Deutscher Ethikrat

Big Data und Gesundheit – Datensouveränität als informationelle Freiheitsgestaltung

STELLUNGNAHME · KURZFASSUNG

30. November 2017

Der vollständige Text der Stellungnahme sowie alle öffentlich verfügbaren begleitenden Informationen und Dokumentationen des Deutschen Ethikrates zum Thema Big Data und Gesundheit sind unter http://www.ethikrat.org/themen/forschung-und-technik/big-data abrufbar.

Herausgegeben vom Deutschen Ethikrat

Jägerstraße 22/23 · D-10117 Berlin
Telefon: +49/30/20370-242 · Telefax: +49/30/20370-252
E-Mail: kontakt@ethikrat.org
www.ethikrat.org

Layout: Torsten Kulick

>> INHALT

>> ZUSAMMENFASSUNG

Grundlagen: Big Data und Gesundheit

1) Big Data gehört zu den Schlüsselbegriffen der gegenwärtigen Debatte über die technologisch induzierte gesellschaftliche Veränderung. Das Stichwort beschreibt einen Umgang mit großen Datenmengen, der darauf abzielt, Muster zu erkennen und daraus neue Einsichten zu gewinnen. Dazu sind angesichts der Fülle und Vielfalt der Daten sowie der Geschwindigkeit, mit der sie erfasst, analysiert und neu verknüpft werden, innovative, kontinuierlich weiterentwickelte informationstechnologische Ansätze notwendig.

2) Die systematische Erhebung und Auswertung von Daten ist spätestens seit Beginn der Neuzeit ein bedeutender Faktor zivilisatorischer Entwicklung und schließt auch den Menschen und seine Lebensumgebung ein, zum Beispiel in der Biologie und Medizin, der Psychometrie, der Epidemiologie und den Sozialwissenschaften. Der Einsatz von modernen Computern, Speichertechnologien und schnellen

Netzwerken erlaubt eine enorme Steigerung des handhabbaren Datenvolumens, aber auch vielfältige qualitative Verbesserungen, wie die Verwendung komplexerer Rechenvorschriften (Algorithmen) in rechenintensiven Computersimulationen und eine Rationalisierung, Standardisierung und Qualitätssteigerung vieler Arbeitsprozesse.

3) Mit der Entwicklung zu Big Data geht eine Transformation aller Phasen der Datenverarbeitung einher, die von zunehmender Automatisierung, Vernetzung und Durchdringung geprägt ist. Volumen und Tempo der voll automatisierten Datenerfassung sind in wenigen Jahren exponentiell gestiegen, und die rasche Verbreitung und Vernetzung von Geräten, die in allen Sphären der menschlichen Lebenswelt zur Datenerhebung genutzt werden können, eröffnet ständig neue Datenquellen.

4) Dies zeigt sich besonders anschaulich im Gesundheitsbereich. Dort nutzen immer mehr Forscher[1], Firmen und Ärzte Informationen, die aus der Verarbeitung riesiger Datenmengen entstanden sind. Zudem nimmt die individuelle Erfassung gesundheitsrelevanter Daten zu, zum Beispiel über die Apps von Mobiltelefonen und am Körper getragene Sensoren. Wenn solch vielfältige Daten verknüpft und analysiert werden, ermöglicht dies tiefe Einblicke in den aktuellen Gesundheitszustand, die Persönlichkeit sowie den Lebenswandel und erlaubt teilweise sogar Vorhersagen, etwa zur Krankheitsentwicklung.

5) Sind Daten einmal erhoben, sorgen Datennetzwerke und vernetzte Softwaresysteme mitunter in Echtzeit für ihren Austausch und ihre Verknüpfung, oft auch über Staatsgrenzen hinweg. Hierfür werden technische Standards für den Datenaustausch über Schnittstellen zur Anwendungsprogrammierung entwickelt, die auch die Festlegung

1 Aus Gründen der besseren Lesbarkeit wird auf eine geschlechterspezifische Differenzierung verzichtet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung für alle Geschlechter.

bestimmter Nutzungsregeln und die Nachverfolgung von Daten erleichtern.

6) Die effiziente Erfassung, Speicherung und Verarbeitung von Daten benötigt eine leistungsfähige Rechenmaschinerie. Sie wird meist in Datenzentren mit vielen vernetzten Servern bereitgestellt und vielfach von kommerziellen Anbietern offeriert. Die Verlagerung von lokalen Rechnern in die Virtualität solcher Datenzentren wird als Cloud-Computing bezeichnet.

7) Wesentlich für die Beurteilung von datenbasierten Aussagen, Schlussfolgerungen oder Vorhersagen sind die Objektivität, Reliabilität, Reproduzierbarkeit und Validität der verwendeten Daten bzw. Analyseverfahren. Mit der Menge der Daten steigen die Aussagekraft der Analyse für einzelne untersuchte Faktoren und die Möglichkeiten, zusätzliche, auch schwach wirkende Faktoren und ihre Interaktionen zu berücksichtigen. Die unabhängige Überprüfung und Verifizierung von Datenanalysen bleibt gleichwohl von zentraler Bedeutung.

8) Aus statistischen Zusammenhängen zwischen Variablen (Korrelationen) kann nicht ohne Weiteres auf Ursachen (kausale Effekte) oder Wirkmechanismen geschlossen werden. Letztere gilt es mittels zusätzlicher Argumente und Annahmen oder mittels Gewinnung zusätzlicher Daten, zum Beispiel aus Langzeit- oder experimentellen Studien, zu klären.

9) Besondere Bedeutung für den Einsatz und die weitere Entwicklung von Big-Data-Anwendungen hat das maschinelle Lernen. Hier „erlernen“ statistische Modelle anhand von Trainingsdatensätzen Berechnungsvorschriften, mit denen Daten in bestimmter Weise klassifiziert oder kategorisiert werden können. Eine zentrale Frage dabei ist, in welchem Umfang solche Techniken zur Entwicklung von entscheidungsfähigen und -befugten maschinellen Agenten führen, die beispielsweise auch an der Therapiegestaltung oder

gesundheitspolitischen Entscheidungsprozessen beteiligt werden könnten.

10) Selbstlernende Systeme können anhand von Daten einer großen Gruppe von Menschen maßgebliche Faktoren, wie etwa gesundheitsrelevante Verhaltensweisen, ermitteln und einzelne Personen und Inhalte in diesem Koordinatensystem verorten. Solche Ansätze erlauben schnelle individualisierte Empfehlungen und Interaktionen mit maschinellen Assistenten. Sie gehen allerdings notgedrungen mit der Preisgabe persönlicher Informationen einher und erleichtern gegebenenfalls Täuschungen und die Manipulation persönlicher Entscheidungen.

11) Big-Data-gestützte Verfahren erkennen bei der Analyse von Zusammenhängen immer feinere Unterschiede zwischen Personen, wodurch eine stärkere Berücksichtigung höchstpersönlicher Eigenschaften und Umstände möglich wird – etwa in der Diagnostik, Prognose und Therapie oder im Versicherungswesen hinsichtlich der Einstufung in Prämiengruppen. Bei der Bildung solcher Gruppen (Stratifizierung) durch komplexe Big-Data-Algorithmen ist es allerdings wichtig, mögliche Fehlerquellen zu berücksichtigen und zu minimieren.

12) Gesundheitsbezogene Daten, die einer bestimmten Person zugeordnet werden können, sind besonders sensibel, weil sie tiefe Einblicke in einen sehr intimen Bereich ermöglichen. Personenbezogene Daten können aus einer immer größeren Zahl von Quellen gesammelt und miteinander verknüpft werden, wobei im Verlauf des Auswertungsprozesses auch solche Daten Gesundheitsrelevanz erlangen können, die einen entsprechenden Anschein zunächst nicht erwecken, zum Beispiel Bewegungsdaten oder Einkaufsdaten.

13) Gesundheitsrelevante Daten fallen in verschiedenen, einander teilweise überschneidenden Kontexten an, von der medizinischen Praxis

und gesundheitsbezogenen Forschung über Behörden und Versicherer bis hin zur aktiven oder unbeabsichtigten Datengenerierung durch Bürger bzw. Patienten. Big-Data-Technologien ermöglichen darüber hinaus eine umfassende Dekontextualisierung und Rekontextualisierung von Daten, die zu unterschiedlichen Zwecken erfasst, analysiert und neu verknüpft werden. Dies führt zu einer Entgrenzung des gesundheitsrelevanten Bereichs. Zudem erleichtert es die Deanonymisierung von Daten bzw. die Reidentifizierung einzelner Personen.

14) Weil alle Daten, die in irgendeiner Form erhoben werden, in Relation zur persönlichen Gesundheit interpretiert werden *können*, ist es prinzipiell möglich, all diese Daten auch als gesundheitsrelevant einzuschätzen. Ob bestimmte Daten als sensibel oder gesundheitsrelevant zu betrachten sind, lässt sich angesichts dieser Entwicklungen somit oft nicht mehr zum Zeitpunkt ihrer Erhebung bestimmen, sondern hängt in erster Linie vom Kontext ab, in dem sie verwendet werden. Dieser Kontext kann sich im Laufe der Zeit ändern.

15) An der Erhebung, Verarbeitung und Nutzung großer Datenmengen sind verschiedene Akteure mit unterschiedlichen Funktionen und zumindest teilweise gegenläufigen Interessen in vielfältigen Handlungskontexten beteiligt. Dabei lassen sich fünf ausgewählte Anwendungsbereiche von Big Data exemplarisch auf ihre jeweiligen Chancen und Risiken untersuchen: erstens die biomedizinische Forschung, zweitens die Gesundheitsversorgung, drittens Datennutzung durch Versicherer und Arbeitgeber, viertens die kommerzielle Verwertung gesundheitsrelevanter Daten durch global agierende IT- und Internetfirmen und fünftens ihre Erhebung durch Betroffene selbst.

16) In der biomedizinischen Forschung (Anwendungsbereich 1) soll die Auswertung großer Mengen gesundheitsrelevanter Daten zu einem besseren Verständnis wissenschaftlich relevanter Zusammenhänge und Prozesse führen. Zu den datenintensivsten Anwendungen gehören moderne bildgebende und molekularbiologische Verfahren, wie

sie etwa in der Neurowissenschaft und den sogenannten Omik-Disziplinen (zum Beispiel Genomik, Proteomik, Metabolomik) eingesetzt werden.

17) Zentrale Akteure im wissenschaftlichen Bereich sind Forschungsinstitutionen und deren Mitarbeiter, aber auch Probanden und Patienten. Die Arbeit mit großen Datenmengen erfolgt in der Forschung in der Regel nach hohen und gut kontrollierbaren Standards der Datenerhebung, -verwendung und -sicherheit und häufig institutionenübergreifend. Wissenschaftsorganisationen machen sich die neuen technischen und infrastrukturellen Möglichkeiten von Big Data zunutze und vernetzen sich zum Zweck des Datenaustauschs und der gemeinsamen Analyse und Auswertung.

18) Bei vielen Erkrankungen sind die krankheitsbedingenden und -modulierenden Zusammenhänge sehr komplex. Big Data eröffnet Chancen, verschiedene Informationen integrativ in umfangreichen und quellenübergreifenden Analysen zusammenzufassen. Für diese Integrationsleistung ist neben der bloßen Menge der einbezogenen Daten auch die Qualität ihrer interpretatorischen Aufbereitung von entscheidender Bedeutung.

19) Die Zusammenführung von Daten, die von mehreren Institutionen in oft unterschiedlichen Kontexten erhoben werden, bringt besondere Herausforderungen für den Einsatz von Big Data in der medizinischen Forschung mit sich. Vielfach fehlen einheitliche Standards zur Erfassung, Annotation und Qualitätssicherung von Daten ebenso wie gut funktionierende Regeln für den Datenaustausch. Das liegt zum einen an Datenschutzbedenken und einem Mangel an geeigneten Kontaktaufnahmemöglichkeiten und Einwilligungsmodellen für Patienten und Probanden zur Sekundärnutzung von Daten. Zum anderen gibt es Unsicherheiten und unterschiedliche Vorstellungen darüber, wer in welchem Ausmaß das Recht hat, über die generierten Daten zu verfügen.

20) Lösungsansätze bieten neben neuen Einwilligungsmodellen vor allem technische Maßnahmen für einen standardisierten Datenaustausch, der sowohl Datenqualität als auch hohe Schutzstandards garantiert, aber auch unterstützende regulatorische und Fördermaßnahmen sowie Initiativen für einen offenen Datenaustausch.

21) In der Gesundheitsversorgung (Anwendungsbereich 2) eröffnet der Einsatz von Big Data Chancen auf stärker personalisierte Behandlungskonzepte sowie Effektivitäts- und Effizienzsteigerungen. Der Rückgriff auf große Datenmengen ermöglicht eine bessere Stratifizierung von Patienten, sodass zum Beispiel Nebenwirkungen reduziert werden und unnötige Therapieversuche unterbleiben können. Die Sammlung und Auswertung gesundheitsbezogener Daten erschließt zudem neue Potenziale bei der Früherkennung und Prävention von Erkrankungen.

22) Der Gesundheitssektor wird von einer Vielzahl von Akteuren mit teilweise divergierenden Interessen geprägt. Dazu gehören die Erbringer, Kostenträger und Empfänger von Gesundheitsleistungen, aber auch Behörden, Interessenverbände und Forscher mit einem unmittelbaren Bezug zur klinischen Praxis.

23) Den Chancen datenintensiver Ansätze stehen Risiken für Patienten gegenüber, etwa Kontrollverluste über die eigenen Daten, der immer weitergehend eröffnete Zugriff auf intime Informationen durch Leistungsanbieter („gläserner Patient“) sowie erleichterter Datenmissbrauch. Hinzu kommen Sorgen, dass eine verstärkte Nutzung Big-Data-gestützter Ansätze die persönliche Zuwendung zum Patienten weiter reduzieren und ihr unkritischer oder unsachgemäßer Einsatz zu Diagnose- und Behandlungsfehlern führen könnte.

24) Für Versicherer und Arbeitgeber (Anwendungsbereich 3) eröffnet Big Data umfangreiche neue Zugriffs- und Auswertungsmöglichkeiten, die von den geltenden rechtlichen Bestimmungen nicht

durchgehend erfasst werden. Immer umfangreichere Datenmengen und -verknüpfungsoptionen ermöglichen zunehmend feinkörnige Profile einzelner Personen oder Personengruppen.

25) Damit verbunden ist eine Sorge vor Diskriminierung, etwa mit Blick auf Szenarien, in denen Versicherer und Arbeitgeber mithilfe der Analyse kommerziell verfügbarer, Big-Data-generierter persönlicher Verhaltensprofile gezielt risikoarme Antragsteller bzw. Bewerber auswählen oder diesen bessere Konditionen anbieten.

26) Auch innerhalb bestehender Verträge haben Arbeitgeber und Krankenversicherungen ein Interesse an der Gesundheit ihrer Vertragspartner, da im Krankheitsfall hohe Kosten entstehen können. Die Überwachung des Patienten- bzw. Arbeitnehmerverhaltens lässt Anreize für eine gesunde bzw. Sanktionen auf eine ungesunde Lebensführung zu. Wo es mit solchen Programmen gelingt, Krankenstände zu reduzieren, eröffnet dies für alle Beteiligten Chancen. Die Risiken dürfen gleichwohl nicht ignoriert werden. Prämienanpassungen oder Abmahnungen wegen gesundheitsschädlichen Verhaltens beispielsweise liegen nicht im Interesse der jeweiligen Datengeber.

27) Global agierende IT- und Internetfirmen (Anwendungsbereich 4) treten in erster Linie als Dienstleister auf. Auf der Grundlage ihres Zugangs zu riesigen Datenmengen und der geeigneten Dateninfrastruktur stellen sie Suchmaschinen, interaktive Informationsplattformen und Angebote wie Online-Shopping, aber auch eine breite Auswahl an multifunktionalen Geräten bereit. Dabei werden unterschiedliche Nutzerdaten in großem Stil gesammelt, gespeichert und verwertet. Solchen Unternehmen, die zunehmend auch in gesundheitsrelevanten Bereichen agieren, ist es daher in besonderer Weise möglich, primär gesundheitsrelevante Daten mit zahlreichen anderen Informationen in Verbindung zu setzen. Hier besteht ein großes Missbrauchspotenzial.

28) Unternehmen bieten Software, Hardware, Technologieentwicklung und Online-Dienste für Big-Data-Anwendungen an. Sie stellen datenorientierten Institutionen Systeme, Algorithmen, Geräte und Infrastruktur zur Datenerhebung, Auswertung, Verwaltung und Speicherung zur Verfügung, mit denen Prozesse beschleunigt und verbessert werden sollen, um eine hocheffiziente Nutzung jeweils relevanter Informationen zu gewährleisten.

29) Die zunehmenden Aktivitäten digitaler Firmen im Gesundheitsbereich bieten Chancen für Forschung und Medizin, da große Internetkonzerne im Vergleich zum öffentlichen Sektor Zugriff auf wesentlich größere Datenmengen haben und oft mit leistungsfähigeren Analysemöglichkeiten sowie besseren technischen und finanziellen Ressourcen ausgestattet sind. Auf der anderen Seite stellen Einschränkungen beim Datenzugang für Datengeber und Nutzungsinteressenten aus Medizin und Forschung jedoch mitunter auch Hindernisse für den medizinischen Fortschritt dar.

30) Für die Erhebung gesundheitsrelevanter Daten durch Betroffene selbst (Anwendungsbereich 5) stehen viele tragbare Geräte mit Sensoren und Apps zur Verfügung, mit denen immer mehr individuelle Gesundheitsdaten sowie tägliche Aktivitäts- und Umweltdaten erfasst, aufbereitet und mit vorhandenen Datenbeständen verknüpft werden können. Die Digitalisierung der Lebenswelt ist zudem so weit fortgeschritten, dass alltägliche Verhaltensweisen und Kommunikationsformen häufig auch jenseits sozialer Netzwerke, Lifestyle-Apps und Ähnlichem eine automatische Datenproduktion nach sich ziehen.

31) Geräte und Apps zur Erhebung gesundheitsrelevanter Daten können den zeit- und ortsunabhängigen Zugang des Betroffenen zu seinen Gesundheitsinformationen und eine faktengestützte Gesundheitsversorgung erleichtern sowie einen gesundheitsbewussten Lebensstil und das persönliche Wohlergehen fördern. Sie eröffnen zudem

Chancen für die Forschung, wenn sie als wichtige quantitative und qualitative Erweiterung der Datengrundlage verwendet werden.

32) Andererseits kann eine überzogene Selbstkontrolle mithilfe solcher Angebote zu einem übertriebenen, der Gesundheit abträglichen Optimierungsstreben sowie der Medikalisierung „natürlicher" Lebensvorgänge beitragen. Zudem ist zweifelhaft, ob Selbstvermessung tatsächlich immer Ausdruck persönlicher Souveränität oder eher eine Form selbstinduzierter Fremdbestimmung ist. Befürchtet wird ferner die Diskriminierung von Personen, die sich an solchen Messungen nicht beteiligen können oder wollen. Auch die bisherige Orientierung vieler Angebote an den wirtschaftlichen Interessen der Hersteller sowie Mängel bei Nutzerfreundlichkeit, Transparenz und Datenschutz lösen Kritik aus.

33) Zusammenfassend lassen sich anwendungskontextübergreifend die folgenden Stärken, Schwächen, Chancen und Risiken von Big Data in gesundheitsrelevanten Bereichen identifizieren: Zu den Stärken gehören die wachsende Datenbasis, die damit verbundene Entwicklung innovativer digitaler Instrumente sowie der hohe Grad der Vernetzung der Akteure. Zu den Schwächen gehören Schwankungen bei der Datenqualität, Intransparenz von Datenflüssen, Kontrollverluste sowie erhöhte Koordinations-, Regulierungs- und Qualifikationsanforderungen.

34) Als Chancen von Big Data sind vor allem bessere Stratifizierungsmöglichkeiten bei Diagnostik, Therapie und Prävention und damit verbundene Effizienz- und Effektivitätssteigerungen sowie die Unterstützung gesundheitsförderlichen Verhaltens zu nennen. Risiken bestehen hinsichtlich Entsolidarisierung, Verantwortungsdiffusion, Monopolisierung, Datenmissbrauch und informationeller Selbstgefährdung.

35) Die konkrete Beurteilung von Big-Data-Anwendungen mit Gesundheitsbezug hängt maßgeblich von den jeweils beteiligten Akteuren

mit ihren unterschiedlichen Interessen und eigenen Chancen- und Risikoeinschätzungen sowie dem jeweiligen Anwendungskontext ab.

Rechtliche Vorgaben für Big Data

36) Big Data stellt eine erhebliche Herausforderung für das Rechtssystem dar. Zu berücksichtigen sind dabei vor allem verfassungsrechtliche Vorgaben, das allgemeine Datenschutzrecht, die speziellen Datenschutzbestimmungen des Gesundheitssektors sowie das Medizinprodukterecht, aber auch die zugrunde liegenden Anreizmechanismen und selbstregulative sowie hybride Steuerungsmechanismen.

37) Die wesentlichen Elemente des Datenschutzrechts sind grundrechtskonstituiert. Die zentrale verfassungsrechtliche Maßstabsnorm auf nationaler Ebene ist das Recht auf informationelle Selbstbestimmung, das vom Bundesverfassungsgericht im Volkszählungsurteil als spezifische Ausprägung des allgemeinen Persönlichkeitsrechts entwickelt worden ist. Es flankiert und erweitert den grundrechtlichen Schutz von Privatheit und Verhaltensfreiheit.

38) Diese Entfaltungsfreiheiten können mit wichtigen Gemeinwohlbelangen kollidieren wie der Förderung des wissenschaftlichen Fortschritts oder der Gewährleistung einer effektiven Gesundheitsversorgung. Konflikte können aber auch mit den Grundrechtspositionen anderer Privatrechtssubjekte bestehen, die ihnen zugängliche Informationen aufgreifen und verarbeiten wollen.

39) Das Datenschutzrecht orientiert sich an den verfassungsrechtlichen Vorgaben. Es wurde allerdings nicht für Verwendungskontexte geschaffen, die erst durch die neuen technischen Möglichkeiten relevant werden, und ist auch nach seinen jüngsten, durch die europäische Datenschutz-Grundverordnung veranlassten Veränderungen auf das Phänomen Big Data unzureichend eingestellt. Dies gilt

ungeachtet der klaren Fortschritte, die diese neuen Vorgaben etwa mit Blick auf die Etablierung grenzüberschreitender Standards sowie die stärkere Einbeziehung des Konzepts von *privacy by design* bedeuten.

40) Grundlegende Annahmen, zentrale Prinzipien und Zielvorgaben des überkommenen Datenschutzrechts sind mit den Besonderheiten von Big-Data-Anwendungen kaum in Einklang zu bringen. Die traditionellen datenschutzrechtlichen Grundsätze des Personenbezugs, der Zweckbindung und Erforderlichkeit der Datenerhebung, der Datensparsamkeit, der Einwilligung und Transparenz stehen der spezifischen Eigenlogik von Big Data entgegen. Will man weder den Einsatz von Big Data grundsätzlich untersagen noch relevante Einbußen am Schutzniveau hinnehmen, müssen neue Gestaltungsoptionen und Regelungsmechanismen entwickelt werden.

41) Das geltende Datenschutzrecht knüpft an den Personenbezug von Daten an und legt besonderen Wert auf die damit einhergehenden spezifischen Zweckbindungen. Für Big Data ist demgegenüber entscheidend, dass bei der Erfassung der Daten die künftigen Anwendungen nicht vorhersehbar sind und auch der Personenbezug bzw. der Bezug zu ihrer Gesundheit unter Umständen erst nachträglich hergestellt wird. Daten, die zu anderen Zwecken gespeichert wurden, werden oft für neue Zwecke ausgewertet oder es werden Daten für noch unbestimmte Zwecke erhoben.

42) In augenfälligem Widerspruch zu Big Data steht ferner der Grundsatz der Datensparsamkeit bzw. Datenminimierung, nach dem so wenig personenbezogene Daten wie möglich erhoben, verarbeitet oder genutzt werden sollen. Das führt leicht zu einem weitgehenden Ausschluss der Möglichkeiten von Big Data. Weil aber mit der Menge an gespeicherten Daten zugleich das Gefährdungspotenzial für das Recht auf informationelle Selbstbestimmung wächst, bedarf es wirksamer alternativer Schutzmechanismen.

43) Auch bei dem im Datenschutzrecht normierten Erfordernis der Einwilligung, wonach eine Datenverwendung nur erlaubt ist, wenn der Betroffene bei Abgabe seiner Einwilligung die Bedeutung und Tragweite der beabsichtigten Datenverwendung überblickt, zeigen sich Inkompatibilitäten mit Big Data. Schon jetzt ist häufig zweifelhaft, dass Datengeber insbesondere die Verwendungszwecke und die damit verbundenen Implikationen tatsächlich verstehen. Big Data verstärkt diese allgemeine Problematik noch einmal erheblich, da künftige Verwendungsarten zum Zeitpunkt der Datenerhebung oftmals unbekannt sind.

44) Das geltende Datenschutzrecht bietet zudem jenseits der Einwilligung nur wenige Möglichkeiten, auf das weitere Schicksal der Daten Einfluss zu nehmen. Jede weitere Verwendung bedarf einer neuen Einwilligung, und sind Daten einmal mit Einwilligung erhoben, können sie von dem Betroffenen nicht mehr weiterverfolgt werden. Die Dynamik von Big Data passt nicht in dieses Regelungskonzept. Gerade wenn man die Zustimmung der Betroffenen für ein zentrales Erfordernis des Datenschutzes erachtet, ist deshalb nach Wegen zu suchen, wie dies auch unter Big-Data-Bedingungen funktional sinnvoll möglich ist.

45) Big Data intensiviert zudem gerade durch die Verknüpfung vielfältiger Daten die Möglichkeiten der Reidentifizierung und verstärkt damit Zweifel an der Effektivität des Anonymisierungs- bzw. Pseudonymisierungsgebots. Die Frage, inwieweit und ab welchem Grad die Gefahr einer Reidentifizierung für sich genommen anonymisierter Daten für die Annahme eines Personenbezugs der Daten ausreichend ist und wie das gemessen werden kann, verschärft die Problematik um den ohnehin schon umstrittenen Begriff des Personenbezugs im Datenschutzrecht.

46) Die Rechte auf Auskunft, Berichtigung, Löschung und Sperrung dienen der Transparenz, bieten aber häufig keinen effektiven Schutz.

Gerade im Kontext von Big Data wird der Datengeber kaum alle potenziellen Anspruchsgegner kennen. Auch die von den Auskunftsrechten umfasste Nachvollziehbarkeit des Datenverarbeitungsprozesses gestaltet sich angesichts komplexer und selbstlernender Algorithmen schwierig. Damit läuft auch das Recht auf Berichtigung und Löschung leer, da der Betroffene diese Rechte ohne eine umfassende Auskunft nicht wahrnehmen kann.

47) Diese auf das allgemeine Datenschutzrecht bezogene Defizitanalyse kann mit gewissen Einschränkungen auf das besondere Gesundheitsdatenschutzrecht übertragen werden, das das zum Teil bereichsspezifisch ausgestaltete Datenschutzrecht um die zivil-, straf- und berufsrechtlichen Vorgaben der ärztlichen Schweigepflicht ergänzt. Im Kern bleiben auch die normativen Lösungsansätze des Gesundheitsdatenschutzrechts weitgehend einer Problemperspektive aus der „Vor-Big-Data-Zeit" verhaftet.

48) Eine kompensatorische Wirkung könnten die Bestimmungen des Medizinprodukterechts entfalten, das den freien Verkehr mit Medizinprodukten regelt und dabei gleichzeitig die Sicherheit, Eignung und Leistung der Medizinprodukte zum Schutz der Patienten, Anwender und Dritter zu gewährleisten versucht. Anders als Arzneimittel bedürfen Medizinprodukte keiner staatlichen Zulassung, wohl aber der Zertifizierung nach einer produktspezifischen Risikobewertung, Risikominimierung und Risiko-Nutzen-Analyse sowie einem dem Risiko des Produkts angemessenen Verfahren der Konformitätsbewertung.

49) Software kann als Medizinprodukt zu klassifizieren sein, wenn sie eine medizinische Zweckbestimmung hat. Ob dies der Fall ist, hängt maßgeblich von den Angaben des Herstellers ab. Die Abgrenzung zwischen medizinischen Anwendungen und bloßen Lifestyle- oder Fitness-Apps gestaltet sich allerdings in der Praxis oft schwierig.

50) Die Vorgaben des Krankenversicherungsrechts erweisen sich ebenfalls als relevant für Big Data. Die Einordnung von M-Health-Applikationen in die Vergütung der gesetzlichen wie privaten Krankenversicherung könnte zum Beispiel finanzielle Anreize für Entwickler solcher Angebote und damit ein Gegenmodell zum „Zahlen mit Daten" schaffen. Dabei sind jedoch Wirksamkeitsnachweise zu erbringen. Ebenso sind Diskriminierungen zu vermeiden, auch bei der Berücksichtigung solcher Daten bei der Beitragsgestaltung.

51) Angesichts der jüngst erfolgten umfassenden Neuordnung des Datenschutzrechts durch die Datenschutz-Grundverordnung und das neue Bundesdatenschutzgesetz ist zwar abzuwarten, ob und wie sich die neuen Normen und Mechanismen bewähren. Indes dürfte feststehen, dass einige Grundprinzipien des geltenden Datenschutzrechts mit dem Konzept von Big Data kaum in Einklang zu bringen sind. Dieser Spannung kann im Rahmen der vom Verfassungsrecht gewährten Handlungsspielräume mit flexiblen, innovationsoffenen Regelungen Rechnung getragen werden, die auch die Verwendung komplexerer, privatrechtlicher wie privat-staatlich kooperativer Steuerungsbeiträge mitberücksichtigen.

52) Insbesondere wäre zu prüfen, ob der Mangel an Konkretheit von gesundheitsrelevanten Big-Data-Anwendungen durch zusätzliche technisch-organisatorische sowie materiell- und verfahrensrechtliche Sicherungen kompensiert werden kann. Im Zuge der Weiterentwicklung des Datenschutzrechts könnte vor allem eine stärker ausdifferenzierte, den Besonderheiten eines Regelungsbereichs und den Präferenzen der Betroffenen Raum gebende Konzeption von Einwilligungsmodellen oder eine verstärkte Erhebung und Nutzung von Daten auf Basis gesetzlicher Erlaubnisnormen in den Blick genommen werden. Auch dem Privatrecht kommt große Bedeutung für die Weiterentwicklung des Datenschutzes zu, vor allem dem Verbraucherrecht, dem Haftungsrecht sowie den Regelungen für die

Zuordnung von Daten und die Befugnis, über ihre Verwendung zu bestimmen („Eigentum“ an Daten).

53) Sämtliche Steuerungsansätze für Big Data haben mit dem Problem zu kämpfen, mit einer territorial begrenzten Rechtsetzung auf ein seiner Natur nach globales Phänomen zu reagieren. Die jeweiligen Datenschutzrechte sind international gesehen sehr unterschiedlich, was sowohl die Betroffenen als auch die Regulierer vor besondere Herausforderungen stellt. Trotz vielfältiger Harmonisierungsbemühungen gibt es nach wie vor zahlreiche praktische Hindernisse, die einer effektiven grenzüberschreitenden Rechtsverfolgung im Wege stehen.

54) Angesichts der spezifischen Dynamik und Volatilität des Regelungsbereichs gewinnen zudem nicht hoheitliche und kooperative Steuerungsmechanismen an Bedeutung, zum Beispiel Zertifizierungen mit Datenschutz- bzw. Datensicherheitssiegeln oder Handlungsregeln und Kodizes für Wissenschaft und Wirtschaft.

Zur Ethik von Big Data und Gesundheit

55) Von Big Data sind sowohl ethische Orientierungsmuster betroffen, die normativ und evaluativ die Rolle, Funktion und Stellung des datengebenden Individuums thematisieren, als auch Maßgaben sozialer Orientierung. Zu den relevanten Begriffen gehören Freiheit und Selbstbestimmung, Privatheit und Intimität, Souveränität und Macht, Schadensvermeidung und Wohltätigkeit sowie Gerechtigkeit, Solidarität und Verantwortung.

56) Der Ausdruck Freiheit wird in vielen Bedeutungen verwendet. Dabei ist zu unterscheiden zwischen Handlungsurheberschaft als grundsätzlicher Freiheitsbedingung und Selbstbestimmung als Praktisch-Werden von Freiheit in Abhängigkeit von mehr oder weniger deutlich

erfahrbaren Umständen. Selbstbestimmt sind Handlungsurheber in unterschiedlichen Graden.

57) Der Begriff der Selbstbestimmung bezeichnet sowohl die Fähigkeit einer Person, ihr Leben nach ihren eigenen Vorstellungen zu gestalten, als auch die tatsächliche Ausübung dieser Fähigkeit und einer als ideal vorgestellten Form der Lebensführung. Von diesen Formen personaler Selbstbestimmung ist der rechtliche Schutz ihrer Ausübung zu unterscheiden. Formen und Grade der Ausübung von Selbstbestimmung sind von erheblicher praktischer Bedeutung. So kann man in bestimmten Zusammenhängen sein Recht auf Selbstbestimmung delegieren oder können Einschränkungen der Selbstbestimmungsfähigkeit teilweise durch Vertreter kompensiert werden.

58) Im Kontext von Big Data sind vor allem für Biobanken in den letzten Jahren neue Einwilligungsmodelle entwickelt worden, die mit Blick auf die Selbstbestimmung der Datengeber eine Balance zwischen einer unrealistisch engen Zweckbestimmung und einer einmaligen, allzu breiten Freigabe garantieren sollen. Hierbei werden dynamische Modelle, bei denen mehrfach in jeweils einzelne Elemente eingewilligt werden kann, um weitere Optionen ergänzt, etwa um Möglichkeiten zur Delegation. Teilnehmer können zudem entscheiden, welche Form der Einwilligung sie grundsätzlich bevorzugen.

59) Für die Beurteilung von Selbstbestimmung ist auch der soziale Kontext des Handelnden einzubeziehen. Frei zu sein und selbstbestimmt handeln zu können, bedeutet vor diesem Hintergrund zumindest die realistische Möglichkeit, die eigene Identität zu bewahren und zu gestalten sowie die eigenen Handlungen vor sich und anderen zu verantworten. Dazu sind verlässliche und faire rechtsstaatliche Standards notwendig, die ohne Ansehen der Person gelten.

60) Privatheit bezeichnet klassischerweise das Recht, in Ruhe gelassen zu werden bzw. eine Lebenssphäre, in der eine ungewollte Kontrolle

durch die Öffentlichkeit und Rechtfertigungsnotwendigkeiten weitgehend zurückgedrängt sind. Eng mit Privatheit verbunden ist der Begriff der Intimität. Er kennzeichnet Lebensbereiche, die ausschließlich den unmittelbar Betroffenen vorbehalten bleiben und deren Details diese – wenn überhaupt – nur ausgewählten anderen selbstbestimmt zugänglich machen.

61) Was als privat und intim gilt oder gelten sollte, ist in erheblichem Umfang kulturvariant. Dessen ungeachtet lässt sich die Wahrung der Privatsphäre jedoch normativ mit ihrer sozialanthropologischen Bedeutsamkeit begründen. Nur in der Sphäre des Privaten können sich soziale Nahbeziehungen wie auch die Entwicklungsbedingungen personaler Identität ausbilden. Privatheit eröffnet Räume von Intimität und Vertraulichkeit, in denen Personen Beziehungen pflegen und unbefangen und unverstellt sie selbst sein können – nach außen abgeschirmt, nach innen aber offen.

62) Mit Blick auf Big Data ergeben sich mögliche Privatheitsgefährdungen aus den vielfältigen neuen Gelegenheiten zur Erfassung, Analyse und neuen Verknüpfung von Daten und Informationen sowie der damit einhergehenden erschwerten Anonymisierung und Pseudonymisierung. Je mehr intime Details digital preisgegeben werden können, desto eher droht zudem eine selbstinduzierte Fremdbestimmung bzw. informationelle Selbstgefährdung im Rahmen einer persönlichen Lebensführung, die sich maßgeblich von äußeren Einflussfaktoren abhängig macht.

63) Auch wenn in der digitalen Gesellschaft eine vollständige Kontrolle der eigenen Datenspuren unmöglich geworden sein mag, legen Menschen Wert darauf, kontextabhängig mitbestimmen zu können, wie ihre Daten gebraucht und weiterverwendet werden. Gleichzeitig gewinnt die Erwartung an Bedeutung, dass Datennutzer die ihnen zur Verfügung gestellten Daten auch im Rahmen von De- und Rekontextualisierungen vertraulich und vertrauenswürdig behandeln.

64) Wie Privatheit unter den Bedingungen von Big Data zu schützen ist, betrifft nicht nur Individuen, sondern auch Gruppen. Die Analyse großer Datenmengen erlaubt es oft, auf Merkmalskombinationen zahlreicher Personen zu schließen. Betroffene werden von Algorithmen zu Gruppen zusammengefasst, mit möglicherweise stigmatisierenden, diskriminierenden oder exkludierenden Folgen. Eine solche Zuordnung ist für den Einzelnen oft nicht erkennbar.

65) Zentrale Bedeutung im Kontext von Big Data erhält der Begriff der Souveränität. Er entstammt kulturhistorisch vornehmlich dem religiös-politischen Bereich und wird in zahlreichen Lebensbereichen unterschiedlich konkretisiert. Souveränität galt als jene Eigenschaft Gottes oder eines absolutistischen Herrschers, kraft derer er absolut und unbedingt von anderen Mächten alles zu tun oder zu lassen imstande sei. Andere Konzepte von Souveränität betonen anstelle einer vermeintlichen absoluten Ungebundenheit des souveränen Subjekts die Abhängigkeiten seiner physischen wie sozialen Leiblichkeit.

66) Nach einem Souveränitätsverständnis, das jedenfalls eine Verfügungsgewalt von Menschen über andere Menschen grundsätzlich ausschließt, sind personenbezogene Daten für die Sammler und Nutzer nur Leihgabe, niemals frei und willkürlich verfügbares Eigentum. Das bedeutet zwar umgekehrt nicht, dass damit der Datengeber automatisch Eigentümer seiner Daten ist oder selbst seinen Souveränitätsanspruch unter allen Umständen realisieren kann, begründet jedoch im Prinzip weitreichende Kontrollmöglichkeiten des Individuums.

67) Der Begriff der Souveränität ist eng mit dem der Macht verbunden. Souveränität verwirklicht sich im Modus der Ausübung von Macht und wird umgekehrt begrenzt durch die Ausübung souveräner Macht anderer. Im Kontext von Big Data werden spezifische Formen der Machtausübung ethisch bedeutsam: erstens solche, mit denen Präferenzen und Überzeugungen anderer manipuliert werden können; und zweitens solche, die darüber hinaus sogar eine subtile Formung,

Veränderung und damit mögliche Beherrschung ihrer Charaktere ermöglichen.

68) Der Einsatz von Big-Data-Algorithmen eröffnet Anbietern von Internetdiensten neue Möglichkeiten gezielter Einflussnahme auf das Denken, Fühlen und Handeln der Nutzer solcher Dienste. Das Spektrum reicht von offenem Nudging, mit dem gesundheitsförderliches Verhalten subtil angeregt werden soll, bis hin zu verdeckten und vor allem fremdnützigen manipulierenden Interventionen. Letztere sind ethisch zumindest besonders rechtfertigungsbedürftig. Denn sie entziehen sich der kognitiven Kontrolle durch den Betroffenen, umgehen damit seine Möglichkeiten zur Beherrschung der Bedingungen seines Handelns und untergraben so seine Selbstbestimmtheit.

69) Ein weiterer relevanter normativer Bezugspunkt ergibt sich aus der moralischen Verpflichtung zur Wohltätigkeit, wonach das eigene Handeln in vielen Situationen über die bloße Schadensvermeidung hinaus auch Vorteile für andere, insbesondere für hilfsbedürftige Menschen erbringen soll. Für das Thema Big Data und Gesundheit sind vor allem zwei Aspekte von Wohltätigkeit von besonderem Interesse: zum einen der Wissens- und Erkenntniszuwachs und zum anderen der therapeutische Mehrwert, der aus neuen Möglichkeiten der digitalen Informationsgewinnung und -verarbeitung großer Datenmengen im Gesundheitsbereich für unterschiedliche Beteiligte resultiert.

70) Wissen und Erkenntnis sind von großer Bedeutung für die Selbstkonstitution des Individuums und seine Befähigung zur autonomen Lebensführung. Darüber hinaus kommt der kritischen Überprüfung, der Sicherung und der Ausweitung von Wissensbeständen eine wichtige gesellschaftliche Funktion zu.

71) Um die mit Wissenszuwachs verbundenen Ziele zu erreichen, bedarf es des Schutzes einer der Wahrhaftigkeit verpflichteten Kommunikation. Zu deren Sicherung insbesondere auf dem Feld der Wissenschaften

haben sich differenzierte methodologische und wissenschaftstheoretische Maßgaben entwickelt. Daher ist darauf zu achten, dass neue digitale Verfahren der Datensammlung, -auswertung und -verknüpfung nicht zur Absenkung epistemischer Standards oder zu Einbußen der Zuverlässigkeit daraus gewonnener Aussagen führen.

72) Zu klären ist auch, welchen Personengruppen die durch Big Data erzielten Erkenntnisfortschritte jeweils primär zugutekommen sollen, wie sich derzeit bestehende Hindernisse auf dem Wege einer effizienteren Gestaltung des Datennutzungsprozesses beseitigen lassen und wie eine gerechte Verteilung jener positiven Effekte erreicht werden kann, die aus dem zu erwartenden Wissenszuwachs resultieren.

73) Die Sammlung und Weitergabe großer Mengen gesundheitsbezogener Daten berührt grundlegende Fragen der Gerechtigkeit. Als normierendes Prinzip sozialer Beziehungen gebietet die Gerechtigkeit, willkürliche Privilegierungen Einzelner oder bestimmter Gruppen zu vermeiden. Vielmehr ist das jedem Einzelnen Angemessene auf rationale Weise zu bestimmen. Das setzt voraus, dass einheitliche Kriterien Verwendung finden und Unterschiede in der Behandlung Einzelner normativ konsensfähig begründet werden.

74) Mit Blick auf Big-Data-Anwendungen im Gesundheitsbereich sind vor allem vier Problemfelder besonders gerechtigkeitsrelevant: erstens der Zugang zu Datensammlungen für den Forschungsbereich, zweitens die schleichende Etablierung monopolartiger Strukturen, drittens die Einbeziehung von Gesundheits-Apps und verschiedenen, der privaten Selbstvermessung dienenden Geräten in die Tarifgestaltung von Krankenversicherungen und viertens Aspekte der Befähigungsgerechtigkeit im Hinblick auf einen verantwortlichen Umgang mit gesundheitsbezogenen Daten.

75) Der Begriff der Solidarität bezeichnet prosoziale Handlungen, Praktiken und Dispositionen sowie institutionelle, politische und

vertragliche Regelungen, die dazu dienen sollen, andere zu unterstützen. Solidarität wird vielfach als komplementär – und oft auch subsidiär – zur Gerechtigkeit verstanden. Sie entsteht regelmäßig vor dem Hintergrund gemeinsamer Ziele einer Gruppe, angesichts einer gemeinsamen Herausforderung oder auch aus der geteilten Vorstellung vom guten Leben in einer Solidargemeinschaft.

76) Solidarität gründet häufig in Reziprozitätserwartungen. Die Bereitschaft zur Solidarität kann nachlassen, wenn Zweifel an der Einlösbarkeit solcher Erwartungen entstehen, etwa wenn auf Dauer der Eindruck entsteht, die Hilfs- und Unterstützungsbedürftigkeit anderer werde durch deren fahrlässige Selbstschädigung oder mangelnde Eigeninitiative verursacht und das Solidaritätsgefüge damit überstrapaziert.

77) Die durch Big Data ermöglichte Auswertung umfänglicher und vielfältiger gesundheitsrelevanter Daten erlaubt die Erstellung genauerer Risikoprofile. Damit verbindet sich die Sorge, dass die Annahme einer allen gemeinsamen Vulnerabilität gegenüber Krankheitsrisiken, die nicht sicher antizipierbar sind, als Grundlage der Solidargemeinschaft in der gesetzlichen Krankenversicherung und der fairen Vertragsgestaltung in der privaten Krankenversicherung infrage gestellt werden könnte. Dann könnten Niedrigrisikogruppen verstärkt die Solidargemeinschaft verlassen, wodurch für Letztere erhebliche Mehrbelastungen entstünden.

78) Innerhalb der gesetzlichen Krankenversicherung unterlaufen verhaltensdatenbasierte Versicherungstarife den Solidargedanken, der die Absicherung gegen krankheitsbedingte Vulnerabilität weitgehend ohne Ansicht individueller verhaltensbedingter Risiken fordert. Die private Krankenversicherung arbeitet hingegen mit risikoäquivalenten Prämien. Auch hier kann sich eine Umverteilung von Risiken zuungunsten der Versicherten ergeben, falls Prämien künftig auf Grundlage der durch Big Data ermöglichten kontinuierlichen

Erhebung und Auswertung individueller Daten auch nach Abschluss der Versicherung regelmäßig angepasst würden. Dies würde das Versicherungsprinzip, nach dem Risiken von einer größeren Gruppe gemeinsam getragen werden und Tarife auch nicht individualisiert angepasst werden dürfen, gänzlich aushebeln. Es könnten zunehmend kleine Tarifgruppen entstehen, bei denen Schadensfälle dann umso schneller zu Beitragserhöhungen führen.

79) Zudem könnten privat Versicherten, die nicht bereit oder in der Lage sind, in einem verhaltensbasierten Versicherungsmodell mitzuwirken, finanzielle Vorteile vorenthalten werden, was auf lange Sicht zu Prämiennachteilen führen muss. Unabhängig davon, ob sie sich gesundheitsförderlich verhalten oder nicht, würden sie dafür bestraft, dass sie ihre Daten nicht der Versicherung überlassen, und somit durch die Ausübung ihres Rechts auf informationelle Selbstbestimmung benachteiligt.

80) Grundsätzlich hat die Freiheit zur Lebensgestaltung und Selbstentfaltung Vorrang vor einer strikten und permanenten Pflicht zur Vermeidung aller Gesundheitsrisiken. Dies gilt zwar nicht unbegrenzt, doch ließen sich die dauernde gezielte Sammlung von Daten über die individuelle Lebensführung und die Nutzung Big-Data-gespeister Risikoprofile, die alle Lebensbereiche umfassen, schwerlich als zumutbare Erwartung an die Mitverantwortung für die eigene Gesundheit qualifizieren.

81) Ob und wie gesetzliche Krankenkassen gesundheitliche Eigenverantwortung berücksichtigen und das Gesundheitsverhalten ihrer Versicherten beeinflussen dürfen, ist umstritten. Datenbasierte Anreizsysteme könnten eine sehr intensive und invasiv-überwachende Wirksamkeit entfalten. Die differenzierte Offenlegung von Risikofaktoren über Big-Data-Analysen, die Daten aus allen Lebensbereichen integrieren, könnte künftig aber auch ergeben, dass der weitaus überwiegende Teil der Bevölkerung gemischte Risikoprofile hat, die

protektive und günstige Faktoren ebenso einschließen wie negative Faktoren körperlicher, mentaler, verhaltensbedingter und anderer Art.

82) In verschiedenen Bereichen der Medizin hat der Einsatz von Big-Data-Technologien bereits zur Entwicklung neuer prosozialer Unterstützungspraktiken geführt, beispielsweise zur Bildung kleinerer Gruppen von Patienten, die insbesondere seltene Krankheitsrisiken oder -erfahrungen teilen und ihre Daten und Bioproben in gemeinschaftlichen Pools zusammenführen, um sie für die Forschung an ihrem Krankheitsbild zur Verfügung zu stellen.

83) Andere Solidaritätsgewinne sind gegenwärtig in Online-Foren zu beobachten, in die Patienten ihre Erfahrungen und Krankheitsdaten aus Klinik und Selbstvermessung einspeisen, sie dort austauschen, gemeinsam diskutieren und für das individuelle Krankheitsmanagement nutzen. Mit der zunehmenden Entwicklung von online vernetzten Instrumenten für die Patienten-Selbsthilfe steht zu erwarten, dass derartige Praktiken zunehmen werden.

84) Verantwortung als moralische Kategorie lässt sich nach Handlungs- und Entscheidungstypen, aber auch nach der Ausgestaltung institutioneller Strukturen differenzieren. Sie kann moralisch, rechtlich, politisch und vertraglich sowie vor und nach einer Handlung oder Entscheidung eingefordert und übernommen werden. Die damit verbundenen unterschiedlichen Typen von Verantwortung stehen oft in einem sachlichen Wechselverhältnis: Man erwartet genau von demjenigen die Übernahme von Verantwortung für die Zukunft, den man in einem tatsächlichen Schadensfall zur Rechenschaft ziehen würde. Das komplexe Zusammenspiel zwischen Einzelnen, Institutionen und Technik beim Einsatz von Big Data gewinnt im gesundheitsrelevanten Bereich besondere Bedeutung. Vermieden werden sollte eine undurchsichtige Diffusion von Verantwortung, die dort droht, wo viele Akteure und hoch technisierte Prozesse zusammenwirken.

85) Damit individuelle Datengeber auch im Big-Data-Zeitalter Verantwortung für ihre Daten übernehmen können, bedarf es bestimmter Rahmenbedingungen, die sich technisch wie organisatorisch leicht und effektiv nutzen lassen. Im sensiblen Gesundheitsbereich gelten zudem erhöhte Sorgfaltspflichten, etwa für Forscher oder Ärzte.

86) Zu den Möglichkeiten von Unternehmen, Big-Data-Prozesse verantwortlich zu gestalten, gehört es vor allem, Bedingungen dafür zu schaffen, gegebene Zustimmungen widerrufbar zu machen und die Verwaltung von Daten auf Abruf zu gestalten. Davon ausnehmen könnte man hinreichend aggregierte Daten, abgeleitete Daten oder Modelle, die nachweislich keinen Rückschluss auf den Einzelnen erlauben. Mit solchen Ansätzen die Big-Data-spezifischen De- und Rekontextualisierungen bei gleichzeitiger Wahrung hoher Anonymisierungsstandards zu ermöglichen und Institutionsvertrauen zu schaffen, dürfte eine der entscheidenden Aufgaben der Zukunft sein.

87) Eine weitere Möglichkeit, Verantwortung für die Rechte des Individuums zu übernehmen und dabei dennoch legitime Geschäftsinteressen zu wahren, wären Stellvertretersysteme an den programmatischen Schnittstellen in Datennetzwerken. Solche Schnittstellen könnten als „Datenagenten“ Präferenzen von Datengebern für die Datenhandhabung umsetzen. Hierdurch würde eine individuelle Datenverwaltung durch eine programmatische Verwaltung ersetzt, die dem Einzelnen eine technisch niedrigschwellige und reliable Möglichkeit gäbe, Verantwortung für die Wahl eigener kurz-, mittel- und langfristiger Strategien der Datenhandhabung zu übernehmen, ohne jede Einzelfrage selbst entscheiden zu müssen.

88) Unternehmen können Verantwortung auch übernehmen, indem sie ihre Verfahren besser überprüfbar machen, etwa mit Blick auf die verwendeten Algorithmen, den Ausschluss systematischer Benachteiligungen, die Einhaltung von Regeln zur Datenaufbewahrung, Anonymisierung oder Datenlöschung und die lückenlose und

manipulationssichere Protokollierung der Herkunft, Verarbeitung, Verwendung und des Austauschs von Daten.

89) Neben staatlicher Regulierung gibt es weitere Möglichkeiten, die Übernahme von Verantwortung durch institutionelle Akteure zu gewährleisten bzw. zu fördern. Zertifizierungen, Qualitätssiegel oder Selbstverpflichtungen, die von Interessen- oder Berufsverbänden bereitgestellt und überprüft werden, können beispielsweise Vertrauen in die jeweiligen Organisationen und Prozesse stärken.

90) Eine weitere Verantwortungsfrage betrifft mögliche Eingriffe von Organisationen in die persönliche Kommunikation zwischen Nutzern, beispielsweise in Form gesundheitsförderlicher Hinweise oder Hilfsangebote. Dagegen spricht einerseits die Ablehnung offensichtlicher Eingriffe in die Privat- oder Intimsphäre. Wäre die Funktionssicherheit solcher Algorithmen aber wissenschaftlich gut belegt, müsste man andererseits aus ethischer Perspektive auch berücksichtigen, dass ihr Einsatz gegebenenfalls schweres Leid oder sogar Todesfälle verhindern könnte, beispielsweise bei Hilfsangeboten für suizidgefährdete Personen in sozialen Netzwerken.

91) Der Staat kann auf nationaler Ebene, im Verbund der EU, aber auch als völkerrechtlicher Akteur Verantwortung übernehmen. Mit Blick auf die angedeutete Problematik der Rechtsumsetzung sollte allerdings ein regulatorischer Subsidiaritätsgrundsatz gelten, der Selbstverpflichtungen und Zertifikaten den Vorzug vor detaillierten rechtlichen Regelungen lässt, sofern und solange diese effektiv funktionieren.

92) Angesichts der drei Ebenen möglicher Verantwortungszuschreibung im Bereich gesundheitsbezogener Big-Data-Anwendungen (Individuen, Organisationen, Staat) bleiben Individuen zwar in der Pflicht, Verantwortung für die Nutzung ihrer Daten zu übernehmen. Vornehmlich tragen jedoch die Daten sammelnden, verarbeitenden und

weitergebenden Organisationen Verantwortung dafür, Rahmenbedingungen für die verantwortliche informationelle Freiheitsgestaltung der Datengeber zu gewährleisten.

93) Je weniger Organisationen willens oder fähig sind, technische Möglichkeiten bereitzustellen, die dem Einzelnen die Kontrolle über seine Daten erleichtern, desto mehr drängt sich in verantwortungsethischer Perspektive die Notwendigkeit für den Staat auf, gewährleistend, überwachend und gegebenenfalls auch regulierend und sanktionierend einzugreifen. Das Ziel, dem Einzelnen die Möglichkeit zum souveränen Umgang mit seinen Daten zu geben, ist nur erreichbar, wenn dazu auf allen Seiten die jeweils gebotene Verantwortung übernommen wird.

Datensouveränität als informationelle Freiheitsgestaltung

94) Datensouveränität, verstanden als eine den Chancen und Risiken von Big Data angemessene verantwortliche informationelle Freiheitsgestaltung, sollte das zentrale ethische und rechtliche Ziel im Umgang mit Big Data sein.

95) Der Begriff der informationellen Freiheitsgestaltung entwickelt das Konzept der informationellen Selbstbestimmung weiter. Er gründet nicht in einem eigentumsanalogen Ausschlussrecht, sondern in der Befugnis, selbst zu bestimmen, mit welchen Inhalten jemand in Beziehung zu seiner Umwelt tritt. Informationelle Freiheitsgestaltung in diesem Sinne meint interaktive Persönlichkeitsentfaltung unter Wahrung von Privatheit in einer vernetzten Welt und ist gekennzeichnet durch die Möglichkeit, auf Basis persönlicher Präferenzen effektiv in den Strom persönlich relevanter Daten eingreifen zu können. Verantwortlich ist eine solche Freiheitsgestaltung dann, wenn sie sich gleichzeitig an den gesellschaftlichen Anforderungen von Solidarität und Gerechtigkeit orientiert.

96) Mit Datensouveränität im hier vertretenen Sinne werden weder die tradierten, letztlich kaum veränderten Regulierungsansätze des Datenschutzes nur unter neuem Namen fortgeschrieben, noch wird damit eine vollständige Neuorientierung oder gar eine Aufgabe des herkömmlichen Datenschutzgedankens oder die generelle Absenkung des bestehenden Schutzniveaus gefordert. Vielmehr geht es darum, die benannten normativen Grundanforderungen, einschließlich der ethisch wie grundrechtlich fundierten informationellen Selbstbestimmung und damit auch des Datenschutzes, unter den Bedingungen von Big Data zur Geltung zu bringen.

97) Datenschutz war und ist kein Selbstzweck, sondern dient dem Schutz der Person: ihrer Privatsphäre ebenso wie der freien Entfaltung ihrer Persönlichkeit in der Öffentlichkeit. Mit dem Begriff der Datensouveränität wird aber zugleich die Absicht betont, den souveränen, also selbstbestimmten und verantwortlichen Umgang des Einzelnen mit seinen eigenen personenbezogenen Daten mit einer Realisierung der Potenziale zu verknüpfen, die Big Data sowohl gesellschaftlich als auch für die individuelle Lebensgestaltung eröffnet.

98) Das Ziel einer verantwortlichen informationellen Freiheitsgestaltung im Gesundheitsbereich besteht darin, die Big-Data-spezifischen Potenziale für die medizinbezogene Forschung, die klinische Anwendung und das individuelle Gesundheitsverhalten zu nutzen und die damit einhergehenden Risiken auf ein Minimum zu reduzieren.

99) Bei der Wahrnehmung und Gestaltung von Datensouveränität lassen sich zwei einander zunehmend annähernde und bereits jetzt teilweise überschneidende Sphären unterscheiden: erstens die Sphäre der bislang schon durch vergleichsweise klare und strikte Datenschutz-, Qualitäts- und Sicherheitsstandards gekennzeichneten Datennutzung in der medizinbezogenen Forschung und klinischen Praxis; zweitens die Sphäre der zunehmend den Gesundheitssektor mitbestimmenden, allerdings sehr heterogenen Angebote des freien

Marktes. Letztere reichen von Anwendungskonzepten, die nahe an der ersten Sphäre und den mit ihr verbundenen Standards liegen, bis hin zu ersichtlich unseriösen, nicht auf nachhaltige Gesundheitsförderung angelegten Angeboten.

100) Big-Data-Entwicklungen lassen sich nicht aufhalten, sehr wohl aber gestalten. Da die Handlungsformen und Schutzmechanismen des traditionellen Datenschutzrechts für eine solche Gestaltung nicht ausreichen, gilt es, ein verändertes, die Komplexität und Entwicklungsdynamik von Big Data stärker spiegelndes Gestaltungs- und Regelungsmodell zu erarbeiten. Dieses sollte Datensouveränität als informationelle Freiheitsgestaltung multidimensional und mit Blick auf unterschiedliche Akteursgruppen und Handlungskontexte reflektieren und dabei die zuvor skizzierten Verantwortungsmöglichkeiten und -zuschreibungen aufgreifen.

101) Unter den Bedingungen von Big Data ist es notwendig, sich von überholten Vorstellungen einer spezifischen, vorgegebenen Sensibilität bestimmter Daten und hierauf rekurrierender besonderer Schutzmechanismen zu lösen. Datenschutz kann nicht mehr statisch an bestimmten Daten und Datennutzungskategorien ansetzen, sondern muss sich auf ständige Rekombinationen und Rekontextualisierungen einstellen.

102) Ein auf Datensouveränität ausgerichtetes Gestaltungs- und Regelungsmodell nimmt dabei vor allem den Datengeber als entscheidend zu schützenden und zu achtenden Zweck in den Blick. Ziel ist es, über eine gleichermaßen kontextsensible wie falladäquate Regulierung und Institutionengestaltung diese Subjekte, aber auch die mit ihnen in Verbindung stehenden Organisationen zu einem souveränen Umgang mit ihren Daten zu befähigen. Vereinfachende Pauschallösungen sollten aufgegeben werden zugunsten komplexerer, aber auch flexiblerer und problemadäquater, institutionell diversifizierter Kombinationsmodelle.

103) Die heterogene zweite Sphäre gilt es dabei nach folgender Grundregel zu gestalten: Je näher einzelne Anwendungen an die erste Sphäre heranreichen, desto mehr besteht ethisch und rechtlich die Aufgabe, ihre Gestaltung multiakteursbezogen in die Richtung der dort generell vorherrschenden Qualitäts-, Schutz- und Vertraulichkeitsstandards zu entwickeln.

>> EMPFEHLUNGEN

Der Deutsche Ethikrat empfiehlt ein Gestaltungs- und Regelungskonzept, das sich am zentralen Ziel der Datensouveränität orientiert. Ein solches Konzept verlangt eine umfassende gesamtgesellschaftliche Anstrengung, die rechtliche wie außerrechtliche Elemente einbezieht, technische Weiterentwicklungen aufnimmt und deren grundrechtswahrende Verfügbarkeit für alle gesellschaftlichen Akteure gewährleistet. Das vorgeschlagene Gestaltungs- und Regelungskonzept enthält konkrete Handlungsempfehlungen zu vier Themenbereichen, die darauf abzielen, erstens die Potenziale von Big Data zu erschließen, zweitens individuelle Freiheit und Privatheit zu wahren, drittens Gerechtigkeit und Solidarität zu sichern und viertens Verantwortung und Vertrauen zu fördern. Die empfohlenen Maßnahmen sollten zeitnah verwirklicht und finanziert werden.

A. Potenziale erschließen

Um die Potenziale von Big Data im Gesundheitsbereich zu realisieren, ist eine möglichst reibungsfreie Kooperation zwischen zahlreichen Akteuren aus der klinischen Praxis, medizinbezogenen Grundlagenforschung, in gesundheitsrelevanten Feldern tätigen Unternehmen und individuellen Datengebern nötig. Sie sollte nicht nur auf die prospektive Sammlung und nachhaltige Bereitstellung von Datensätzen abzielen, sondern es auch ermöglichen, bereits vorhandene Datensätze aus Klinik und Forschung mit jeweils neu gewonnenen Daten in ethisch verantwortbarer Weise zu verknüpfen.

A1. Infrastrukturelle Grundvoraussetzungen schaffen

Die Nutzung der Chancen von Big Data im Gesundheitsbereich hängt entscheidend von der Verfügbarkeit einer leistungsfähigen Infrastruktur zur Erfassung, Speicherung, Analyse und Übertragung großer Datenmengen ab. Um problematische Abhängigkeiten von kommerziellen Anbietern infrastruktureller Dienstleistungen, die zudem häufig nicht den deutschen bzw. europäischen Schutzstandards unterliegen, zu vermeiden, sollte die öffentliche Hand gewährleisten, dass eine derartige Infrastruktur – insbesondere für die klinische Praxis und medizinbezogene Grundlagenforschung zeitnah und mit angemessenen Zugangsmöglichkeiten und öffentlicher Kontrolle geschaffen bzw. weiterentwickelt wird.

A2. Datenaustausch und -integration erleichtern

Ebenso sind der verantwortungsvolle Austausch und die Integration von gesundheitsrelevanten Daten zwischen vielfältigen institutionellen Akteuren durch eine Reihe von Maßnahmen und deren ausreichende öffentliche Finanzierung zu gewährleisten:

A2.1. Standardisierte Verfahren der Interoperabilität von Daten entwickeln und bereitstellen

Um eine adäquate Zusammenführung von Daten aus unterschiedlichen Quellen unter Berücksichtigung der Privatheitsansprüche der Datengeber

zu ermöglichen, müssen Daten miteinander vergleichbar sein, das heißt einheitlich benannt und angemessen annotiert sein. Eine wesentliche Voraussetzung hierfür ist die Standardisierung von Datenformaten und die Schaffung von Möglichkeiten zur Qualitätskontrolle einschließlich einer transparenten Dokumentation der durchlaufenen Schritte.

A2.2. Kooperatives Forschungsdatenmanagement weiterentwickeln
Die bestehenden Initiativen zur Etablierung effizienter Kommunikations-, Kollaborations- und Koordinationsstrukturen zwischen beteiligten Einrichtungen sollten gebündelt, intensiviert und auf Dauer gestellt werden. Dabei ist auch auf geeignete Schnittstellen zur Telematikinfrastruktur sowie auf eine angemessene Verzahnung mit der im E-Health-Gesetz vorgesehenen Weiterentwicklung der Vernetzung im Gesundheitswesen zu achten.

A3. Daten- und Forschungsqualität fördern und schützen
Eine zentrale Zukunftsaufgabe ist es, die Qualität der Daten zu kontrollieren, um auf diese Weise zu hinreichend verlässlichen Aussagen zu gelangen. Dafür sind folgende Maßnahmen geboten:

A3.1. Epistemische Standards einhalten, insbesondere die der evidenzbasierten Medizin
Bei der Weiterentwicklung von Kontrollmechanismen für die Sicherheit und Wirksamkeit medizinischer Maßnahmen, die bisher nicht auf Big-Data-Anwendungen zugeschnitten waren, dürfen die etablierten Maßstäbe der evidenzbasierten Medizin nicht unterschritten werden. Auch Big-Data-basierte Verfahren müssen sich für medizinische Verwendungszwecke den etablierten klinischen Prüfungen zur Wirksamkeit und Sicherheit unterziehen.

A3.2. Einheitliche Daten- und Dokumentationsstandards einführen
Nicht nur im Sinne der Interoperabilität und Kooperation, sondern auch zur Sicherstellung einer effektiven Qualitätskontrolle ist es sinnvoll, einheitliche Standards einzuführen. Das umfasst beispielsweise Fragen der Formate der Daten selbst, der sie beschreibenden Metadaten, der Rekonstruktion der Verarbeitungsschritte und Versionskontrolle sowie die

möglichst einheitliche Abbildung von semantischen Verknüpfungen und Hierarchien von Daten. Zu den die Datenqualität sichernden Standards zählen namentlich Dokumentationspflichten, mit deren Hilfe die Herkunft von Daten nachvollzogen werden kann und ihre weitere Nachverfolgbarkeit zumindest erleichtert wird.

A3.3. Datengütesiegel etablieren
Um die genannten Qualitätsstandards und die damit verbundenen Anforderungen transparent zu machen, sollten entsprechende Konformitätsbescheinigungen („Gütesiegel") vergeben werden, die die Herkunft und Qualität der Originaldaten und ihrer Verarbeitungsschritte nachweisbar darstellen (zum Beispiel durch Verwendung der Blockchain-Technologie). Weil die Qualitätssicherung auch im Eigeninteresse der jeweiligen Akteure liegt, ist primär auf wissenschafts- und wirtschaftsinterne Kontrollmechanismen zu setzen. Soweit diese sich indes als defizitär erweisen, sind auch übergreifende rechtliche Vorgaben einzuführen.

A4. Rechtliche Rahmenbedingung für die Datennutzung zu Forschungszwecken anpassen

A4.1. Sekundärnutzung von Forschungsdaten weiterentwickeln
Wo es nach geltendem Datenschutzrecht zulässig ist, personenbezogene Daten auf der Grundlage einer sorgfältigen Interessenabwägung auch ohne Einwilligung zu verarbeiten, wenn dies wissenschaftlichen, historischen oder statistischen Zwecken dient und für diese erforderlich ist (§ 27 BDSG n. F.), sollten im Interesse der Datensouveränität grundsätzlich entsprechende zusätzliche, prozedurale Schutz- und Gestaltungsmaßnahmen wie das Kaskadenmodell (siehe Empfehlung B2) zum Einsatz kommen.

A4.2. Rechtliche Möglichkeit für Individuen erleichtern, die umfassende Nutzung ihrer Daten für die medizinische Forschung zu erlauben („Datenspende")
Das traditionelle Einwilligungsmodell setzt für die Erhebung personenbezogener Daten prinzipiell eine enge Zweckbindung voraus. Gerade weil am

Einwilligungsmodell grundsätzlich festzuhalten ist, sind hier nicht nur prozedurale Erweiterungen, sondern auch bereichsbezogene Öffnungen sinnvoll. Namentlich sollte es erleichtert werden, im Sinne einer umfassenden Zustimmung Datennutzung ohne enge Zweckbindung zugunsten der klinischen und medizinbezogenen Grundlagenforschung zu erlauben („Datenspende"). Voraussetzung ist eine umfassende Aufklärung über mögliche Konsequenzen, insbesondere mit Blick auf die Rechte anderer, etwa mitbetroffener Familienmitglieder. Notwendig ist ferner die wissenschaftlich begleitete Entwicklung einer entsprechenden Infrastruktur für die Erfassung, Speicherung, Pflege, Verarbeitung und Weitergabe von gespendeten Daten.

A5. Digitale Entscheidungshilfesysteme in der klinischen Praxis fördern
Der wechselseitige Wissenstransfer zwischen Forschung und klinischer Praxis und die Zulassung digitaler Angebote zur Unterstützung von Entscheidungen für eine verbesserte Versorgung von Patienten sollten beschleunigt werden. Zu diesem Zweck ist für dazu legitimierte Akteure ein – unter Wahrung der Datensouveränität – möglichst umfassender Zugang zu Forschungs- bzw. Versorgungsdaten und geeigneten gesundheitsrelevanten Big-Data-Anwendungen notwendig.

A6. Internationale Anschlussfähigkeit fördern
Mit Blick auf den internationalen Austausch von Daten sollten Standardisierungsbemühungen nicht auf das nationale Territorium beschränkt bleiben. Vielmehr bedarf es weitreichender Anstrengungen auf allen Ebenen (der Politik, der Wissenschaft und Technologieentwicklung) zur Angleichung von Standards.

Um die internationale Wettbewerbsfähigkeit deutscher bzw. europäischer Digitalanwendungen im Gesundheitsbereich einschließlich der damit verbundenen hohen Qualitäts- und Datenschutzstandards zu fördern und um diesbezüglich problematischen Abhängigkeiten entgegenzuwirken, sollten zudem Investitionen im Bereich Medizininformatik deutlich höher ausfallen und schneller umgesetzt werden, als bislang geplant. Sinnvoll erscheint insbesondere eine zielgerichtete Förderung des Datenmanagements in öffentlichen Krankenhäusern.

B. Individuelle Freiheit und Privatheit sichern

Die Bereitschaft, personenbezogene Daten zur Verfügung zu stellen, ist als Teil der informationellen Freiheitsgestaltung der Datengeber zu verstehen. Deshalb müssen sie dazu befähigt werden, souverän mit diesen Daten umzugehen und ihre Privatsphäre zu gestalten. Zudem müssen die Rahmenbedingungen geschaffen werden, um entsprechend angemessene Handlungsspielräume zu garantieren.

B1. Datenhoheit bewahren

Die Bestimmungsmacht des Datengebers über die eigenen personenbezogenen Daten ist angesichts der Zweckoffenheit und Verknüpfungsmöglichkeiten von Big Data so umfassend wie möglich zu wahren.

B1.1. Programmatische Schnittstellen für Datengeber öffnen („Datenagenten“)

Insbesondere dort, wo die Datennutzung nicht vorab präzise eingegrenzt werden kann oder wenn eine Datensammlung und -verarbeitung kontinuierlich erfolgt, sollten in Ergänzung zu gängigen Zustimmungsmodellen geeignete Software-Werkzeuge („Datenagenten“) zur Verfügung gestellt werden, die die eingespeisten Daten fortdauernd nach den Vorstellungen der Datengeber verwalten und damit größere Kontrolle, Transparenz und Nachvollziehbarkeit ermöglichen. Es sollte eine Standardisierung entsprechender programmatischer Schnittstellen durch Selbstregulation oder gesetzgeberische Maßnahmen erfolgen, die die Entwicklung solcher Datenagenten erleichtert. Die korrekte Funktionsweise der Schnittstellen und Datenagenten sollte durch Auditierungs- bzw. Zertifizierungsmaßnahmen unterstützt werden.

B1.2. Mitbestimmung bei der Datenweitergabe erleichtern

Bei der Weitergabe von Daten sollte grundsätzlich die Reversibilität der Datenerhebung sichergestellt werden: Jedes System, das personenbezogene Daten sammelt und als Input akzeptiert, muss – von wohlbegründeten Ausnahmen abgesehen – in der Lage sein, diese Daten ganz oder teilweise

auch wieder zu löschen. Auch hier sollte daher ein Modell von Datenagenten, die als Kontrollinstanz in Datenpipelines integriert werden, zum Einsatz kommen. Durch geeignete Kommunikationskanäle (etwa eine entsprechende App) sollte der Datengeber nachträglich um Zustimmung zur Weitergabe ersucht werden und diese je nach Fall auch relativ einfach einschränken oder widerrufen können.

B1.3. Rechtsprobleme eines vermeintlichen Eigentums an Daten klären
Datensouveränität ist nicht mit einem „Eigentum" an Daten zu verwechseln. Soweit der Eigentumsbegriff seine wesentlichen rechtlichen Elemente impliziert – dauerhaft feste Beziehung und absolute Ausschlussmacht gegenüber Dritten –, ist er für die Zwecke der Gewährleistung von Datensouveränität wenig geeignet. Weil andererseits aber eine gewisse (allerdings flexible) Datenhoheit des Einzelnen anzuerkennen ist, ist es sinnvoll, sich stattdessen intensiver auf die rechtlichen Rahmenbedingungen der Nutzung von Daten zu konzentrieren. Der Deutsche Ethikrat empfiehlt, zu diesem Themenkomplex eine umfassende, nicht nur mit juristischem Sachverstand, sondern interdisziplinär besetzte Expertenkommission einzurichten.

B2. Kaskadisch strukturierte Einwilligungsmodelle etablieren
Grundsätzlich sollte in der klinischen Praxis und medizinbezogenen Forschung weiterhin ein einwilligungsbasiertes Regelungskonzept Verwendung finden (Opt-in-Modell). Wann immer möglich, sollten Kaskadenmodelle der persönlichen Einwilligung eingesetzt werden, die verschiedene, dynamisierte Möglichkeiten bieten, Einwilligungsentscheidungen einmalig, regelmäßig oder für jeden Entscheidungsfall neu zu treffen oder zu delegieren (etwa an unabhängige Einrichtungen/Treuhänder oder Ähnliches). Unter der Voraussetzung, dass die in der Stellungnahme entwickelten Sicherungs- und Qualitätsstandards und privatsphärenfreundliche Grundeinstellungen gewährleistet sind, sollten bereits praxiserprobte, erfolgreiche Vorbilder, insbesondere aus dem Bereich der Biobanken, auch auf andere Sektoren übertragen bzw. angepasst werden.

B3. Privatsphärenfreundliche Grundeinstellungen gewährleisten
Weil Datengeber aus Zeitmangel, fehlendem Verständnis, subjektiv empfundener Alternativlosigkeit oder aus gutem Glauben häufig die vorgegebenen Einstellungen von Daten sammelnden und Daten verarbeitenden Anwendungen übernehmen, sollten Grundeinstellungen technisch entwickelt und weiter rechtlich abgesichert werden, die von vornherein einen angemessenen Schutz der Privatsphäre bieten (*privacy by design/privacy by default*). Dies gilt insbesondere für den bislang vergleichsweise unregulierten Bereich privater Angebote, zum Beispiel gesundheitsrelevante Apps für Mobilgeräte und entsprechende Messgeräte. Über die Vorgaben der Datenschutz-Grundverordnung zu nutzerfreundlichen Einstellungen hinaus ist durch zusätzliche Aufklärung darauf hinzuwirken, dass Nutzer die Konsequenzen einer Änderung der Grundeinstellungen tatsächlich verstehen.

B4. Einsatz von Algorithmen transparent machen und erläutern
Über die rechtlich ohnehin vorgesehenen Auskunftspflichten hinaus sollten die Zielvorgaben, Funktions- und Wirkweisen der Datenakkumulation und der verwendeten Algorithmen so erläutert werden, dass sie auch für Nichtspezialisten nachvollziehbar sind. Insbesondere sollte dies – unter Berücksichtigung der jeweiligen Erfordernisse des Schutzes von geistigem Eigentum – die folgenden Aspekte umfassen:

- welche Nutzerdaten als Eingabe in welche Analysen, Vorhersagemodelle und Entscheidungs- oder Auswahlprozesse einfließen bzw. welche Attribute, etwa zur Vermeidung von Diskriminierung, ausdrücklich nicht erhoben und einbezogen werden,
- welche Ableitungen, Schlüsse, Vorhersagen, Selektionen oder Entscheidungen auf der Basis dieser Daten mittels Algorithmen getroffen werden,
- ob und inwiefern Profile des Datengebers erstellt werden und welche erwartete Aussagekraft solche abgeleiteten Größen haben,
- in welcher Form personenbezogene Daten in anonymisierter Form in (statistische) Modelle einfließen und wer über deren Nutzungsrechte verfügt.

B5. Täuschung und Manipulation entgegenwirken
Es ist zu unterscheiden zwischen offenen, transparenten Methoden der Einflussnahme auf andere einerseits und problematischeren verdeckten Eingriffen, die sich daher der kognitiven Kontrolle der Adressaten entziehen, andererseits. Eine manipulative Datengewinnung und -nutzung, die die Datengeber etwa über Art und Zweck der Erhebung täuscht und/oder ihre mangelnde Einsichtsfähigkeit ausnutzt, ist rechtlich wie moralisch unzulässig. Insbesondere in sozialen Netzwerken, bei Apps und Online-Spielen sollten nicht nur staatliche Instanzen, sondern auch die Betreiber selbst entsprechenden Tendenzen strikter entgegenwirken.

B6. Digitale Bildung fördern
Datensouveränität setzt Grundkenntnisse über die Bedeutung und den Wert von Big Data und die damit verbundenen Risiken voraus. Da bereits Kinder digitale Anwendungen nutzen und dabei Daten generieren, sollte eine entsprechende Nutzerkompetenz schon in der Schule vermittelt werden. Über die rein technischen Aspekte der gängigen Digitalisierungsstrategien schulischen Unterrichts hinaus sollte dies als Querschnittsaufgabe für alle Fächer des schulischen Curriculums ausgestaltet sein, um der gerade bei Kindern und Jugendlichen virulenten informationellen Selbstgefährdung entgegenzuwirken und schon früh ein Bewusstsein für die rechtlichen, sozialen und ethischen Implikationen zu schaffen. Die Vermittlung solcher Nutzerkompetenz sollte daher zukünftig Teil der Lehreraus- und -fortbildung werden. Einrichtungen der Erwachsenenbildung sollten zudem kontinuierlich niedrigschwellige Angebote für alle Altersgruppen vorhalten. Auch Unternehmen und Institutionen sollten regelmäßig entsprechende interne Schulungen durchführen.

B7. Diskurs und Teilhabe stärken
Die kontinuierliche öffentliche Debatte über Big Data sollte stärker gefördert werden. Dafür sollten staatlicherseits verlässliche Informationen zur Verfügung gestellt und partizipative Verfahren etabliert werden. Diese sollten eine breite Beteiligung der Öffentlichkeit und einen Austausch mit der Fachwelt gewährleisten.

C. Gerechtigkeit und Solidarität sichern

C1. Fairen Zugang zu digitalen Angeboten schaffen
Von den Vorteilen der Digitalisierung sind manche Nutzergruppen regelmäßig ausgeschlossen, etwa aufgrund von Bildungshemmnissen. Um dem entgegenzuwirken, bedarf es nicht nur spezieller Informations- und Bildungsangebote, sondern es ist auch Sorge dafür zu tragen, dass digitale Angebote nicht von vornherein so konzipiert werden – zum Beispiel durch unverständliche, unnötig komplizierte Handhabung oder unnötig technische Sprache – dass sie exklusiv wirken. Software und Nutzeroberflächen sollten möglichst barrierefrei gestaltet werden.

C2. Diskriminierung und Stigmatisierung aufdecken bzw. verhindern
Es ist sicherzustellen, dass eine über Big Data erweiterte Entscheidungsbasis für gesundheitsrelevante Allokationsentscheidungen nicht dazu missbraucht wird, Personen oder Personengruppen zu diskriminieren oder zu stigmatisieren. Bei der Verwendung von Erkenntnissen aus Big-Data-Analysen besteht eine Gefahr darin, dass die zugrunde liegenden Daten, die gewählten Randbedingungen der Analyse und angewandten Algorithmen zu Ergebnissen führen können, die eine systematische und nur schwer erkennbare Diskriminierung von Personen oder Gruppen nach sich ziehen. Deshalb ist nicht nur vorab auf die Unzulässigkeit entsprechender Selektionskriterien ohne klare und angemessene Zweckbestimmung hinzuweisen, sondern es sind auch Verfahren zu entwickeln, mit denen eventuelle Verstöße aufgezeigt und sanktioniert werden können. Auch wenn hierfür sektor- bzw. institutioneninterne, subsidiäre Regelwerke durchaus sinnvoll sind, muss es darüber hinaus aber auch justiziable, sanktionsbewehrte hoheitliche Sicherungsmechanismen geben.

C3. Widerspruch bei automatisierten Entscheidungen ermöglichen
Bei algorithmenbasierten Entscheidungen bedarf es strukturierter Widerspruchsmöglichkeiten. Speziell im Bereich privater Versicherungen muss für abgelehnte Antragsteller der Anspruch auf eine für sie verständliche, individuelle Begründung der Ablehnung garantiert sowie ein kostenfreier

und niederschwelliger Zugang zu internen und externen Beschwerde- und Schlichtungsinstanzen sichergestellt werden.

C4. Vulnerable Gruppen und Individuen schützen

Besondere Aufmerksamkeit erfordern Personen und Gruppen, die aufgrund individueller oder sozialer Umstände (gegebenenfalls vorübergehend) besonders anfällig dafür sind, dass ihnen mittelbar oder unmittelbar, strukturell oder intentional die Vorteile einer Digitalisierung des Gesundheitssektors vorenthalten oder die Nachteile im Übermaß aufgebürdet werden. Dies gilt in besonderem Maße für Kinder und Jugendliche sowie Menschen mit Behinderung und ältere Menschen. Sie sind nicht nur mit Blick auf den Erwerb der Fähigkeit zur verantwortungsvollen Inanspruchnahme digitaler Dienste zu unterstützen, sondern müssen in ihrer spezifischen Vulnerabilität auch im Prozess der Datensammlung und -verwendung besonders geschützt werden. Datensouveränität berücksichtigt insoweit auch die keineswegs fixe, sondern individuell und situationsbedingt variierende Verantwortungsfähigkeit der Betroffenen.

C4.1. Einwilligungserfordernisse bei Kindern und Jugendlichen streng beachten

Die Vorgaben der Datenschutz-Grundverordnung zu Einwilligungen von Minderjährigen in Bezug auf Dienste der Informationsgesellschaft sollten strikt und zügig umgesetzt werden. Über die von der Datenschutz-Grundverordnung zugelassene Möglichkeit, das Mindestalter abzusenken, sollte nicht entschieden werden, ohne die Betroffenen (Kinder und Jugendliche) zu beteiligen.

C4.2. Schutzmechanismen für die Datenerhebung an sonstigen Personen mit eingeschränkter Einwilligungsfähigkeit entwickeln

Für die Datenerhebung an sonstigen Personen mit eingeschränkter Einwilligungsfähigkeit sollten besondere Schutzmechanismen entwickelt werden, ohne damit die Chancen einer Big-Data-basierten Forschung mit diesen Personen und zu deren Gunsten zu unterbinden. Die beteiligten Forschungsinstitutionen sollten sicherstellen, dass entsprechend dem

Konzept der Entscheidungsassistenz den betroffenen Menschen selbst, ihrer Einsichtsfähigkeit gemäß, und ihren Betreuungspersonen hinreichende Informationen zur Entscheidungsfindung an die Hand gegeben werden.

C4.3. Einsatz von Chatbots restriktiv regeln
Der Einsatz von Chatbots zur Datenerhebung an Personen mit eingeschränkter Einsichtsfähigkeit bietet ein besonders hohes Manipulationspotenzial und sollte daher besonders restriktiv geregelt werden.

C5. Zuwendungsorientierte Medizin gewährleisten
Die persönliche Zuwendung zum Patienten in der medizinischen Praxis sollte durch den Einsatz von Big-Data-Anwendungen nicht geschwächt, sondern gestärkt werden. Zeitliche und finanzielle Kapazitäten, die etwa durch die Entlastung des versorgenden Personals von Routine-Tätigkeiten oder die schnellere und präzisere Diagnostik durch digitale Algorithmen frei werden, sollten in mehr persönliche Zuwendung für Patienten umgesetzt werden.

C6. Wirksame Haftung von Unternehmen, die im Gesundheitsbereich mit Daten arbeiten, sicherstellen
Angesichts der mit Big Data verbundenen Risiken erscheint es angemessen, speziell hierauf zugeschnittene Haftungsmodelle zu entwickeln. Hier ist zunächst genau zu beobachten, ob und inwieweit die neuen Regelungen des deutschen Datenschutzrechts, die die Möglichkeiten der europäischen Datenschutz-Grundverordnung (DSGVO) bislang nicht ausschöpfen, ausreichen. Die DSGVO eröffnet die Möglichkeit, für einen effektiven Schutz von Personen vor Schädigung die Gefährdungshaftung einzuführen. Angesichts der Unsicherheiten der Haftung und der Beweisregelung ist eine derartige, auf die spezifischen Risiken von Big Data zugeschnittene Gefährdungshaftung zu erwägen. Diese Haftung sollte unabhängig von der Befugnis der Verwendung nur dann ausgeschlossen sein, wenn der Schaden unvermeidbar ist. Eine eventuelle summenmäßige Begrenzung der Haftung sollte so hoch sein, dass sie auch gegenüber großen Unternehmen spürbare Wirkung entfaltet.

D. Verantwortung und Vertrauen fördern

D1. Schutz- und Qualitätsstandards garantieren

D.1.1. Bestmögliche Schutzstandards gegen unbefugte Identifizierung von Individuen aus anonymisierten, pseudonymisierten oder aggregierten Datensätzen etablieren

Angesichts der unzureichenden Schutzeffekte der traditionellen Anonymisierung und Pseudonymisierung sollten angemessene ergänzende Schutzstandards etabliert werden, um die Hürden für eine Reidentifizierung zu erhöhen:

- Wo Identifikatoren einen relativ unmittelbaren Rückschluss auf die jeweilige Person erlauben (E-Mail, Login, Geräte-ID, Cookie-ID), sind diese durch anonymisierte Schlüssel zu ersetzen, deren Lebensdauer möglichst kurz zu halten ist.
- Wenn immer ein anonymer Nutzer sich unerwartet oder versehentlich direkt oder indirekt identifiziert, hat der Datensammler Sorge zu tragen, dass die Identifizierung durch Datenlöschung rückgängig gemacht wird (versehentliche Preisgabe von Namen, E-Mail, Telefonnummern, Kreditkartennummer, Ausweisnummer usw.).
- Wo immer ein Datensatz durch die Kombination von Attributen und Daten einen Nutzer mit hoher Wahrscheinlichkeit identifizierbar macht, sind auf jenen die gleichen datenschutzrechtlichen Maßnahmen anzuwenden wie bei expliziten Identifikatoren.
- Datensätze, deren Verbindung eine entsprechende Schutznivellierung mit sich bringt, müssen getrennt gehalten werden oder dürfen nur „flüchtig“ (das heißt ohne persistent in Datenbanken gespeichert zu werden) für wohldefinierte Zwecke verknüpft werden.

D.1.2. Anonymisierungsdefizite durch kontrollierten Zugang zu Daten kompensieren

Angesichts des verbleibenden Reidentifizierungsrisikos kommt der Kontrolle des Datenzugriffs besondere Bedeutung zu. Insbesondere in der klinischen Praxis und der medizinbezogenen Grundlagenforschung ist daher

der Zugang zu Daten durch Aufbewahrung von gesundheitsrelevanten Daten in sicheren, technisch getrennten und voneinander unabhängigen Repositorien und die Etablierung kontrollierter Zugangswege, einschließlich robuster Verifikations- und Authentifizierungssysteme, angemessen auf befugte Akteure zu beschränken.

D.1.3. Umsetzung von Schutzvorgaben gewährleisten und nachweisen
Datensouveränität setzt ein Miteinander von technischen und regulatorischen Standards voraus. In Anknüpfung an existierende Vorgaben zu *privacy by design* sollten Datenverarbeiter und Datennutzer noch stärker darauf achten, dass schon in der Planungs- und Entwicklungsphase datenschutzbezogene Erwägungen oberste Priorität besitzen. Es sollte zudem den betroffenen Einrichtungen (in der Forschung, in der medizinischen Praxis, oder im kommerziellen Bereich) obliegen, für ihren Verantwortungsbereich die Übereinstimmung mit den Datensouveränität sichernden Vorgaben nachzuweisen. In Anknüpfung an die diesbezüglich bestehenden Erfahrungen mit internen Datenschutzbeauftragten lässt sich deren Aufgaben- und Befugnisprofil sinnvoll in diese Richtung (*corporate data governance*) weiterentwickeln.

D1.4. Informationspflicht bei Pannen und Fehlverhalten etablieren
Es ist darauf zu achten, dass mögliche Pannen oder Fehlverhalten nicht verborgen bleiben, sondern in ihrer Relevanz für das Gesamtsystem verstanden und produktiv als Lerneffekt genutzt werden. Deshalb bedarf es einer entsprechenden Informationspflicht gegenüber den potenziell geschädigten Nutzern und – sofern diese nicht zu ermitteln sind – der Öffentlichkeit, sowie einer Meldepflicht gegenüber den Aufsichtsbehörden/-gremien.

D2. Kontrollmechanismen verbessern

D2.1. Datenschutzbeauftragte stärken
Zur Sicherstellung von Datensouveränität bedarf es einer Vielzahl interner (privater) und externer (hoheitlicher) Kontrollstellen. Deren Zuständigkeiten sollten genauer abgegrenzt und gegebenenfalls ihre Kapazitäten und

Kompetenzen erweitert werden. Insbesondere ist es sinnvoll und geboten, die Tätigkeit der bestehenden Datenschutzbeauftragten – und zwar sowohl im öffentlichen wie im privaten Bereich – in Richtung Datensouveränität neu zu justieren und gegebenenfalls auszuweiten. Sie sollten die Arbeit von lokalen Kontrollinstanzen, wie etwa Forschungsethikkommissionen, ergänzen und auf der Grundlage transparenter Entscheidungskriterien in Konfliktsituationen moderierend und schlichtend wirken. Soweit sich die existierenden Kontrollstrukturen gegenüber den spezifischen Problemen von Big Data als unzulänglich erweisen, beispielsweise bei überregionalen und internationalen Verbundprojekten, ist eine stärkere Zentralisierung zu erwägen.

D2.2. Datenprüfer etablieren
Gerade mit Blick auf die als gesamtgesellschaftlich bedeutsame Datenqualität, insbesondere in der medizinbezogenen Forschung und klinischen Praxis, sollte eine entsprechende Prüfstruktur etabliert werden. Diese muss nicht notwendig rein hoheitlicher Natur sein, sondern ließe sich – etwa analog zum Abschlusswesen und zur Rechnungslegung im Gesellschaftsrecht – auch als private Regulierung konzipieren.

D2.3. Datentreuhandmodelle einführen
Um Vertrauen zu fördern und Missbrauch zu verhindern, sollten Datenverwender die technischen und organisatorischen Voraussetzungen dafür schaffen, dass Datenbestände nicht unmittelbar an sie selbst übergeben werden müssen, sondern Treuhandmodelle (zum Beispiel gemeinnützige Stiftungen) zwischengeschaltet werden können. Das kann nicht nur Machtungleichgewichte verringern, sondern auch Interessenkollisionen entgegenwirken. Zumindest im Bereich der medizinbezogenen Forschung und klinischen Praxis sollte politisch darauf hingewirkt werden, dass solche Modelle insbesondere auch in Bezug auf Datenverwender im internationalen Kontext (zum Beispiel Google, Apple, Facebook, Amazon und Microsoft) wirksam werden.

D3. Kodizes für Forschung, Klinik und Wirtschaft erarbeiten
Nach dem Vorbild bereits existierender Selbstverpflichtungen sollte konsequent weiter darauf hingewirkt werden, in allen datenschutzsensiblen Bereichen umfassende interne Verhaltensstandards zu etablieren. Dabei gilt es nicht nur die jeweiligen regulatorischen Vorgaben aufzunehmen und gegebenenfalls zu intensivieren, sondern auch – zumindest branchenintern oder mit Blick auf spezifische Anwendungsfelder – internationale Abstimmungen und Harmonisierungen anzustreben.

D4. Gütesiegel für Anbieter und Anwendungen unterstützen und ausbauen
Da eine besondere Berücksichtigung der Datensouveränität auch und gerade im Interesse der Datenverwender liegt, sollten entsprechende marktbasierte, teilweise bereits existierende Klassifizierungen („Gütesiegel") unterstützt und ausgebaut werden. Über Mindeststandards setzende, zwingende gesetzliche Vorgaben hinausgehende Bemühungen können auf diese Weise zum profilbildenden Wettbewerbsfaktor avancieren. Soweit diese selbstregulativen Mechanismen sich als unzureichend erweisen, sind Koregulierungsmaßnahmen – etwa in Form von Zertifizierungen – einzubeziehen und die staatlichen Kontrollstrukturen einschließlich Haftungsregelungen zu verstärken.

D5. Kompetenz im verantwortungsvollen Umgang mit Daten für alle, die professionell mit Big Data zu tun haben, stärken
In Tätigkeitsfeldern, in denen Big Data rapide zunimmt, muss das Bewusstsein für die ethischen Herausforderungen und für die neuen Verantwortlichkeiten, die sich aus der Nutzung gesundheitsrelevanter Daten ergeben, befördert werden. Für einen solchen Kulturwandel ist bei allen Beteiligten ein besseres Verständnis von Forschungs- und Datenethik sowie wissenschaftstheoretische Reflexionskompetenz erforderlich. Die Förderung solcher Kompetenzen sollte daher verpflichtendes Element in der Aus-, Fort- und Weiterbildung in allen relevanten Fächern und Bereichen werden. Um der Komplexität und Bedeutung des Themas gerecht zu werden, könnten beispielsweise verstärkt betriebs- und institutionenintern Data-Science-Fachabteilungen eingerichtet werden.

>> SONDERVOTUM

In einem Sondervotum fordert Christiane Fischer den Verzicht auf die Nutzung von Big Data zu Forschungszwecken oder anderen Anwendungen, sofern ein umfassender Datenschutz, die Umsetzung effektiver Anonymisierungs- und Pseudoanonymisierungsstandards und das Recht auf Vergessen nicht gewährleistet werden können.

Mitglieder des Deutschen Ethikrates

Prof. Dr. theol. Peter Dabrock (Vorsitzender)
Prof. Dr. med. Katrin Amunts (Stv. Vorsitzende)
Prof. Dr. phil. Dr. h. c. Dipl.-Psych. Andreas Kruse (Stv. Vorsitzender)
Prof. Dr. med. Claudia Wiesemann (Stv. Vorsitzende)

Constanze Angerer
Prof. Dr. iur. Steffen Augsberg
Prof. Dr. theol. Franz-Josef Bormann
Prof. Dr. med. Alena M. Buyx
Prof. em. Dr. iur. Dr. h. c. Dagmar Coester-Waltjen
Dr. med. Christiane Fischer
Prof. em. Dr. phil. habil. Dr. phil. h. c. lic. phil. Carl Friedrich Gethmann
Prof. Dr. rer. nat. Dr. phil. Sigrid Graumann
Bischof Prof. Dr. theol. Martin Hein
Prof. Dr. med. Wolfram Henn
Prof. Dr. iur. Wolfram Höfling
Prof. Dr. (TR) Dr. phil. et med. habil. Ilhan Ilkilic
Prof. Dr. rer. nat. Ursula Klingmüller
Stephan Kruip
Prof. Dr. phil. Adelheid Kuhlmey
Prof. Dr. med. Leo Latasch
Prof. Dr. iur. Dr. h. c. Volker Lipp
Prof. Dr. theol. Andreas Lob-Hüdepohl
Prof. em. Dr. iur. Reinhard Merkel
Prof. Dr. phil. Gabriele Meyer
Prof. Dr. med. Elisabeth Steinhagen-Thiessen
Dr. phil. Petra Thorn

Mitarbeiterinnen und Mitarbeiter der Geschäftsstelle

Dr. rer. nat. Joachim Vetter (Leiter)
Dr. theol. Katrin Bentele
Carola Böhm
Malica Christ
Ulrike Florian
Dr. phil. Thorsten Galert
Steffen Hering
Christian Hinke
Petra Hohmann
Torsten Kulick
Dr. Nora Schultz