachsen
LG	Landgericht
lit.	Buchstabe
LS	Leitsatz
MBOÄ	Musterberufsordnung für die deutschen Ärztinnen und Ärzte
MedR	Medizinrecht (Zeitschrift)
Min.	Minute
Mio.	Millionen
MMR	Multimedia und Recht (Zeitschrift)
MPG	Medizinproduktegesetz
Mrd.	Milliarden
MVVerfG	Verfassungsgericht von Mecklenburg-Vorpommern
m. w. N.	mit weiteren Nachweisen
NDR	Norddeutscher Rundfunk
NJW	Neue Juristische Wochenschrift
NVwZ	Neu Zeitschrift für Verwaltungsrecht
NZA	Neue Zeitschrift für Arbeitsrecht
OLG	Oberlandesgericht
OVG	Oberverwaltungsgericht
PatG	Patentgesetz
PinG	Privacy in Germany (Zeitschrift)
PKV	Private Krankenversicherung
pwc	PricewaterhouseCoopers (Unternehmen)
RDV	Recht der Datenverarbeitung (Zeitschrift)
RFID	Radio Frequency Identification Device
RfII	Rat für Informationsinfrastrukturen
RL	Richtlinie
Rn.	Randnummer
S.	Seite od. Satz
SächsVerfGH	Verfassungsgerichtshof des Freistaates Sachsen
SGB	Sozialgesetzbuch
SchHA	Schleswig-Holstein Anzeigen (Zeitschrift)
SignaturG	Signaturgesetz
sog.	so genannt/e/r
s. u.	siehe unten
s. o.	siehe oben
StV	Strafverteidiger (Zeitschrift)
SZ	Süddeutsche Zeitung

TB	Tätigkeitsbericht
TI	Telematik-Infrastruktur
TKG	Telekommunikationsgesetz
TMF	Technologie- und Medienplattform für die vernetzte medizinische Forschung
TMG	Telemediengesetz
TPG	Transplantationsgesetz
u.	und
u. a.	unter anderem
UAC	Use and Access Committee
u. Ä.	und Ähnliches
UKlaG	Unterlassungsklagegesetz
ULD	Unabhängiges Landeszentrum für Datenschutz
UNESCO	United Nations Educational, Scientific and Cultural Organization, Organisation der Vereinten Nationen für Erziehung, Wissenschaft und Kultur
UN/O	United Nations/Organization
UrhG	Urhebergesetz
USA	United States of America, Vereinigte Staaten von Amerika
usw.	und so weiter
v.	vor od. von
vgl.	vergleiche
VuR	Verbraucher und Recht (Zeitschrift)
vzbv	Verbraucherzentrale Bundesverband
WHO	World Health Organization, Weltgesundheitsorganisation
WP	Working Paper
z. B.	zum Beispiel
ZD	Zeitschrift für Datenschutz
zit.	zitiert