}essentials{

Patrik Hummel · Matthias Braun
Steffen Augsberg ·
Ulrich von Ulmenstein ·
Peter Dabrock

Datensouveränität

Governance-Ansätze für den Gesundheitsbereich

OPEN ACCESS

Springer VS

essentials

essentials liefern aktuelles Wissen in konzentrierter Form. Die Essenz dessen, worauf es als „State-of-the-Art“ in der gegenwärtigen Fachdiskussion oder in der Praxis ankommt. *essentials* informieren schnell, unkompliziert und verständlich

- als Einführung in ein aktuelles Thema aus Ihrem Fachgebiet
- als Einstieg in ein für Sie noch unbekanntes Themenfeld
- als Einblick, um zum Thema mitreden zu können

Die Bücher in elektronischer und gedruckter Form bringen das Fachwissen von Springerautor*innen kompakt zur Darstellung. Sie sind besonders für die Nutzung als eBook auf Tablet-PCs, eBook-Readern und Smartphones geeignet. *essentials* sind Wissensbausteine aus den Wirtschafts-, Sozial- und Geisteswissenschaften, aus Technik und Naturwissenschaften sowie aus Medizin, Psychologie und Gesundheitsberufen. Von renommierten Autor*innen aller Springer-Verlagsmarken.

Weitere Bände in der Reihe http://www.springer.com/series/13088

Patrik Hummel · Matthias Braun ·
Steffen Augsberg ·
Ulrich von Ulmenstein · Peter Dabrock

Datensouveränität

Governance-Ansätze für den Gesundheitsbereich

Springer VS

Patrik Hummel
Lehrstuhl für Systematische Theologie II (Ethik)
Friedrich-Alexander-Universität
Erlangen-Nürnberg
Erlangen, Deutschland

Matthias Braun
Lehrstuhl für Systematische Theologie II (Ethik)
Friedrich-Alexander-Universität
Erlangen-Nürnberg
Erlangen, Deutschland

Steffen Augsberg
Professur für Öffentliches Recht
Justus-Liebig-Universität Gießen
Gießen, Deutschland

Ulrich von Ulmenstein
Professur für Öffentliches Recht
Justus-Liebig-Universität Gießen
Gießen, Deutschland

Peter Dabrock
Lehrstuhl für Systematische Theologie II (Ethik)
Friedrich-Alexander-Universität
Erlangen-Nürnberg
Erlangen, Deutschland

ISSN 2197-6708 ISSN 2197-6716 (electronic)
essentials
ISBN 978-3-658-33754-4 ISBN 978-3-658-33755-1 (eBook)
https://doi.org/10.1007/978-3-658-33755-1

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Planung/Lektorat: Jan Treibel
Springer VS ist ein Imprint der eingetragenen Gesellschaft Springer Fachmedien Wiesbaden GmbH und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Was Sie in diesem *essential* finden können

- Eine Untersuchung des Begriffs der Datensouveränität sowie der mit ihm verknüpften rechtlichen und moralischen Ansprüche
- Analysen zum Dynamic Consent als Umsetzungsmechanismus von Datensouveränität
- Governance-Empfehlungen für die Ermöglichung von Datensouveränität

Im vorliegenden Dokument werden wir zwischen den unterschiedlichen Geschlechterbenennungen wechseln. Die anderen Geschlechter sind jeweils in gleicher Weise mitgemeint.

Dieses *essential* ist im Rahmen des vom Bundesgesundheitsministerium geförderten Drittmittelprojekts „Datensouveränität in klinischen Big-Data-Regimes“ (DABIGO ZMV/1 – 2517 FSB 013) entstanden. Der Förderer hatte keinen Einfluss auf Inhalte, Analysen und Ergebnisse des vorliegenden *essentials.*

Einleitung

Souveränität ist ein häufig verwendeter Begriff, wenn es um die Analyse und Gestaltung digitaler Prozesse und Veränderungen geht. So hat beispielsweise die deutsche EU-Ratspräsidentschaft 2020 digitale Souveränität zu einem ihrer Leitbegriffe erklärt [1]. Andere sprechen von Souveränität im Umgang mit Daten, von Souveränität im Cyberspace oder auch von virtueller Souveränität. Bei allen Unterschieden im Detail lässt sich ein zentraler gemeinsamer Fokus ausmachen: Wie können in digitalen Gesellschaften Freiheitsräume gesichert und fortentwickelt werden?

Daten spielen hierbei eine zentrale Rolle. Das zeigt sich anschaulich im Gesundheitsbereich. Ob Tracing Apps im Rahmen der Pandemiebekämpfung, elektronische Patientenakten oder die medizinische Diagnostik unterstützende Gesundheits-Apps: Es besteht ein grundlegendes rechtliches und ethisches Spannungsverhältnis. Denn auf der einen Seite dienen solche Anwendungen dem Gesundheits- und Lebensschutz. Gesundheitsdaten zu analysieren und zu verwenden, trägt in dieser Perspektive gerade zu einem selbstbestimmten Leben bei. Auf der anderen Seite können mit den aus Daten gewonnenen Erkenntnissen negative, freiheitsbeeinträchtigende Konsequenzen verbunden sein.

Die sich hieraus ergebenden ethischen, rechtlichen und gesellschaftlichen Herausforderungen werden nachfolgend untersucht und es werden konkrete Handlungsvorschläge unterbreitet. Als Referenzpunkt für dieses Analyse-, Gestaltungs- und Regelungskonzept schlagen wir den Begriff der Datensouveränität vor. Wir verwenden den Begriff pragmatisch-konstruktiv. Wir beschreiben und untersuchen, wie ein weiterentwickeltes Konzept informationeller Selbstbestimmung verstanden und umgesetzt werden kann. Ziel ist es, auch in Zeiten von Big Data und Künstlicher Intelligenz (KI) ein angemessenes Verhältnis von Privatheit und Offenheit sicherzustellen. Vor dem Hintergrund dieser Zielsetzung werden

Governance-Ansätze zur praktischen Umsetzung von Datensouveränität unter den Bedingungen von Big-Data und KI entwickelt.

Zu diesem Zweck wird zunächst in Kap. 1 untersucht, was genau mit einem souveränen Umgang mit Daten gemeint sein kann. Wir untersuchen, welche Vorstellungen, aber auch welche rechtlichen und moralischen Ansprüche artikuliert werden, wenn von Souveränität im Umgang mit Daten die Rede ist. Diese Vorstellungen und Ansprüche werden nicht in einem luftleeren Raum diskutiert, sondern sind an bestimmte grundrechtliche Vorgaben und werthaltige Vorstellungen gekoppelt. Wir werden begründen, warum und inwiefern Datensouveränität an die Bewahrung, Gestaltung und Ermöglichung von Freiheit gebunden sein muss.

In Kap. 2 argumentieren wir, dass der gebotene Ausgleich von Privatheit und der gemeinschaftlichen Nutzung von Daten unter Bedingungen von Big Data und KI funktional über dynamische Einwilligungs- und Kontrollmöglichkeiten zu erreichen ist. Wir plädieren also dafür, bestehende Schutzkonzepte nicht aufzugeben, sondern kontextadäquat weiterzuentwickeln.

Den konzeptionellen Überlegungen zur Datensouveränität und ihrer Umsetzung folgt in Kap. 3 ein Vorschlag für Governance-Ansätze für den Gesundheitsbereich. Hier entwickeln wir Empfehlungen auf den vier Ebenen von Hard Law, Soft Law, Teilhabe und IT.

Inhaltsverzeichnis

Datensouveränität als informationelle Freiheitsgestaltung

1

1.1 Souveränität im digitalen Raum

Daten können die Grundlage für nutzenbringende Innovationen und technologischen Fortschritt sein. Intensive Datennutzung und automatisierte Entscheidungsfindung können jedoch in Spannung zu den Rechten und Interessen der sie betreffenden Individuen stehen. In den vergangenen Jahren tritt Souveränität als Leitkonzept im Kontext der Digitalisierung immer häufiger in Erscheinung [2, 3]. So werden beispielsweise Forderungen nach Digitaler Souveränität [4] und Datensouveränität [5, 6] laut.

Die Begriffsverwendung ist dabei nicht immer einheitlich. Eine ganze Reihe von Konnotationen, Ansprüchen und Zielsetzungen werden unter dem Schlagwort Souveränität in digitalen Räumen verhandelt. Meist ist jedoch die Kontrolle von Daten, Zugang, Verarbeitung und Infrastrukturen zumindest mit angesprochen. Souverän können in diesem Sinne sowohl Nationen als auch Individuen sein. So wird Souveränität im Zusammenhang mit dem Versuch staatlicher Regulierung des Internets [7] ebenso wie mit Gesundheitsdaten von Individuen [6] thematisiert. In Cloud-Anwendungen geht es bei Datensouveränität um die räumliche Lokalisierung von Daten [8] und das Wissen um die damit verbundenen rechtlichen Rahmenbedingungen [9], beispielsweise zum Zugriff Dritter und/oder staatlicher Institutionen – mit Implikationen für die nationale Sicherheit, wenn staatliche Organisationen Cloud-Anwendungen nutzen [10].

In einer systematischen Studie haben wir untersucht, was unter dem Begriff der Datensouveränität verstanden wird, welche normativen Ansprüche welcher Akteure verhandelt werden und welche Herausforderungen sich dadurch stellen [11]. Über die unterschiedlichen Publikationen hinweg ist auffällig, dass sehr unterschiedliche Akteurinnen als potentiell datensouverän verstanden werden: von

P. Hummel et al., *Datensouveränität,* essentials,
https://doi.org/10.1007/978-3-658-33755-1_1

Konsumenten über bestimmte Populationen bis hin zu Ländern. Ebenso vielfältig sind die Kontexte, in denen Datensouveränität diskutiert wird. Sie umfassen die Gestaltung von IT-Systemen ebenso wie Gesetzgebung und Forschung. In diesen Kontexten werden im Zusammenhang mit Datensouveränität Aspekte wie Kontrolle und Macht, Privatheit, Deliberation, Partizipation und weitere normative Konzepte thematisiert. Schon bei der basalen Frage, um was es sich bei Datensouveränität eigentlich handelt, variieren die Bestimmungen der Autorinnen meist stillschweigend und ohne explizite Sichtbarmachung oder Auseinandersetzung mit alternativen Ansätzen: Um nur wenige Beispiele zu nennen, wird Datensouveränität als ein Recht oder Anspruch des Akteurs, als eine Fähigkeit oder als aus Gesetzgebung resultierender Zustand begriffen.

Auch außerhalb des Kontexts der Digitalisierung ist Souveränität ein schillerndes und kontrovers diskutiertes Konzept. In der Ideengeschichte ist sie immer mit Machtansprüchen verbunden, wobei sie vor allem in der Politischen Theorie Staaten zugeschrieben wird. Autoren weisen ferner auf die Fiktionen und Imaginationsprozesse hin, die mit der Zuschreibung von Souveränität und der mit ihr einhergehenden Macht und Repräsentation verbunden sind [12]. So ist der Souverän auf dem Frontispiz von Hobbes' *Leviathan* aus seinen Untertanen zusammengesetzt. Seine Macht leitet sich aus einem Moment der Stellvertretung der Untertanen ab. Zuweilen wird bezweifelt, ob Souveränität ein fruchtbares Konzept für politische Diskurse sein kann, weil sie einen vermeintlich unwiederbringlichen Machttransfer zwischen Volk und Souverän reflektiert [13]. Eine weitere Kontroverse betrifft die Frage, ob Souveränität spannungsfrei mit transnationaler Integration, z. B. in der Europäischen Union [14], zusammengedacht werden kann, welche die Souveränität einzelner Staaten prima facie beschneidet.

Unter anderem in den Vereinigten Staaten, Kanada und Australien wird Datensouveränität im Umgang mit Daten von Angehörigen indigener Völker diskutiert. *Indigenous Data Sovereignty* [15] hat mit den soeben skizzierten Verwendungen von Datensouveränität gemein, dass die Kontrolle über die Erhebung, Analyse und Interpretation von Daten zentral ist. Besonders auffallend ist dabei, dass *Indigenous Data Sovereignty* als die Erweiterung bzw. Spezifizierung eingeforderter oder bereits vollzogener, rechtlich verbindlicher Formen von Anerkennung indigener Gemeinschaften, Völker und/oder Nationen verstanden wird [16–19].

Wohlwissend um die variierenden Hintergründe und Verständnisse des Begriffs in der Literatur werden wir einen spezifischen Fall von Datensouveränität in den Blick nehmen und entfalten: die Datensouveränität von Patientinnen im deutschen Gesundheitswesen.

1.2 Datensouveränität

Souveränität beinhaltet Ansprüche auf Macht und Kontrolle, die an wechselseitigen Zuschreibungen und Anerkennungsverhältnissen anknüpfen. Unter Datensouveränität verstehen wir im Folgenden die Souveränität von Akteuren über die Verwendung von Daten. Datensouverän sind diese Akteure dann, wenn sie zur Ausübung von Kontrollansprüchen rund um die Verwendung sie betreffender Daten befähigt sind. Für datensouveräne Akteure soll kontrollierbar bleiben, wer Zugriff auf diese Daten hat, zu welchen Zwecken sie von wem verarbeitet werden dürfen, und vor allem wie Zugang und Verarbeitung die Freiheitsvollzüge der Akteure beeinflussen. Datensouveränität umfasst dabei folgende Aspekte (siehe Abb. 1.1):

- *Normativität:* Als normatives Ankerkonzept ist Datensouveränität mit der Forderung verbunden, datenverarbeitende Technologien und deren Anwendung so zu gestalten, dass Datensouveränität der betroffenen Akteure ermöglicht wird.
- *Individualfokus:* Datensouverän können sowohl Individuen als auch Organisationen oder Kollektive sein. Im Folgenden beschäftigen wir uns mit der Datensouveränität von *Individuen.*
- *Grundrechtsbezug:* Wie Souveränität kann auch Datensouveränität eingefordert, zugesprochen, anerkannt und kritisiert werden. Bezugspunkte für die Bewertung solcher individuellen Ansprüche sind im vorliegenden Kontext die Grundrechte, insbesondere das allgemeine Persönlichkeitsrecht und das Recht auf informationelle Selbstbestimmung.
- *Kontrollierbarkeit:* Datensouveränität schließt ein, Daten schützen und Rückwirkungen auf individuelle Freiheit unterbinden zu können, erschöpft sich darin jedoch nicht. Sie schließt ferner ein, dass das Individuum Daten gemäß seinen Präferenzen teilen und für Datenverarbeitung freigeben kann. Solche Entscheidungen können sowohl aus Eigeninteresse erfolgen als auch auf ein Gemeinwohl abzielen.
- *Multidimensionalität:* Datensouveränität von Individuen hängt von einer ganzen Reihe von Governance-Mechanismen ab, die später auf den vier Ebenen Hard Law (3.1), Soft Law (3.2), Teilhabe (3.3) und IT (3.4) behandelt werden.

Datensouveränität bezeichnet in diesem Sinne die individuelle Kontrollierbarkeit von Daten und deren Verarbeitung: die Möglichkeit und Befähigung zu steuern, wer Zugang hat, wofür Daten verarbeitet werden und welche Konsequenzen sich auf die Freiheitsräume des Individuums ergeben. Diese Freiheitsräume sind nicht

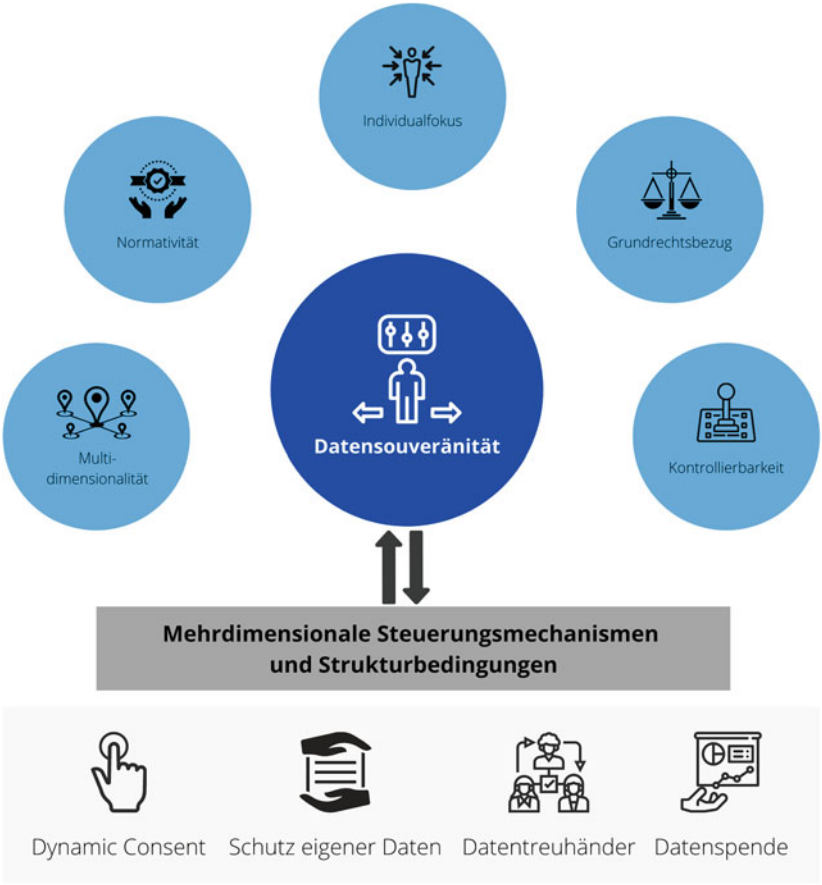

Abb. 1.1 Fokus und Dimensionen von Datensouveränität

einfach vorhanden, sondern müssen eben gerade im digitalen Raum aufrechterhalten, gestaltet und mitunter verteidigt werden. Als zentrales Element der Sicherung individueller Freiheitsräume bedarf es der konkreten Möglichkeit, Kontrolle über Rückschlüsse und Rückwirkungen aus der Nutzung, Analyse und Prädiktion von Daten zu haben. Warum eine solche Kontrolle geboten ist, wie sie verstanden und nicht zuletzt wie sie einer Gestaltung zugeführt werden kann, wird zentraler Gegenstand dieser Analyse sein.

1.3 Die Probleme der aktuellen Input-Orientierung von informationeller Selbstbestimmung

Ein etablierter Mechanismus zur Wahrung von individuellen Freiheitsräumen ist der Datenschutz. Allerdings ist ein zentrales Problem, dass angesichts der Funktionsweisen und Prinzipien von Big-Data-Anwendungen und KI ausschließlich *input-orientierte* Datenschutzprinzipien die Kontrollierbarkeit von Datenverarbeitung nicht mehr sicherstellen können. Mit *Input*-Orientierung ist gemeint, dass diese Prinzipien am Beginn von Datenverarbeitungsprozessen ansetzen. Willigt das Individuum zum Beispiel im Wissen um den Zweck der Verarbeitung seiner personenbezogenen, medizinischen Daten ein, so können diese Daten verarbeitet werden (Art. 9 Abs. 2 Nr. 1 DSGVO). Das Beispiel rückt mindestens drei Bezugspunkte in den Mittelpunkt, an welchen *input-orientierte* Datenschutzprinzipien ansetzen: erstens der *Zweck* der Verarbeitung, zweitens die *Sensibilität* der Daten (hier: Gesundheitsdaten) und drittens der *Personenbezug*. Alle drei sind jedoch problembehaftet.

Erstens können Verarbeitungs*zwecke* in Big-Data-Anwendungen allenfalls grob umrissen werden. Ein Spezifikum von Big Data ist das Zusammenführen sowie die De- und Rekontextualisierung von Daten, um unvorhergesehene Bezüge [20] zu erkennen.

Zweitens sind Gesundheitsdaten eine fluide und *a priori* kaum eingrenzbare Kategorie geworden. Big Data und KI basieren darauf, Daten verschiedener Sphären zusammenzuführen. So erlauben beispielsweise Tracing Apps Rückschlüsse auf ein Gesundheitsrisiko auf Basis der systematischen Analyse von Daten, die für sich genommen keine oder allenfalls begrenzte medizinische Aussagekraft haben, beispielsweise Aufenthalts- und Bewegungsdaten.

Drittens ist auch *Personenbezug* ein unscharfes Kriterium geworden. Durch die Zusammenführung von Datensätzen können auch zunächst nicht-personenbezogene Daten einen Personenbezug erlangen. Paradigmatisch sei hier die Forschung von Latanya Sweeney angeführt, die bereits 2000 – also weit vor der heutigen Akzeleration und Vertiefung digitaler Verarbeitung – zeigen konnte, dass 87 % der Einwohner der Vereinigten Staaten durch die Kombination von Postleitzahl, Geschlecht und Geburtsdatum eindeutig individuiert werden können [21]. Unter Big-Data- und KI-Bedingungen sind Re-Personalisierungen noch wahrscheinlicher, da mehr Daten aus den verschiedensten Kontexten zugänglich werden und miteinander in Beziehung gesetzt werden können [22].

Von dieser Möglichkeit ganz abgesehen ist ferner zu berücksichtigen, dass nicht-personenbezogene Daten in aggregierter Form die Generierung von Hypothesen über Populationen erlauben. Korrelationsmuster können auf diese Weise

generiert werden, *ohne* dass personenbezogene Daten notwendig sind. Sobald ein Individuum jedoch der Population zugeordnet wird, kann es selbst auch im Lichte dieser Hypothesen betrachtet werden. Aus diesem Grund fordern Autoren neben der Privatheit von Individuen auch *Gruppen-Privatheit* als genuine, nicht auf individuelle Privatheit reduzierende Kategorie in den Fokus zu rücken [23, 24]. Dies zeigt: Einwilligung beim Input *personenbezogener* Daten zu fordern, greift zu kurz.

Traditionelle Datenschutzprinzipien stehen vor von ihnen nicht mehr zu bewältigenden Herausforderungen. Wenn beispielsweise auch von nicht-personenbezogenen und/oder nicht-gesundheitsbezogenen Daten Rückschlüsse auf die Gesundheit von Einzelpersonen wie auch Populationen möglich sind, erfüllen bloß *input*-orientierte datenschutzrechtliche Normen nicht mehr die Funktion, intime Daten und Freiheitsräume zu schützen und zugleich die Potentiale von Big Data zu nutzen.

Vor diesem Hintergrund hat der Deutsche Ethikrat in seiner Stellungnahme „Big Data und Gesundheit" [6] vorgeschlagen, Datensouveränität als *informationelle Freiheitsgestaltung* zu verstehen. Die Grundidee der informationellen Freiheitsgestaltung wurde dabei bisher unter dem Terminus der informationellen Selbstbestimmung behandelt. Informationelle *Selbstbestimmung* tritt 1983 im Volkszählungsurteil des Bundesverfassungsgerichts als Aspekt des im Grundgesetz formulierten Allgemeinen Persönlichkeitsrechts in Erscheinung [25]: Kontrollansprüche über persönliche Daten leiten sich aus der Bedeutung einer individuellen privaten Sphäre ab, welche zur Entfaltung der Persönlichkeit der Bürgerinnen und schließlich auch für den demokratisch legitimierten Staat funktionsnotwendig ist.

Informationelle *Freiheitsgestaltung* geht insofern über informationelle Selbstbestimmung hinaus, als sie mehr als ein bloßes Ausschlussrecht meint. Vielmehr umfasst sie ebenso eine „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" [6]. Was folgt daraus für das Konzept der Datensouveränität?

Datensouveränität ist darauf ausgerichtet, individuelle Freiheitsvollzüge unter Bedingungen von Big Data und KI zu gewährleisten und zu ermöglichen. Sie beinhaltet sowohl die Möglichkeit, sich vor Eingriffen in die Freiheit zu schützen – und geschützt zu werden – als auch die Möglichkeit Freiheit zu leben und auszudrücken, beispielsweise in der Gabe von Daten für kollektive Ziele.

1.4 Schutz eigener Daten als Aspekt von Datensouveränität

Zunächst kann Datensouveränität mit einer abwehrrechtlichen Perspektive verknüpft sein, die den Schutz individueller Freiheitsrechte fokussiert. In diesen Entscheidungskontexten haben Individuen nicht nur ein Interesse am Schutz von Daten, sondern sind für die Möglichkeit freiheitlicher Vollzüge auf Räume des Nichtwissens angewiesen. Die mit Datensouveränität verbundenen Kontrollansprüche schließen daher die Möglichkeit mit ein, Privatheit [26] zu schützen und Daten abschirmen zu können. Erst vor dem Hintergrund solch negativ-protektiver Aspekte von Selbstbestimmung sind gehaltvolle Entscheidungen über die eigenen Daten möglich.

Bei Daten mit medizinischer Relevanz handelt es sich um besonders sensible Daten, deren Verarbeitung Freiheitsräume verengen können. Datensouveränität kann daher mit Ansprüchen einhergehen, Gesundheitsdaten vor Zugriffen zu schützen, d. h. Privatheit im Sinne eines Rechts in Ruhe gelassen zu werden [27] durchzusetzen. Zwar abstrahiert das solidarische Gesundheitssystem ganz bewusst vom individuellen Risikoprofil und sieht gleichen Zugang und Versorgung für alle vor. Doch selbst unter diesen Vorzeichen sind Szenarien denkbar, in denen die Verfügbarmachung von Gesundheitsdaten Einfluss auf Versicherungsleistungen hat, beispielsweise wenn durch Anreize zum Teilen von Gesundheitsdaten mit dem Versicherer *de facto* diejenigen einen Malus erleiden, die an solchen Programmen nicht teilnehmen möchten [6]. Zudem wirken der Solidargedanke und die damit verbundene Abstraktion von Risikoprofilen weniger in Gesundheitssystemen mit stärker stratifizierten Versicherungsprämien. Unabhängig von möglichen Implikationen für Versicherungsstatus und Versorgung weisen Kommentatorinnen insbesondere im Hinblick auf klinische Big-Data-Forschung darauf hin, dass sich Individuen ausgebeutet fühlen und Vertrauensverluste verursacht werden könnten, wenn private Datenverarbeiter auf Basis verfügbar gemachter Daten hohe Profite erzielen, ohne Studienteilnehmerinnen oder Patientinnen bzw. Patientenkollektive daran zu beteiligen und in die Steuerung von Forschungsprozessen einzubinden [28]. Schließlich können Individuen auch in anderen Bereichen ein Interesse an der Vertraulichkeit von Gesundheitsdaten haben, sei es bei weiteren Versicherungsleistungen, gegenüber dem Arbeitgeber oder im Privatleben.

Datensouveränität erfordert, dass Daten bestimmten Individuen zugeschrieben werden können, d. h. definiert ist, über welche Daten sie souverän sein und berechtigte Kontrollansprüche stellen können. Fragen, welche Kontroll-, Ausschluss- und Verwertungsrechte welches Individuum an welchen Daten hat

und haben sollte, sind zentraler Bestandteil der Debatte, ob es ein Eigentum an Daten gibt [29]. Im Zentrum stehen Ansprüche wie Partizipation in Deliberations- und Steuerungsprozessen sowie die Beteiligung der Subjekte an der Generierung ökonomischen Werts, die durch die Verarbeitung „ihrer" Daten ermöglicht wird. An einem Ende des Spektrums fordern Autoren die Vergütung von Datensubjekten in genau der Höhe, in der sie und ihre Daten zur Wertsteigerung beitragen [30]. Am anderen Ende des Spektrums fordern andere, dass zumindest manche Datensorten, beispielsweise genomische Daten [31], zunächst als der Allgemeinheit oder Öffentlichkeit gehörendes Gut zu betrachten sind, beispielsweise weil das Individuum keine produktive Kraft in die Generierung dieser Daten eingeführt hat. Individuelle und gemeinschaftliche Ansprüche an Datenverwertung können sich also gegenüberstehen und verlangen nach Aushandlungsprozessen, in denen ihr Verhältnis austariert wird.

Auch aus rechtlicher Perspektive wird intensiv überlegt, wie Rahmenbedingungen für solche Aushandlungsprozesse aussehen können. Argumentiert wird zum Beispiel, dass das Datenschutzrecht den betroffenen Personen, also den Personen, auf die sich die bearbeiteten Daten inhaltlich beziehen, bereits heute eine Rechtsposition verschafft, die einem Eigentum an Personendaten – im Sinne eines übertragbaren Ausschließlichkeitsrechts – zumindest nahekommt. Auch konkrete Regelungsoptionen wurden bereits vorgestellt. Zu den denkbaren Varianten zählt dabei zum einen eine tatsächliche „eigentumsnahe" Ausgestaltung, die Personendaten in die bestehende Eigentumsordnung zu inkorporieren versucht [32, 33]. Zum anderen wird aber – wohl erfolgversprechender, da die genannten Unterschiede zwischen den klassischen Eigentumsobjekten und Daten doch schwer wiegen – darüber nachgedacht, wie ein „originäres Immaterialgüterrecht sui generis an verhaltensgenerierten Informationsdaten der Bürger" [34] aussehen könnte, das den „Nutzern als Datenproduzenten ein eigentumsrechtliches Abwehr- und Vermögensrecht" ([35], vgl. für einen anderen Zuordnungsansatz [36]) verschaffen soll.

1.5 Verfügbarmachung von Daten als Ausdruck von Datensouveränität

Datensouveränität ist nicht auf negativ-protektive Aspekte beschränkt. Als soziale und vernetze Wesen haben Datensubjekte nicht nur ein Interesse an der Beschränkung von Informationsflüssen, sondern lassen sie zu, erwarten und benötigen sie. Zu Datensouveränität befähigt zu sein schließt die Artikulation und Durchsetzung positiv-partizipativer Ansprüche ein, um die jeweils eigene Balance

zwischen der Abschirmung und dem kontrollierbaren Verfügbarmachen von Daten zu wählen und in Aushandlungsprozesse einzubringen. Wenn Daten bewusst bestimmten Zwecken zugeführt werden können, ermöglicht dies Teilhabe an datengetriebenen Koordinations-, Erkenntnis- und Innovationsprozessen. Insoweit bestehen durchaus Überschneidungen zwischen dem aktuellen Data-Governance-Vorschlag der EU-Kommission (COM[2020] 767 final), der u. a. das Konzept des Datenaltruismus stark macht, und unserem Verständnis von Datensouveränität.

Durch das Teilen von Daten können Individuen den in der informationellen Freiheitsgestaltung angedeuteten Ausdruck der Persönlichkeit sowie individueller Auffassungen und Werte praktisch werden lassen. So kann man zum Beispiel *Solidarität* als einen gemeinsamen Willen fassen, Kosten in einem weiten Sinne – also finanzielle, sozial-emotionale oder andere Kosten – gemeinsam zu tragen, um anderen zu helfen [37]. Das Teilen von medizinischen Daten kann folglich insofern als solidarisches Handeln verstanden werden, als es einen notwendigen Beitrag zu Forschungsprozessen liefert, wodurch Wissen generiert und neue Erkenntnisse gewonnen werden können. Die Gabe und Spende von Daten zu Forschungszwecken kann dabei als Ausdruck individueller Freiheitsvollzüge verstanden werden. Zugleich ist zur Verwirklichung von Freiheit ein gemeinsamer Gestaltungsrahmen nötig. Ohne die Möglichkeit, zu drängenden gesellschaftlichen Herausforderungen zu forschen und neue Erkenntnisse zu gewinnen, wären individuelle Freiheitsvollzüge stark gefährdet.

Digitalisierung im Gesundheitssektor könnte so den Raum für neue gesellschaftliche Solidaritätsmuster eröffnen [6]. Die Option, Daten für die Forschung zur Verfügung zu stellen, kann ferner als Komponente der Teilhabe an Forschungsprozessen gesehen werden, wie sie Befürworter einer *citizen science* und eines *human right to science* [38] einfordern.

Eine besondere Form des Teilens von Daten ist die Datenspende, verstanden als die *Gabe* [39–41] von Daten [42]. Manche Akte des Gebens zielen auf einen Effekt bzw. eine Gegenleistung. Das Geben von Gesundheitsdaten kann aus der Motivation heraus geschehen, die eigene Behandlung zu optimieren. Akte des Gebens gehen jedoch nicht vollends in solchen Motivationen auf. Verschiedene Gabe-Theorien weisen darauf hin, dass Gaben zwar kein voraussetzungsloses Geben darstellen, jedoch nicht, oder nicht primär, auf Gegenleistung abzielen.

In den vorherigen Fallbeispielen tritt klar zutage: Natürlich kann eine Gesellschaft von datenintensiven Anwendungen profitieren, z. B. wenn digitale Epidemiologie frühzeitig Spielräume für Vorsorge- und Gegenmaßnahmen eröffnet. Datengetriebene biomedizinische Forschung im Allgemeinen kann ungeachtet eines gewissen Hypes [43–45] zu Erkenntnisgewinnen und Innovationen führen, die die Lebensqualität aller steigern und die Versorgung im gesamten

Gesundheitssystem verbessern, ohne dass es eine Garantie für einzelne Patienten gibt.

Gaben enthalten Stiftungselemente, die sich auf Anerkennung und die Knüpfung eines sozialen Bandes beziehen. Solche Stiftungselemente können an ein konkretes Gegenüber oder ein unkonkreteres Gemeinwohl gerichtet sein. Gaben eröffnen neue Möglichkeitsräume und sind der Souveränität der Individuen zuträglich, insofern sie soziale Strukturen stärken, in denen individuelle Lebensvollzüge eingebettet sind. Gerade weil sich die Gabe einer solchen Reziprozität verwehrt, kann sie nicht genötigt oder durch Anreize erzeugt werden. Mit Gaben können Prekarität und Unsicherheit verbunden sein, da zunächst offenbleibt, welche Folgen die Gabe hat und ob Stiftungselemente anerkannt und erwidert werden. Mit Gaben kann ein soziales Band geknüpft werden, sie können jedoch auch Asymmetrien verstärken, Vulnerabilitäten exponieren, hinter Erwartungen zurückbleiben oder als Übergriff empfunden werden. Mit der Gabe von Daten ist somit nicht klar, ob sie zum Gemeinwohl beitragen oder Ungerechtigkeiten exponieren werden. Obwohl die Gabe von Daten also intentional erfolgt, markiert sie zugleich einen gewissen Kontrollverlust für den Gebenden. Selbst wenn sich ein Subjekt beim Transfer der Gabe nicht genötigt oder gar übergangen fühlt, sondern freiwillig eingewilligt hat, kann es auch nach dem Akt des Gebens Erwartungen an den Umgang mit dem Gegebenen haben.

Gaben können auf ganz verschiedene Weisen gegeben werden und ganz verschiedene Güter betreffen. In aktuellen Debatten wird der Begriff der Datenspende zuweilen als Paraphrase für Broad Consent [46, 47] Arrangements bzw. der Verfügbarmachung von Daten ohne enge Zweckbindung [6] verwendet. Dieser Begriffsverwendung scheint zugrunde zu liegen, dass Spenden und weite Einwilligung aufgrund einer in beiden Fällen vorliegenden willentlichen Aufgabe von Kontrolle parallelisiert werden können. Dies ist jedoch keineswegs notwendig. Konzeptionell spricht nichts gegen eine Datenspende, bei der Spender fortwährend über Verwendungsmöglichkeiten informiert blieben und bestimmen könnten, für welche Zwecke und bis wann ihre Daten verarbeitet werden. Bei der Entscheidung zu Geben gibt es zwischen dem Bestehen auf vollkommene Kontrolle und der völligen Aufgabe jeglicher Ansprüche rund um das Gegebene ein Spektrum, in dem bestimme Erwartungen an Verwendungskontexte bestehen bleiben, ohne dass die Gabe dadurch unterminiert wird. Es liegt sogar nahe, dass Elemente der Stiftung, Widmung und symbolischen Aufladung des Gegebenen hinreichende Informiertheit und Kontrolle über Verwendungskontexte gerade voraussetzen. Das gegebene Gut im Falle der Datenspende könnte beispielsweise in dem zeitlich befristeten sowie zweckgebundenen Zugang zu den Daten bestehen [42]. So

verstanden steht auch die prinzipielle Möglichkeit, Daten zurückzuziehen, der Datenspende nicht entgegen.

1.6 Strukturbedingungen von Datensouveränität

Als Ergebnis der bisherigen Erörterung kann festgehalten werden, dass Datensouveränität mindestens zwei Aspekte umfasst. Zum einen hat Datensouveränität eine abwehrrechtliche Dimension, die primär den Schutz von Persönlichkeitsrechten und die Bewahrung von Freiheitsvollzügen betrifft. Zum anderen ist mit Datensouveränität der Anspruch verknüpft, Daten verfügbar machen zu können. Datensouveränität umfasst die Befähigung des Individuums, Abwägungen zwischen diesen Aspekten vorzunehmen und umzusetzen. Dafür ist die Kontrollierbarkeit von Daten zentrale Voraussetzung. Ein Punkt, an dem eine solche Abwägung besondere Bedeutung bekommt, ist die Einwilligung in die Verwendung von personenbezogenen Gesundheitsdaten zu Forschungszwecken. Als eine Möglichkeit dies umzusetzen, werden im Folgenden unterschiedliche Formen der Einwilligung untersucht und beleuchtet. Wir werden dabei aufzeigen, warum und wie ein Dynamic Consent eine Möglichkeit darstellt, Kontrollierbarkeit und Gemeinwohl zusammenzudenken.

Die Kontrollierbarkeit von Daten ist dabei eingebettet in und angewiesen auf soziale Aushandlungsprozesse. Erstens können wie eingangs erwähnt verschiedene Akteure Ansprüche auf Datensouveränität erheben, die nicht immer spannungsfrei miteinander in Beziehung stehen und daher nach Aushandlung verlangen. Zweitens ist individuelle Freiheitsgestaltung auf einen sozialen Gestaltungsrahmen angewiesen. Um diesen Rahmen zu wahren und zu stärken, sind Abwägungen zwischen individuellem Kontrollanspruch und öffentlichem Interesse nötig.

Schließlich wird Kontrollansprüchen nicht allein dadurch Genüge getan, dass sie als gültig anerkannt werden, sondern dass zugleich soziale und technische Strukturbedingungen zur Ermöglichung und Befähigung von Kontrolle über Daten vorhanden sind. Mit der Forderung nach *Stewardship* rund um Daten ist der Hinweis auf die Notwendigkeit eines nachhaltigen Umgangs mit Datenressourcen durch umsichtige Formatierung, Strukturierung und Archivierung verbunden, um sie für gegenwärtige und zukünftige Entdeckungs- und Innovationsprozesse langfristig anschlussfähig und zugänglich zu machen [48, 49]. Dadurch kann der Grundstein für eine Reihe von potentiell nutzenbringenden Innovationen gelegt werden, beispielsweise eine verbesserte klinische Versorgung durch Informationsaustausch zwischen verschiedenen Kliniken und Ärzten, die Nutzbarmachung

von Daten aus der klinischen Versorgung für die biomedizinische Forschung und die Entwicklung von Anwendungen maschinellen Lernens in Forschung und Versorgung.

Auch wenn die Ausübung der mit Datensouveränität in Anspruch genommenen Kontrollierbarkeit sich an konkreten Individuen und Situationen zeigt, kann sie nicht auf singuläre und lokale Entscheidungsmomente über die eigenen Daten verkürzt werden. Erst vor dem Hintergrund bestimmter Strukturbedingungen wird die Wahrnehmung dieser Kontrollansprüche möglich und gehaltvoll. Diese werden wir in Kap. 3 entlang vier interagierender Governance-Ebenen beleuchten. Den Grundstein bildet hierbei stets das Gesetz, konkret das Datenschutzrecht (siehe 3.1), das ausgehend von seiner aktuellen Ausgestaltung auch von einer Entwicklungsoffenheit gekennzeichnet ist, welche die Etablierung Datensouveränität stiftender Mechanismen wie insbesondere den Dynamic Consent (siehe Kap. 2) ermöglicht. Wie bereits erwähnt reicht Datensouveränität aber auch über seine gesetzlich festgeschriebenen Strukturbedingungen hinaus und verwirklicht sich auch und besonders in un- oder nur teils regulierter Selbstbindung (siehe 3.2). Zudem bedarf es geeigneter technischer Strukturen sowie der Präsenz von Akteuren wie Datentreuhändern, die Datenflüsse im Sinne der Individuen steuern (siehe 3.3). Ferner ist auf Kompetenzen im Umgang mit Informationstechnologien sowie ein Bewusstsein um mögliche Formen von Datenverarbeitung mit Gesundheitsrelevanz zu verweisen (siehe 3.4), die zur gehaltvollen Nutzung solcher Steuerungsmöglichkeiten nötig sind.

2 Dynamic Consent als Umsetzungsmechanismus von Datensouveränität

2.1 Die informierte Einwilligung als basales – und weiterhin zentrales – Legitimationsmodell des Datenschutzrechts

Das Datenschutzrecht nutzt bekanntlich unterschiedliche Möglichkeiten, die Verwendung personenbezogener Daten zu legitimieren. Von besonderer praktischer wie konzeptioneller Bedeutung ist dabei die individuelle Einwilligung [50]. Sie bringt den verfassungsnormativ abgesicherten, im Grundrecht auf informationelle Selbstbestimmung (als spezielle Ausprägung des allgemeinen Persönlichkeitsrechts, Art. 1 Abs. 1 i. V. m. Art. 2 Abs. 1 GG) fundierten Gedanken zum Ausdruck, dass im Grundsatz die Datengeber selbst über die Preisgabe und Verwendung ihrer persönlichen Daten entscheiden [grdl. BVerfGE 65, 1 (43)]. Dabei bezieht sich die Einwilligung dem herkömmlichen datenschutzrechtlichen Denken zufolge auf einen vorab vergleichsweise präzise bestimmten Zweck der Datenverarbeitung. Der Betroffene soll wissen, für welche Verarbeitungsprozesse er seine Daten zur Verfügung stellt. Hieraus resultieren spezifische, sowohl das nationale wie das supranationale Recht prägende prozedurale Anforderungen: Damit die Betroffenen die konkrete Bedeutung und Tragweite der beabsichtigten Datenverwendung überblicken können, müssen datenschutzrechtliche Einwilligungen insbesondere freiwillig, informiert und bestimmt erteilt werden [51]. Das steht namentlich allzu allgemeinen oder gar völlig offen formulierten (Blanko-)Einwilligungen entgegen.

Dieses Einwilligungsverständnis liegt grundsätzlich auch der DSGVO zugrunde [52]. Sie definiert in Art. 4 Nr. 11 DSGVO die „Einwilligung" der betroffenen Person zunächst eng zweckbezogen als „jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene

P. Hummel et al., *Datensouveränität,* essentials,
https://doi.org/10.1007/978-3-658-33755-1_2

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 personenbezogenen Daten einverstanden ist.“ Art. 6 Abs. 1 S. 1 lit. a), 9 Abs. 2 lit. a) DSGVO sieht im Rahmen der Rechtmäßigkeit der Datenverarbeitung allerdings die Option vor, dass die betroffene Person in die Verarbeitung der sie betreffenden personenbezogenen Daten „für einen oder mehrere bestimmte Zwecke“ einwilligen kann. Die DSGVO enthält insoweit eine interne Spannung, als sie einerseits an einer klaren Zweckbestimmung festhält, andererseits aber in Erwägungsgrund 33 für die Forschung die Möglichkeit breiterer und multipler Zwecksetzungen thematisiert. Demnach sollte, soweit der Verarbeitungszweck zum Zeitpunkt der Erhebung der personenbezogenen Daten nicht vollständig angegeben werden kann, „es betroffenen Personen erlaubt sein, ihre Einwilligung für bestimmte Bereiche wissenschaftlicher Forschung zu geben, wenn dies unter Einhaltung der anerkannten ethischen Standards der wissenschaftlichen Forschung geschieht. Die betroffenen Personen sollten Gelegenheit erhalten, ihre Einwilligung nur für bestimmte Forschungsbereiche oder Teile von Forschungsprojekten in dem vom verfolgten Zweck zugelassenen Maße zu erteilen.“ Letztlich verdeutlichen aber gerade diese, in ihrer konkreten Bedeutung umstrittenen Sonderbestimmungen, dass die DSGVO prinzipiell am traditionellen Einwilligungsmodell festhält.

Es bedarf einer Neuorientierung des bestehenden datenschutzrechtlichen Regelungsmodells gerade dann, wenn die ihm zugrunde liegenden basalen Werte und Überzeugungen auch unter den Bedingungen von Big Data als bedeutsam verstanden werden. Dies verlangt nach Governance-Ansätzen, einschließlich eines Rechtsrahmens, der angesichts rasanter und neuartiger Entwicklungen hinreichende Sicherheit und Zuverlässigkeit der Anwendungen gewährleistet, umgekehrt aber auch angesichts der mit ihnen verbundenen Chancen hinreichend Raum zur Entfaltung lässt. Ein entscheidender Baustein hierfür stellt die Flexibilisierung des Einwilligungserfordernisses dar.

2.2 Dynamic Consent als problemadäquate Lösung

Die Einwilligung stellt im deutschen wie im europäischen Recht die wichtigste Voraussetzung (Erlaubnistatbestand) für den Umgang mit personenbezogenen Daten dar. Für Wissenschaft und Forschung gibt es jedoch Möglichkeiten, den Einwilligungsvorbehalt zu umgehen. So ist es unter bestimmten Umständen datenschutzrechtlich zulässig, nicht nur opt-in-, sondern auch opt-out-Modelle zu

wählen, also Datenerhebungen und -nutzungen auf Basis gesetzlicher Erlaubnisnormen durchzuführen. Dem liegt eine funktionale Beobachtung zugrunde: Mit Blick auf die Datenqualität und die Bedeutung möglichst vollzähliger Datensätze (Repräsentativität) kann ein zu umfassendes Einwilligungskonzept Probleme verursachen: Ein striktes Einwilligungserfordernis kann die verfügbare Datengrundlage massiv reduzieren und ein großes Hemmnis für datenintensive Forschungsbereiche darstellen. Ersichtlich besteht ein Widerspruch zwischen der (Ideal-)Vorstellung einer – jedenfalls dem Grundansatz nach – freiwilligen Datenübermittlung und dem gleichzeitigen Streben nach einer möglichst vollständigen und repräsentativen Datengrundlage (exemplarisch [53]).

Ein Versuch mit diesem Dilemma umzugehen besteht darin, datenschutzrechtliche Standards bereichsbezogen aufzuspalten: Während (Gesundheits-) Versorgung auf einem Informed oder Narrow Consent basiert, wäre in der Forschung ein Broad Consent oder gar eine von der Einwilligung gelöste Verwendung zulässig. § 27 Abs. 1 BDSG erlaubt die Verarbeitung „für wissenschaftliche oder historische Forschungszwecke“ auch ohne Einwilligung und benennt in Abs. 3 eine prinzipielle Anonymisierungspflicht personenbezogener Daten als Voraussetzung. Das Gesetz für eine bessere Versorgung durch Digitalisierung und Innovation (Digitale-Versorgung-Gesetz – DVG) [Bundesgesetzblatt 2019, Teil I, Nr. 49, S. 2562] zielt ebenfalls darauf ab, Patientendaten pseudonymisiert auch unabhängig von einer individuellen Einwilligung für Forschungszwecke nutzen zu können. Wie in Kap. 1 skizziert, dürfte die nachhaltige Beseitigung von Personenbezug allerdings durch neue technische Möglichkeiten der Re-Identifizierung erschwert sein.

Wer grundrechtlich vorzugswürdig weiterhin primär auf ein einwilligungsbasiertes Regelungskonzept setzt (Opt-in-Modell) [54], muss nach komplexeren Mechanismen fragen, um Einwilligungsentscheidungen so treffen und sie gegebenenfalls auch delegieren zu können, dass fortlaufende Kontrolle ermöglicht wird. Das verdeutlicht, warum es attraktiv ist, das Modell eines Dynamic Consent [55–60] zu entfalten und kontextsensibel weiterzuentwickeln. Wir verstehen dabei den Dynamic Consent weniger als eine eigenständige dritte Variante, sondern als einen prozedural erweiterten, die beiden an entgegengesetzten Polen befindlichen Formen (Narrow Consent und Broad Consent) aufnehmenden Spezialfall des allgemeinen Zustimmungsgedankens. Der Dynamic Consent zielt darauf ab, einen angemessenen Ausgleich zwischen unrealistisch engen Zweckbestimmungen einerseits und bloßen Blankozustimmungen andererseits sicherzustellen. Dem Grundkonzept der engen, zweckgebundenen Einwilligung wird entsprochen, indem sie nicht einmalig vorab, sondern im Rahmen eines dynamischen und

ggf. iterativen Prozesses erhoben und integriert wird [57, 60]. Prozedural verlangt dies ein komplexeres Kooperationsregime. Die Beteiligten müssen nicht nur punktuell, sondern längerfristig miteinander in Kontakt stehen. Das setzt eine entsprechende technische Infrastruktur voraus, mittels derer den Teilnehmern regelmäßig unterschiedliche Optionen vorgelegt werden und sie entscheiden können, welche zusätzlichen Informationen sie benötigen und ob und für welche Projekte sie ihre Daten zur Verfügung stellen. Sie werden frühzeitig über die wesentlichen Parameter der konkreten Datennutzung (z. B. Eigenschaften und Ziele einer Bio- oder Datenbank, deren Finanzierung, das jeweilige Datenschutz- und Governance-Konzept, etwaige etablierte Kooperationen und Weitergabevereinbarungen) informiert und müssen dann ihre präferierte Einwilligungsvariante festlegen. Das Spektrum reicht dabei von der klassischen Variante einer separaten Einwilligung für jedes Projekt (Narrow Consent) bis zu umfassenderen Lösungsansätzen, bei denen nicht nur in Einzelverwendungen, sondern in relativ breite Verwendungskategorien eingewilligt werden kann (Broad Consent). In bestimmten Zusammenhängen und für bestimmte Bereiche könnte sogar eine Pauschalzustimmung (Blanket Consent) erteilt werden. Auch Kombinationen der verschiedenen Einwilligungsoptionen sind denkbar.

Der Dynamic Consent erfordert aber zugleich, dass Individuen auch die Möglichkeit haben, auf Entwicklungen in der Nutzung von Daten zu reagieren. Eine unverzichtbare Ergänzung zu den vorab festgelegten Präferenzen, die dann von einem technischen System umgesetzt werden, ist die Möglichkeit für Individuen, Präferenzen zu ändern oder anzupassen. Ein so verstandener Dynamic Consent bildet einen überzeugenden Mechanismus, um in einem hochdynamischen Regelungsumfeld eine gegenstandsadäquate Kontrollierbarkeit und Output-Orientierung zu ermöglichen. Eine derartige Weiterentwicklung der Einwilligung ist im Funktionszusammenhang der hier beschriebenen, übergreifenden Gestaltungs- und Regulierungsstrategie zu verstehen. Funktional ist das Ziel, weiterhin ein angemessenes Maß an Selbstbestimmung im Spannungsfeld von Privacy und Gemeinwohl (z. B. durch Forschung) zu gewährleisten. In diesem Sinne geht es um einen situationsangemessenen Mittelweg zwischen kategorischem Forschungsvorrang und unrealistisch enger Zwecksetzung bei der Einwilligung.

Der Dynamic Consent stellt zwar kein Allheilmittel dar; insofern ist es durchaus berechtigt und notwendig, Kritik an allzu optimistischen Umsetzungsfantasien zu üben [61]. Zugleich schießt es aber über das Ziel hinaus, ihn per se abzulehnen und für unrealistisch zu erachten. Er kann durchaus einen funktional überzeugenden Ansatz bilden, der nicht nur die Verfolgung der Ziele des Datenschutzes unter den Bedingungen von Big Data und KI erlaubt, sondern auch seinerseits offen ist für ergänzende Zusatzoptionen. Es wäre voreilig, einzelne Schutzmechanismen

isoliert zu betrachten und übertriebene Hoffnungen allein in sie zu setzen. „Deswegen kann und muss die informierte Einwilligung […] durch die Einbettung in einen Kontext mehrdimensionaler Regelungs- und Schutzmechanismen in ihrer Funktionsfähigkeit gestärkt werden“ [62]. Das zeigt sich besonders anschaulich etwa an der Verbindung von Dynamic Consent und Datentreuhandkonzepten.

2.3 Dynamic Consent und Datentreuhänder

Für eine robuste Umsetzung des Dynamic Consent bedarf es zugleich Delegationsmöglichkeiten. Der Einsatz sog. Datentreuhänder gehört zu den prominenten Vorschlägen, wie unter Big-Data-Bedingungen ein adäquater Datenschutz gewährleistet werden kann [63–65]. Datentreuhänder verwalten die ihnen anvertrauten Daten im Sinne der Präferenzen des Datensubjekts. Prinzipiell können individuelle, aber auch kollektive oder gar gesamtgesellschaftliche Interessen durch den Treuhänder repräsentiert und umgesetzt werden. Es kann sich bei einem Treuhänder um menschliche Akteure handeln, etwa eine Biobank-assoziierte Ethikkommission oder ein Governance Board, die auf Wunsch der Individuen Zugang zu Daten in Ihrem Sinne steuern. Besonders effektiv wird Dynamic Consent, wenn er nicht allein auf eine menschliche Kontrolle setzt, sondern mit spezifischer technischer Unterstützung – etwa in Gestalt spezieller Software-Agenten, die Nutzer-Präferenzen in Echtzeit umsetzen – kombiniert wird.

Im Forschungskontext dient der Treuhänder zunächst dazu, pseudonymisierte/anonymisierte Datensätze weiterzuverarbeiten [66, 67]. Noch stärker ist der Begriff des Datentreuhänders datenschutzrechtlich geprägt, wenn darunter auch sog. „Einwilligungsassistenten“ verstanden werden. Hierbei überprüft der Treuhänder, ob die mit den Daten verbundenen generellen Verarbeitungspräferenzen der betroffenen Personen mit denen einzelner Verarbeitungsvorhaben übereinstimmen. In diesem Fall holt der Treuhänder eine Einwilligung ein oder gibt die Daten für das betreffende Vorhaben direkt frei und verwaltet gleichzeitige Widerrufs-/Widerspruchsoptionen (z. B. beim System CoMaFeDS, vgl. [68]). Befürworter solcher Einwilligungsassistenten versprechen sich so mehr Übersichtlichkeit von Verarbeitungsprozessen [68], aber auch mehr Rechtssicherheit, da sie eine konzentriertere Überprüfung der Einwilligungserklärungen böten [68, 69]. Ein Übergang zu einem technischen System der digitalen Selbstverwaltung des Einzelnen (Stichwort: PMT/PIMS [64]) ist dabei fließend [68]. Ein Beispiel dafür wäre etwa die elektronische Gesundheitskarte und die elektronische Patientenakte als Teil der Telematik-Infrastruktur des Gesundheitswesens: Hier sollen

die Karteninhaber gem. § 291a V 2 SGB V unabhängig von konkreten Behandlungsvorgängen auf für medizinische Behandlungen erhobene Daten gesammelt zugreifen und diese ggf. für weitere Datenverarbeitungsprozesse bereitstellen können [70].

Dieser zunächst eher technische Lösungsansatz lässt sich um drei Interpretationsweisen erweitern. Erstens um *datenschutzrechtliche Fürsorgekonzepte.* In diesem Modell ist es denkbar, dass der Treuhänder auch Datenverarbeitungsvorhaben berücksichtigt, die (noch) nicht unmittelbar mit den Präferenzen der betroffenen Person korrespondieren und sie nach einer Bewertung anhand bestimmter datenschutzrechtlicher Prämissen der betroffenen Person vorschlägt [5, 71]. Hier treten entsprechend mehr Fürsorgemerkmale der Einwilligungsassistenz zu Tage – und werfen entsprechend Haftungsfragen auf, falls die Bewertungen unzutreffend und somit auch wettbewerbsverzerrend ausfallen.

Zweitens ist eine *Einwilligungsassistenz* vorstellbar, bei der der Datentreuhänder selbst die datenschutzrechtlichen Entscheidungen über ihm anvertraute personenbezogene Daten trifft. Hierbei unterstützt der Datentreuhänder das jeweilige Datensubjekt bei der Verwirklichung der informationellen Selbstbestimmung, indem stellvertretend entlang der vorher bestimmten generellen Einwilligungspräferenzen der betroffenen Personen deren datenschutzrechtliche Entscheidungen umgesetzt werden [72]. Insgesamt changiert die datenschutzrechtliche Einwilligungsassistenz des Datentreuhänders zwischen einer Art technisch optimiertem Erklärungsboten und einem Stellvertreter für die datenschutzrechtliche Einwilligung.

Drittens ist ein *vermögensrechtliches* Verständnis des Begriffs des Datentreuhänders möglich. Meist unter Bezugnahme auf ein Dateneigentum wird hier über eine Art verwertungsgesellschaftliche Datentreuhänderschaft nachgedacht (anders hingegen [72, 73]). Bzgl. der Verwertung von Daten wird argumentiert, dass die immense passive Generierung von Daten gerade den Grundstein für die besonders gewinnbringenden Big-Data-Anwendungen bildet. Kurzum: Ein individueller Handel mit Daten als Wirtschaftsgut behebt nicht dessen eigentliches Problem der Machtasymmetrie [72, 74]. Bei der dabei angedachten Verwaltungsgesellschaft „VG-Daten“ [75] (angelehnt an die bekannte VG-Wort) handelt es sich um eine Stelle, die mittels einer Bewilligung durch die ursprünglichen Rechteinhaber umfassende Verwertungsrechte an Daten erlangen soll.

Zusammengefasst können mit „Datentreuhändern“ sowohl Aspekte technischer Zugriffsbeschränkung als auch digitaler Einwilligungsverwaltung adressiert werden. Die konkrete rechtliche Umsetzung ist derzeit noch nicht geklärt und setzt wohl gesetzliche Neuregelungen voraus – entsprechende Regelungsvorschläge enthält nunmehr der Data-Governance-Vorschlag der EU-Kommission.

Im Übrigen ermöglicht das bestehende Recht bereits Datentreuhänderschaft, die über ein digitales Netzwerk individuell generierter Datensammlungen Verarbeitungspräferenzen der Betroffenen mit den Verarbeitungszwecken interessierter verantwortlicher Stellen abgleicht und dabei anfallende Treffer als Grundlage für nachfolgende gesetzlich- oder dezidiert einwilligungsbasierte Verarbeitungsvorgänge bieten können. Auch hier sind aber gesetzliche Erlaubnistatbestände und insbesondere eine dynamisierte Einwilligung kombinierbar.

2.4 Dynamic Consent und erweiterte Schutzperspektiven

Ein wie oben präsentierter Dynamic Consent kann einen Rahmen bilden, innerhalb dessen eine transparenz- und qualitätsbezogene Rechenschaft von Analyseergebnissen sowie kontextuell angepasste Erklärungen prozedural integrierbar sind. Er bietet damit Möglichkeiten, kurrente Problembeschreibungen und -lösungsvorschläge aufzunehmen und umzusetzen:

Der Einfluss unterschiedlicher Daten in verschiedenen, auch nicht antizipierten Verarbeitungskontexten gerade durch Big-Data-Analysen führt zu der Erkenntnis, dass sich eine gerechte Datenwirtschaft nicht nur auf bestimmte Dateninhalte oder nur einzelne Datensätze fokussieren kann (statt vieler [76]), wenn sie weiter freiheitssichernd ausgestaltet sein soll. Überlegungen zu einer sog. *Group Privacy* ([24, 64], ähnlich [77]) verweisen auf die Schutzbedürftigkeit nicht nur individueller, sondern auch kollektiver Interessen. Die durch Big-Data-Analysen gewonnenen und weiterverwendeten Korrelationsmuster betreffen und beeinflussen danach ganze Gruppen und nicht nur die darin zusammengefassten Individuen. Rechtlich lassen sich Korrelationsanalysen spätestens bei einem (Rück-)Bezug der gewonnenen Muster auf Vergleichsgruppen oder Einzelpersonen als datenschutzrechtlich relevant ansehen [78, 79]. Insofern würden Korrelationsmuster bereits zum eigenständigen Objekt datenschutzrechtlicher Entscheidungs- oder Überprüfungsprozesse und nicht nur jene Daten, die als Input zu ihrer Entstehung geführt haben. Sie könnten einem *Right to Reasonable Inferences* [80] unterliegen, welches die in Art. 15 Abs. 1 lit. h) DSGVO statuierten Begründungs- und Transparenzpflichten für automatisierte Entscheidungsfindungen für Konstellationen erweitert, in denen sich aus der Verwendung von Korrelationsmustern Risiken für einzelne Personen – als solche oder Teil einer Gruppe – ergeben. Solche basalen oder erweiterten Rechte könnten gerade auch Teil einer dynamisierten Datenverwaltung sein, indem etwa eine regelmäßige Begründung und

Überprüfung von korrelationsbasierten Schlussfolgerungen als persönliche Bedingung für eine primäre und sekundäre Datennutzung gesetzt wird oder indem die Datenfreigabe ab einem gewissen Begründungsniveau angepasst wird.

Zwei Punkte werden jedoch einer erweiterten Transparenz und Begründung von Korrelationsanalysen regelmäßig entgegengehalten: Die berechtigten Interessen der Datenverarbeiter an der Geheimhaltung ihrer Analysemethoden und Algorithmen und der möglicherweise nur geringe Nutzen für Datensubjekte durch eine technisch detaillierte Aufschlüsselung sie betreffender Korrelationsmuster, da nicht davon ausgegangen werden kann, dass diese von jeder Person verstanden werden. Als Reaktion ließen sich auch sog. *counterfactual explanation* [81] in eine dynamisierte Datenverwaltung integrieren. Danach werden nicht notwendigerweise die – unverständlichen oder zurecht geheimen – technischen Grundlagen der verwendeten Korrelationsmuster preisgegeben, sondern es werden die Verhaltensweisen und Umstände erklärt, die zu dem begründungsbedürftigen Ergebnis geführt haben und bei deren Adaption ein anderes Ergebnis zu erwarten ist. Dies böte dem Datensubjekt auch, ganz im Sinne der informationellen Freiheitsgestaltung, die Möglichkeit, innerhalb von laufenden Datenverarbeitungsprozessen auf die zugrunde liegenden Parameter Einfluss zu nehmen.

Governance-Ansätze

3

Wir haben argumentiert, dass Datensouveränität die Befähigung von Akteuren zu informationeller Freiheitsgestaltung durch Kontrolle der Verwendung sie betreffender Daten bezeichnet (Kap. 1). Im Anschluss haben wir den Dynamic Consent als Umsetzungsmechanismus von Datensouveränität vorgeschlagen (Kap. 2). Im Folgenden fokussieren wir vier miteinander in Wechselwirkung stehende Governance-Ebenen (siehe Abb. 3.1), auf denen Datensouveränität im deutschen Gesundheitssystem ermöglicht und gestärkt werden kann: Hard Law (3.1), Soft Law (3.2), Teilhabe (3.3) und IT (3.4).

3.1 Hard Law

Datensouveränität ist kein Rechtsbegriff, erfüllt aber auch und gerade in juristischer Perspektive eine wichtige heuristische Funktion, soweit er im positiven Recht bereits niedergelegte Grundentscheidungen aufnimmt und in einer bestimmten Funktionalität neu interpretiert. In diesem Sinne baut eine diesem Leitprinzip verpflichtete, umfassende Governancestrategie auf den gegebenen nationalen wie supranationalen Rechtsvorgaben auf. Darüber hinaus dient dieser hier als *Hard Law* bezeichnete Rechtsrahmen als kontinuierlicher Orientierungspunkt der weiterreichenden ethischen und auf das *Soft Law* bezogenen Überlegungen; er verdeutlicht Anschlussmöglichkeiten wie Spannungen und zeigt auf, wo gegebenenfalls eine rechtspolitische Auseinandersetzung geboten ist.

1. **Verfassungsrechtliche Vorgaben weiterentwickeln:** Das Datenschutzrecht besitzt eine verfassungsrechtliche wie einfachgesetzliche Basis. Es entspricht gerade dem Grundansatz des Bundesverfassungsgerichts zum „informationellen Selbstbestimmungsrecht“, nicht starr an einem einmal in die Welt gesetzten

P. Hummel et al., *Datensouveränität,* essentials,
https://doi.org/10.1007/978-3-658-33755-1_3

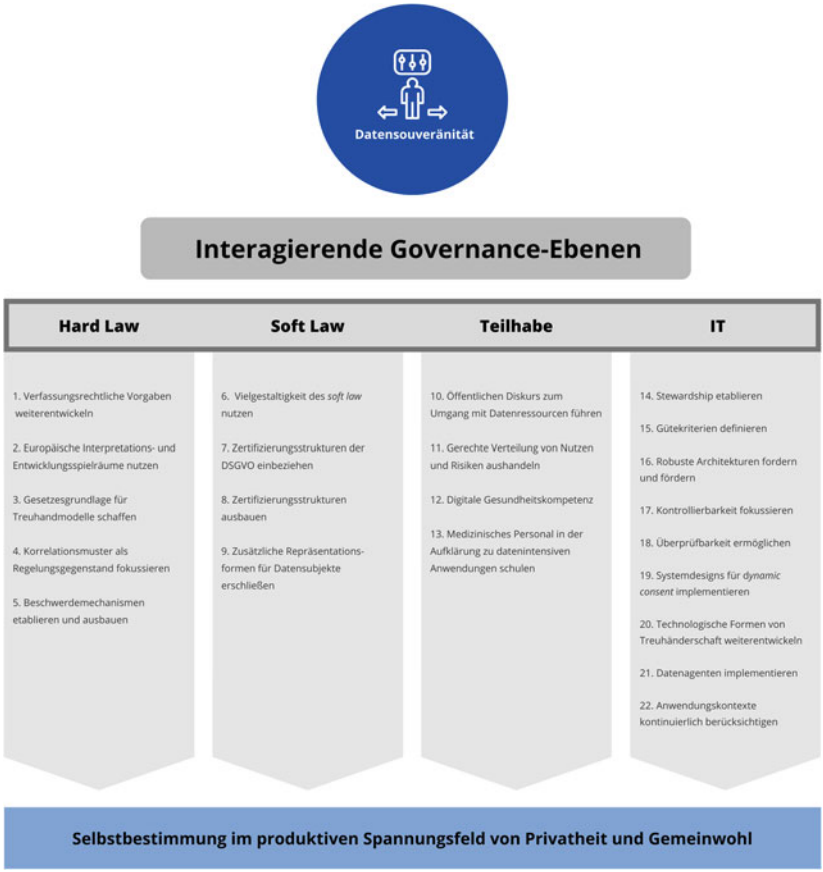

Abb. 3.1 Ansätze und Empfehlungen zur Ermöglichung von Datensouveränität

Konzept festzuhalten, sondern dieses so weiterzuentwickeln, dass seine Grundintentionen möglichst optimal verwirklicht werden können. Dem dient die Idee der Datensouveränität als informationelle Freiheitsgestaltung [6]. Ihr geht es gerade darum, unter den Bedingungen moderner Datenverarbeitung und -verwendung die basalen Ziele des Datenschutzrechts, namentlich einen Schutz der Bürger vor Macht- und Wissensasymmetrien und hierdurch bedingten Freiheitseinbußen, besser umzusetzen.

2. **Europäische Interpretations- und Entwicklungsspielräume nutzen:** Wesentliche Vorgaben zum Datenschutz erfolgen auf EU-Ebene; sie können in einzelnen Bereichen national weiter spezifiziert werden. Die beschriebenen Herausforderungen der Freiheitsverwirklichung durch globale Big-Data-Anwendungen machen gleichzeitig nicht an Staatsgrenzen halt und lassen einen nationalen Alleingang wenig sinnvoll erscheinen. Allerdings sind, erstens, auch die Regelungen der DSGVO interpretations- und entwicklungsoffen. So bieten die gesetzlichen Privilegien verschiedener Verarbeitungskontexte in Art. 5 Abs. 1 lit. b), 89 Abs. 2, Abs. 3 DSGVO – eingedenk der Erwägungsgründe 33 und 43 – Auslegungsansätze für die Praxis eines Dynamic Consent. Entsprechend könnten auch Big-Data-Analysen in diesen Kontexten auf einen Dynamic Consent gestützt und damit in einem Datensouveränität fördernden Rahmen vollzogen werden. Zweitens sind rechtspolitische Impulse natürlich auch auf der Ebene der EU prinzipiell möglich und sollten im Sinne einer stärkeren Output-Orientierung genutzt werden.
3. **Gesetzesgrundlage für Treuhandmodelle schaffen:** Komplizierter erweist sich die Rechtslage – jedenfalls in Deutschland (exemplarisch für die Schweiz [82]) – hinsichtlich der Umsetzung von Datentreuhandmodellen, sofern diesen die Idee einer Stellvertretung bei datenschutzrechtlichen Erklärungen zugrunde liegt: Das Stellvertretungsrecht setzt eine rechtsgeschäftliche Handlung voraus, die im fremden Namen vorgenommen werden soll. Einwilligungen in Rechtseingriffe wie etwa die datenschutzrechtliche Einwilligung werden dem hergebrachten, primär abwehrrechtlichen Verständnis des Datenschutzrechts entsprechend wegen ihres Rechtfertigungscharakters nicht als Rechtsgeschäft eingeordnet [63]. Die hier angenommene Entwicklungsoffenheit des Datenschutzrechts und seiner verfassungsrechtlichen Grundlagen führt indes dazu, dass flexiblere Mechanismen auch mit Blick auf die datenschutzrechtliche Stellvertretung angängig sind. Insbesondere kommt durch die kooperative und durch längerfristige Interaktionen bestimmte Prägung des Dynamic Consent ein rechtsgeschäftlicher und nicht bloß rechtfertigender Ausdruck zum Tragen. So ist es denkbar, dass – wenn das Datenschutzrecht nicht nur der Eingriffsrechtfertigung in Bezug auf das informationelle Selbstbestimmungsrecht dient, sondern auch als rechtsgeschäftliches Regelungsregime angesehen wird – die datenschutzrechtliche Einwilligung auch im fremden Namen abgegeben werden kann. Die im Dynamic Consent enthaltenen Delegationsmöglichkeiten, für deren Möglichkeit wir bereits argumentiert haben, bilden dabei offensichtliche Überschneidungspunkte mit einer datenschutzrechtlichen Stellvertretung

durch Datentreuhänder, welche über eine bloß technische Assistenz hinausgehen und auch Elemente der Stellvertretung, der Fürsorge oder der Verwertung umfassen.

4. **Korrelationsmuster als Regelungsgegenstand fokussieren:** Eine denkbare Erweiterung des Schutzbereichs könnte zudem in der grundsätzlichen Anerkennung von Korrelationsmustern als datenschutzrechtlich relevante Gegenstände liegen. Spätestens bei einem praktischen Rückbezug von diesen Mustern auf einzelne Fälle, lassen sich nach der Rechtsprechung des EuGH diese Muster als personenbezogen und damit als datenschutzrechtlich relevant verstehen [83]. Aber auch schon davor sind Konstellationen denkbar, in denen diese Muster sich praktisch als „Sammeldaten" im hergebrachten Sinne darstellen, die auf die Gruppe der Personen „durchschlagen", von denen die Datenmengen ursprünglich erhoben wurden. Dies ermöglicht praktisch erst die oben präferierte Output-Orientierung datenschutzrechtlicher Mechanismen, da diese andernfalls für wesentliche freiheitsrechtliche Auswirkungen von Big-Data-Anwendungen blind blieben.
5. **Beschwerdemechanismen etablieren und ausbauen:** Damit das Datensubjekt seine Datensouveränität zeitnah und effektiv umsetzen kann, muss darüber nachgedacht werden, welche Beschwerdemechanismen etabliert und wie sie abgesichert werden sollen. Denkbare Optionen sind etwa: haftungsrechtliche Sanktionsmechanismen, ggf. mit Beweislastumkehr; gestufte und sich verschärfende Rechenschafts- und Auskunftspflichten. Dabei könnte an bestehende Rechenschaftsfristen wie in Art. 12 Abs. 3, 14 Abs. 3 lit. a) DSGVO angeknüpft werden, die eine adäquate Information spätestens innerhalb eines Monats einfordern. Ebenso enthält Art. 82 Abs. 2 DSGVO auf der individuellen Haftungsebene bereits eine Beweislastumkehr.

3.2 Soft Law

Die Diskussion über das Datensouveränitätskonzept erschöpft sich nicht in der Frage nach seiner *Hard-Law*-Kompatibilität. *Soft-Law*-Mechanismen, die anders als das *Hard Law* nicht auf staatliche Sanktionen setzen, können ebenfalls dazu beitragen, die Ziele des Datensouveränitätskonzepts in unterschiedlichen institutionellen Settings umzusetzen. Auszugehen ist dabei von den übergeordneten Zielen der Transparenz, Kontrollierbarkeit und Benutzerfreundlichkeit. In einem kompetitiven Umfeld erweist es sich zumal dann als Wettbewerbsvorteil diesen Vorgaben zu entsprechen, wenn entsprechend informierte Datensubjekte (s. unten sub 3.3) nach ihnen verlangen. Über diese sich ohne (zentrale) Steuerung

vollziehenden Prozesse hinausgehend sind bewusste, aber nicht direkt (rechts-) verbindlich wirkende Einwirkungsformen denkbar. Das verweist auf das weite Feld von ko- und selbstregulatorischen sowie *Soft-Law*-Regelungen. Diese etwas vergröbernde Terminologie wird hier im Sinne einer analytischen Unterscheidung zum *Hard Law* verwendet – allerdings eingedenk der Tatsache, dass binäre Schemata unterkomplex und gerade die Kooperations- und Überschneidungsformen von besonderem Interesse sind [84].

6. **Vielgestaltigkeit des *soft law* nutzen:** Diese Governance-Ebene umfasst frei und ungeplant entwickelnde „spontane Ordnungen", aber auch fest umrissene und zumindest partieller staatlicher Aufsicht unterliegende Normen. Teilweise steht der informatorische Gehalt im Vordergrund, teilweise wird auf freiwillige Befolgung, teilweise (zusätzlich) auf Sanktionsmaßnahmen gesetzt. Manche Steuerungsmechanismen erzeugen wirtschaftlichen Druck oder nutzen umgekehrt spezifische Incentives. Mit anderen Steuerungsmechanismen wird mehr oder weniger bewusst auf staatliche Steuerungsleistungen Bezug genommen bzw. sie werden durch hoheitliches Recht rezipiert (z. B. durch Verweisungen) und damit in Rechtsverbindlichkeit überführt. Durchgängig vorhandene oder auch nur dominante Ordnungsmuster sind *a priori* nicht auszumachen; augenfällig sind vor allem die Vielzahl, Vielfalt und Ausdifferenziertheit der Regelsetzung. Das sollte im Sinne eines Varianz als Stärke wahrnehmenden Regelungspluralismus genutzt werden.
7. **Zertifizierungsstrukturen der DSGVO einbeziehen:** Zertifizierung und Akkreditierung stellen im modernen Verwaltungsrecht durch die Verschränkung staatlicher/hoheitlicher und privater/wirtschaftlicher Handlungsbeiträge adäquate Werkzeuge dar. Bekannt ist das etwa aus den inhaltlich wie strukturell sehr disparaten Bereichen des Wissenschafts- und des Produktsicherheitsrechts. Es hat aber spätestens mit den Art. 42 f. DSGVO auch für den Datenschutz eine erhebliche (gerade auch im internationalen Kontext intensiv diskutierte) Bedeutung erlangt [85]. Im Grundsatz geht es hierbei um eine extern, aber nicht notwendig staatlich/hoheitlich überprüfte und nach außen kenntlich gemachte – etwa durch Datenschutzsiegel und -prüfzeichen – Normbefolgung. Charakteristisch ist die freiwillige Mitwirkung, wobei aber gleichzeitig klar ist, dass eine erfolgte Zertifizierung von Rechts wegen mit deutlichen Vorteilen verbunden wird. Grundlegend in der DSGVO geregelt, wird der Kommission die Möglichkeit eingeräumt, verbindliche Detailvorgaben in „Durchführungsrechtsakte[n] über technische Standards und Mechanismen zur Förderung und Anerkennung von Zertifizierungen" (Art. 43 Abs. 9 DSGVO) zu regeln. Typisch für eine Koregulierungssituation ist es, dass

zur Zertifizierung nicht allein die Aufsichtsbehörden berufen sind. Stattdessen genügt es, wenn diese informiert werden, aber im Übrigen (private) sog. Zertifizierungsstellen tätig werden, die gemäß Art. 43 Abs. 1 DSGVO „über das geeignete Fachwissen hinsichtlich des Datenschutzes verfügen“ müssen. Ersichtlich wird damit ein breites Spektrum an möglicher Zertifizierung abgedeckt, wobei sie gleichzeitig einer qualitativen Kontrolle nach Art. 42 Abs. 5 DSGVO unterliegt.

8. **Zertifizierungsstrukturen ausbauen:** Die von der DSGVO angesprochenen „datenschutzspezifischen Zertifizierungsverfahren“ beziehen sich ausdrücklich darauf „nachzuweisen, dass diese Verordnung bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern eingehalten wird“ (Art. 42 Abs. 1 DSGVO). Deshalb ist es keineswegs ausgeschlossen, das Zertifizierungsmodell nutzbar zu machen, um über die rechtlichen (Mindest-)Maßgaben hinausgehende, namentlich dem Souveränitätsmodell verpflichtete, Verhaltensregeln zu implementieren.
9. **Zusätzliche Repräsentationsformen für Datensubjekte erschließen:** Treuhandkonzepte können auch dazu verwendet werden, Interessen zu aggregieren, um bestehende Machtgefälle in der Datenwirtschaft zu kompensieren. Es bestehen dabei auch Wechselbeziehungen zu den beschriebenen Zertifizierungsmechanismen [65]. Daneben sind im „Raum des Unverbindlichen“ auch zusätzliche repräsentative Partizipationsformen denkbar, die nicht dazu dienen, die konkrete Datenhandhabung zu steuern, sondern die Betroffenen auf einer abstrakteren Ebene ansprechen und so eine Möglichkeit bieten, Interessen zu artikulieren und damit gleichzeitig den Ideenwettbewerb zu befördern.

3.3 Teilhabe

In Kap. 2 haben wir vorgeschlagen, Datensouveränität durch Dynamic Consent zu implementieren. Neben technischen Erfordernissen erwachsen daraus auch Anforderungen an das Wissen und die Kompetenzen der Subjekte, deren Entscheidungen durch Dynamic Consent artikuliert werden. Der Dynamic Consent als Lösungsstrategie erscheint vor allem deswegen attraktiv, weil er den Individuen fortwährend erlaubt, ihre Präferenzen über geeignete technische Infrastrukturen in die Tat umzusetzen. Für eine solche selbstbestimmte Umsetzung und Gestaltung sind unterschiedliche individuelle wie soziale Formen von Teilhabe nötig. Diese je nach Entscheidungs- und Handlungskontext unterschiedlich durch Hard Law, Soft Law oder reine Empfehlungen umzusetzenden Teilhabe-Formen werden im Folgenden skizziert:

10. **Öffentlichen Diskurs zum Umgang mit Datenressourcen führen:** Datensouveränität als ein zugeschriebener Status verweist darauf, dass ein ausschließlich individualistischer Ansatz zu kurz greift. Statt lediglich von Bildungsprozessen auf der individuellen Ebene auszugehen, verweist sie darüber hinaus auf die Ebene der Formierung eines gesellschaftlichen Willens um die Aushandlung von Ansprüchen an Daten und deren Verwertung. Wie im Zusammenhang mit der Figur des Dateneigentums angedeutet, sind Spannungen zwischen individuellen Ansprüchen und Ansprüchen der Allgemeinheit denkbar. Auf beiden Ebenen werden berechtigte Interessen artikuliert, denen nicht immer gleichzeitig gefolgt werden kann. Die Klärung der Frage, welche Ansprüche als gerechtfertigt gelten und welche letztlich wie Vorrang zu nehmen haben, bedarf eines gesamtgesellschaftlichen Diskurses und Reflexionsprozesses. In ihm wäre zu klären, ob und wie individuelle Ausschlussrechte und Freiheitsvollzüge zusammengedacht werden können mit der Verwertung gesellschaftlich potentiell nützlicher genomischer Daten, Bewegungsprofile, Social-Media-Daten und anderer Datensorten, deren Analyse die öffentliche Gesundheit langfristig stärken können. Die Befähigung zur verantwortlichen Verwertung von Daten ist nicht nur entlang individualethischer, sondern auch auf gesellschaftlicher Ebene zu denken.
11. **Gerechte Verteilung von Nutzen und Risiken aushandeln:** Die Einführung und Nutzung von Big Data im Gesundheitsbereich wird sich kaum zurückdrehen lassen. Das wäre auch wenig sinnvoll, denn die Nutzung von Big Data kann zu einer Verbesserung der Gesundheitsversorgung führen. Zugleich darf nicht verkannt werden, dass auch in diesem Bereich in den letzten Jahren der gesellschaftliche Nutzen und die möglichen Risiken ungleichmäßig verteilt waren. Allzu schnell wurden Daten als das neue Gold/Öl des digitalen Zeitalters oder anderweitig zu verwertende Ressource verstanden, ohne dass zugleich eine Idee davon implementiert wurde, wie auch die breite Zivilgesellschaft von den Ergebnissen und Errungenschaften profitieren kann. Es bedarf dringend rigoroser Forschung, die verschiedene Disziplinen und Perspektiven einbezieht, um uns dabei zu helfen, die kurz- und langfristigen Auswirkungen der Nutzung von Big Data in sozialen und wirtschaftlichen Institutionen zu messen und zu verstehen. Nur wenn sichergestellt ist, dass Teilhabe nicht nur die Beteiligung an Diskussionen, sondern auch eine ökonomische Teilhabe beinhaltet, wird sich auf lange Sicht gesellschaftliches Vertrauen in Big-Data-Anwendungen, beteiligte Organisationen und öffentliche Institutionen aufrechterhalten lassen.
12. **Digitale Gesundheitskompetenz:** Als eine Komponente digitaler Gesundheitskompetenz [86] sind Informationsangebote für Patienten und potentielle

Teilnehmerinnen an datenintensiver Forschung und Versorgung essentiell. Dies gilt nicht weniger in Zeiten, in denen sich Patientinnen einerseits im Internet selbst informieren, andererseits mit wenig Hintergrundwissen Online-Angeboten und klinischen Anwendungen mit hohem Komplexitätsgrad gegenübertreten. Bei der gemeinsamen Einordnung von Big-Data-basierten Hypothesen ist der Grundstein durch ein zumindest implizites Verständnis von für Big Data charakteristischen Konzepten und Mechanismen zu legen. Benötigt wird ein Diskussionsrahmen, in dem sowohl Klarheit über grundlegende Begriffe besteht als auch die Ausgestaltung und Priorisierung bestimmter Gesundheitskompetenzen in institutionellen Settings debattiert werden können.

13. **Medizinisches Personal in der Aufklärung zu datenintensiven Anwendungen schulen:** Auch die Ausbildung des medizinischen Fachpersonals bedarf der intensivierten Berücksichtigung von kommunikativen Herausforderungen, die bei der Vermittlung des Umfangs der Datenverarbeitung, eventuellen Risiken sowie den Ergebnissen datenintensiver Anwendungen auftreten können. Anschließend an die positiv-partizipativen Aspekte von Datensouveränität umfasst dies die Bewusstseinsbildung für Möglichkeiten zur Teilnahme an Forschung, zum Beispiel in Form der oben beschriebenen Datenspende. Diskutiert wird in diesem Zusammenhang die neu zu schaffende Rolle von *health information counsellors* [87], die Expertise in IT, Statistik, Recht und Kommunikation vereinen und somit als Bindeglied zwischen Patientin und datenintensiver Klinik fungieren könnten. In dieser Rolle würden sie Informationen filtern, für medizinische Laien verständlich und so für Arzt-Patientengespräche anschlussfähig machen, die das Ideal eines *shared-decision making* [88, 89] verfolgen.

3.4 IT

Datensouveränität erfordert technologische Infrastruktur, um Möglichkeiten zur Kontrolle auch konkret umzusetzen. Das bedeutet im Umkehrschluss nicht, dass jede technische Möglichkeit auch wirklich einen Teil zur Lösung beitragen kann. Ebenso wenig wäre es sinnvoll oder zielführend, im Sinne eines technologischen Solutionismus [90] allein technologische Lösungen zu fokussieren. Vielmehr muss gerade ausgehend von den bisherigen Überlegungen zur Datensouveränität als einem normativen Ankerkonzept geprüft werden, wie ein Dynamic Consent zwischen Datengebern, -nutzern und -verarbeitern technisch so gestaltet werden kann, dass Individuen eine tatsächliche Kontrollmöglichkeit erhalten.

14. **Stewardship etablieren:** Mit *Stewardship* rund um Datenbestände ist deren verantwortliche und nachhaltige Verwaltung und Pflege angesprochen. Durch diesen Umgang können die von Individuen anvertrauten Daten für Forschung und Versorgung nutzbar gemacht und gehalten werden. Damit dies gelingt, ist die Erfüllung bestimmter technischer Voraussetzungen erforderlich. So artikulieren beispielsweise die FAIR-Leitprinzipien [49] Gütekriterien für wissenschaftliche Daten mit dem Ziel, sie für Erkenntnis- und Innovationsprozesse zugänglich zu machen: Daten sollten zunächst für interessierte Wissenschaftler *auffindbar* (findable) sein. Ferner sollten Daten *zugänglich* (accessible) sein. Dazu bieten sich die Nutzung und Verfügbarmachung von Metadaten und Identifikatoren sowie die Verwendung standardisierter Protokolle in der Datenverarbeitung an. Schließlich sollten Daten *interoperabel* (interoperable) sein. Damit ist die Beschaffenheit von Systemen gemeint, Information austauschen und nutzen zu können. Sie hat sowohl technische (z. B. die Verfügbarkeit von Schnittstellen), syntaktische (z. B. Format und Struktur der Daten), semantische (z. B. verwendete medizinische Konzepte) und organisationale (die Nutzbarmachung von Informationsaustausch in organisationalen Workflows) Aspekte [91]. Durch informative Beschreibung, transparente Zugangslizenzen und die Übereinstimmung mit sektorspezifischen Formaten und Standards sollen Daten ferner für andere Forschungsaktivitäten *wiederverwendbar* (reusable) sein.
15. **Weitere Gütekriterien von Datenformaten und Datenverarbeitungssystemen definieren:** Angesichts sich stetig wandelnder Wissens- und Forschungsprozesse erscheint es unwahrscheinlich, dass sich Anforderungen an Datenformate dauerhaft festschreiben lassen. Neben der Übereinstimmung mit Gütekriterien bedarf es eines kontinuierlichen wissenschaftlichen und gesellschaftlichen Diskurses (siehe Empfehlung 11) über die Bewertung dieser Kriterien und ggf. die Notwendigkeit, sie zu modifizieren, kontextsensitiv zu spezifizieren und um weitere Gütekriterien zu ergänzen.
16. **Robuste Architekturen zur Umsetzung von Stewardship fordern und fördern:** Angesichts sich immer wieder ereignender Datenlecks und Hackerangriffe, beispielsweise kürzlich im Zusammenhang mit einer umfangreichen Datenbank von psychiatrischen Behandlungen im finnischen Gesundheitssystem [92], ist die Bedeutung robuster Sicherheitsarchitekturen nicht hoch genug einzuschätzen. Verschlüsselungstechnologien und dezentralisierte Speicherung sind dabei nur zwei Beispiele für Optionen, die sich zum Verfolgen dieser Ziele als hilfreich erweisen könnten.

17. **Kontrollierbarkeit bereits bei der Konzeptualisierung von datenverarbeitenden Systemen fokussieren:** Wenn Autoren bei der Gestaltung datenintensiver Systeme von Ethik [93] oder Privatheit [94] *by design* oder der *Einbettung* von Ethik in den Innovationsprozess sprechen, so ist der Gedanke, diese nicht im Nachhinein oder bei der Ausrollung einer Technologie in den Blick zu nehmen, sondern schon bei der Konzeption und Entwicklung als zentralen Gesichtspunkt zu berücksichtigen, sodass sie im Idealfall *by default* bestimmte Kriterien erfüllen.
18. **Überprüfbarkeit von Übereinstimmung mit Gütekriterien ermöglichen:** Die Umsetzung von Gütekriterien und Benchmarks für Zielgrößen wie Robustheit und Kontrollierbarkeit sollte für die beteiligten Akteure überprüfbar und nachvollziehbar sein. Durch obligatorische Evaluationen und Audits könnten Qualitätsstandards sowohl eingefordert als auch sichtbar gemacht werden. Erst durch Überprüfbarkeit kann Fehlverhalten problematisiert, Verantwortlichkeit zugeschrieben und die Erarbeitung konstruktiver Lösungen vorangetrieben werden.
19. **Systemdesigns zur Ausübung von Dynamic Consent implementieren:** Auf der Ebene der Architektur von Datenverarbeitungssystemen setzt Datensouveränität technische Mechanismen zur Umsetzung von Kontrollierbarkeit voraus, die es Nutzerinnen erlauben, Datenströme durch Dynamic Consent (siehe Kap. 2) zu steuern. Gemeint sind damit Systeme, die Daten entsprechend den Erwartungen der Nutzerinnen schützen, den Nutzerinnen erlauben, in verschiedene Arten und Zwecke der Verarbeitung einzuwilligen und den Zugang zu einmal verfügbar gemachten Daten auf Wunsch wieder zu beschränken. Eine Grundvoraussetzung ist dafür zunächst, Gesundheitsdaten in digitaler Form für das jeweilige Individuum zugänglich und handhabbar zu machen. Im Anschluss bedarf es zur Umsetzung des Dynamic Consent benutzerfreundlicher Interfaces zur Kontrollierbarkeit von Zugang, Verarbeitung und Rückholung.
20. **Technologische Formen von Treuhänderschaft weiterentwickeln:** Technologische Treuhänder bringen die datenbezogenen Präferenzen der Individuen in Verarbeitungsprozesse ein. Zu diesem Zweck sind Architekturen nötig, welche Präferenzen über benutzerfreundliche Schnittstellen erheben und den Erwartungen der Individuen an Zugang und Verarbeitung ihrer Daten genügen. Ob eine technologische Form von Treuhänderschaft gelingt, hängt jedoch auch von weiteren Faktoren ab. Als ein Beispiel sei auf Modelle verwiesen, in denen Blockchain zur Kontrollierbarkeit von Gesundheitsdaten in Forschung [95] und Versorgung vorgeschlagen wird [96–98], zum Beispiel

indem Einwilligung in Datenverarbeitung sowie Parameter wie deren Zweckbindung in der Blockchain protokolliert und Zugriffe nur in Übereinstimmung mit diesen Vorgaben ermöglicht werden. Auf den Hype um Blockchain-Technologie ist aber auch der Vorbehalt gefolgt, dass sie ein Buzzword und ihre Implementierungen komplex und ressourcenintensiv sei. Ferner darf die Tatsache, dass in der Blockchain durch kryptographische Methoden die Struktur des Systems selbst für die Integrität von Transaktionen bürgt nicht darüber hinwegtäuschen, dass menschliche Akteure über Gestaltung, Zugang und Einsatz des Systems bestimmen. Das Gelingen technologischer Treuhänderschaft hängt somit neben der Wahl der Technologie selbst nicht zuletzt davon ab, ob und wie Debatten zur Modifikation eines Systems und dessen Einsatz zugelassen und Machtasymmetrien vermieden werden. Sofern sich Anwendungen im Rahmen solcher Prozesse als tragfähig erweisen, stellen sie hilfreiche Instrumente zur Umsetzung von Datensouveränität dar.

21. **Datenagenten implementieren:** Um Kontrollierbarkeit technisch umsetzbar zu machen, sind Schnittstellen und Software-Agenten in und an datenverarbeitenden Systemen zu implementieren, anhand derer ein Dynamic Consent des Individuums wirksam eingebracht werden kann. *Personal Information Management Systems* (PIMS) bieten den Nutzern beispielsweise differenzierte Steuerungsmöglichkeiten in Bezug darauf, welche Verarbeiter zu welchen Zwecken Zugang auf ihre Daten erhalten. Solche Ansätze können gewinnbringend mit weiteren Anforderungen an Systemarchitekturen kombiniert werden. So gehört es zum Ansatz des sog. *Personal Health Train,* dass Daten nicht weitergegeben, sondern Verarbeitungsprozesse vor Ort in sicherer Umgebung durchgeführt werden [99], verbunden mit differenzierten Kontrollmöglichkeiten für die Datensubjekte *via* Software-Agenten oder „Broker“, mittels derer sie die Freigabe steuern können [100].
22. **Anwendungskontexte bei der Beurteilung datenintensiver Systeme kontinuierlich berücksichtigen:** Auch wenn ethische und rechtliche Gesichtspunkte im Design-Prozess eines Systems berücksichtigt wurden, ist fortwährende Reflexion in konkreten Anwendungssituationen nötig, um den konkreten Bedeutungsgehalt der in Kap. 1 dargestellten Aspekte von Datensouveränität zu erörtern. So kann beispielsweise Privatheit eng als negativ-protektiver Anspruch [27] oder weiter als die Übereinstimmung von Datenströmen mit kontextuellen Normen und Erwartungen [101] verstanden werden. Im erstgenannten Sinn kann die Beschränkung von Zugang und Verarbeitung *by design* für bestimmte Anwendungskontexte vollkommen angemessen sein, wohingegen in anderen – wie in der oben angesprochenen Möglichkeit zur Datenspende – gerade mehr gefordert ist, und zwar nicht nur ein

Recht allein gelassen zu werden durchzusetzen, sondern darüber hinaus differenziert-kontrollierbar Daten mit anderen zu teilen.

Die Datenethikkommission der Bundesregierung hat vorgeschlagen, algorithmische Systeme in fünf sogenannte Kritikalitätsstufen zu sortieren, die sich aus dem „Schädigungspotential" der Systeme ableiten lassen und in einer „Kritikalitätspyramide" visualisiert sind [102]. Stufe 2–4 sollen dabei bereichsspezifisch reguliert und Stufe 5 verboten werden. Das kürzlich erschienene „Proposal for a Regulation on a European approach for Artificial Intelligence" [105] der Europäischen Kommission arbeitet mit einem ähnlichen Kritikalitätsmodell. Einem algorithmischen System ein Schädigungspotential zuzuschreiben wirft die Herausforderung auf, dass Funktionsweisen und Effekte eines Systems schwerlich in abstracto fassbar sind. Der Grad an möglichem Schaden oder Nutzen ergibt sich zumeist erst bei der Implementierung des Systems in praktische Vollzüge sowie seiner Konfiguration zur Bearbeitung eines bestimmten Problems [103, 104]. Schaden und Nutzen hängen also nicht alleine am algorithmischen System selbst, sondern zumindest ebenso an dem konkreten Anwendungskontext, der zeitlichen Dauer der Anwendung, den Kontrollmöglichkeiten und den Formen der Zustimmung oder Ablehnung. Mit Datensouveränität und dem Hinweis auf *Output*-Orientierung wird genau dies betont.

Was Sie aus diesem *essential* mitnehmen können

- In diesem Beitrag wurde Datensouveränität untersucht und als normatives Ankerkonzept mit Individualfokus und Grundrechtsbezug auf den Gesundheitsbereich angewandt.
- Datensouveränität meint die Befähigung von Akteuren zur Wahrnehmung von Kontrollansprüchen rund um die Verwendung sie betreffender Daten. Für datensouveräne Akteure soll kontrollierbar bleiben, wer Zugriff auf diese Daten hat, zu welchen Zwecken sie von wem verarbeitet werden dürfen, und vor allem wie Zugang und Verarbeitung die Freiheitsvollzüge der Akteure beeinflussen.
- Zur Ermöglichung von Datensouveränität im Gesundheitsbereich entfalten wir die folgenden Steuerungs- und Strukturelemente: Dynamic Consent, den Schutz eigener Daten, die Implementierung von Datentreuhändern sowie die Ermöglichung der Datenspende.
- Datensouveränität erfordert multidimensionale Regelungsansätze auf verschiedenen Governance-Ebenen. Wir formulieren insgesamt 22 Empfehlungen für die Bereiche Hard Law, Soft Law, Teilhabe und IT.

P. Hummel et al., *Datensouveränität,* essentials,
https://doi.org/10.1007/978-3-658-33755-1

Literatur

1. Bundesregierung. (2020). *Gemeinsam. Europa wieder stark machen. Programm der deutschen EU-Ratspräsidentschaft 1. Juli bis 31. Dezember 2020*. Berlin: Auswärtiges Amt der Bundesrepublik Deutschland. https://www.eu2020.de/blob/2360246/d0e7b758973f0b1f56e74730bfdaf99d/pdf-programm-de-data.pdf.
2. Hummel, P., Braun, M., Augsberg, S., & Dabrock, P. (2018). Sovereignty and Data Sharing. *ITU Journal: ICT Discoveries*, *2*. https://www.itu.int/en/journal/002/Documents/ITU2018-11.pdf.
3. Couture, S., & Toupin, S. (2019). What does the notion of "sovereignty" mean when referring to the digital? *New Media & Society*, *21*(10), 2305–2322. https://doi.org/10.1177/1461444819865984.
4. Friedrichsen, M., & Bisa, P.-J. (Hrsg.). (2016). *Digitale Souveränität*. Wiesbaden: Springer VS. https://doi.org/10.1007/978-3-658-07349-7.
5. De Mooy, M. (2017). *Rethinking Privacy Self-Management and Data Sovereignty in the Age of Big Data: Considerations for Future Policy Regimes in the United States and the European Union*. Bertelsmann Stiftung.
6. Deutscher Ethikrat. (2017). *Big Data und Gesundheit. Datensouveränität als informationelle Freiheitsgestaltung*. Berlin: Deutscher Ethikrat. https://www.ethikrat.org/fileadmin/Publikationen/Stellungnahmen/deutsch/stellungnahme-big-data-und-gesundheit.pdf.
7. Mueller, M. (2017). *Will the Internet Fragment?: Sovereignty, Globalization and Cyberspace*. Cambridge: Polity Press.
8. Peterson, Z. N. J., Gondree, M., & Beverly, R. (2011). A Position Paper on Data Sovereignty: The Importance of Geolocating Data in the Cloud. In *Proceedings of the 3rd USENIX Conference on Hot Topics in Cloud Computing*. Berkeley, CA, USA: USENIX Association. https://www.usenix.org/legacy/events/hotcloud11/tech/final_files/Peterson.pdf.
9. De Filippi, P., & McCarthy, S. (2012). Cloud Computing: Centralization and Data Sovereignty. *European Journal of Law and Technology*, *3*(2).
10. Irion, K. (2013). Government Cloud Computing and National Data Sovereignty. *Policy & Internet*, *4*(3–4), 40–71.
11. Hummel, P., Braun, M., Tretter, M., & Dabrock, P. (2021). Data Sovereignty: A Review. *Big Data & Society*. https://doi.org/10.1177/2053951720982012.

P. Hummel et al., *Datensouveränität,* essentials,
https://doi.org/10.1007/978-3-658-33755-1

12. Klein, R. A. (2016). *Depotenzierung der Souveränität: Religion und politische Ideologie bei Claude Lefort, Slavoj Zizek und Karl Barth.* Tübingen: Mohr Siebeck.
13. Maritain, J. (1951). *Man and the State.* Chicago: Chicago Universit Press 1998.
14. Esposito, R. (2018). *A philosophy for Europe: from the outside* (English edition.). Cambridge, UK ; Medford, MA, USA: Polity Press.
15. Kukutai, T., & Taylor, J. (Hrsg.). (2016). *Indigenous Data Sovereignty* (1st Aufl.). ANU Press. https://doi.org/10.22459/CAEPR38.11.2016.
16. Harding, A., Harper, B., Stone, D., O'Neill, C., Berger, P., Harris, S., & Donatuto, J. (2012). Conducting Research with Tribal Communities: Sovereignty, Ethics, and Data-Sharing Issues. *Environmental Health Perspectives*, *120*(1), 6–10. https://doi.org/10.1289/ehp.1103904.
17. James, R., Sahota, P., Parker, M., Dillard, D., Sylvester, I., Lewis, J., … for the Kiana Group. (2014). Exploring pathways to trust: a tribal perspective on data sharing. *Genetics in Medicine*, *16*(11), 820–826. https://doi.org/10.1038/gim.2014.47.
18. Walker, J., Lovett, R., Kukutai, T., Jones, C., & Henry, D. (2017). Indigenous health data and the path to healing. *The Lancet*, *390*(10107), 2022–2023. https://doi.org/10.1016/S0140-6736(17)32755-1.
19. The First Nations Information Governance Centre. (2019). First Nations data sovereignty in Canada. *Statistical Journal of the IAOS*, *35*(1), 47–69. https://doi.org/10.3233/SJI-180478.
20. Mittelstadt, B., & Floridi, L. (2016). The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts. *Science and Engineering Ethics*, *22*(2), 303–341.
21. Sweeney, L. (2000). *Simple Demographics Often Identify People Uniquely.* Data Privacy Working Paper 3, Carnegie Mellon University, Pittsburgh. https://dataprivacylab.org/projects/identifiability/paper1.pdf.
22. Organisation for Economic Co-operation and Development. (2019). *Artificial intelligence in society.* https://doi.org/10.1787/eedfee77-en.
23. Taylor, L., Floridi, L., & van der Sloot, B. (Hrsg.). (2017). *Group Privacy: New Challenges of Data Technologies.* Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-46608-8.
24. Mittelstadt, B. (2017). From Individual to Group Privacy in Big Data Analytics. *Philosophy & Technology*, *30*(4), 475–494. https://doi.org/10.1007/s13347-017-0253-7.
25. Hornung, G., & Schnabel, C. (2009). Data protection in Germany I: The population census decision and the right to informational self-determination. *Computer Law & Security Review*, *25*(1), 84–88. https://doi.org/10.1016/j.clsr.2008.11.002.
26. Véliz, C. (2020). *Privacy is power*. London: Bantam Press.
27. Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review*, *4*(5), 193. https://doi.org/10.2307/1321160.
28. Cassel, C., & Bindman, A. (2019). Risk, Benefit, and Fairness in a Big Data World. *JAMA*, *322*(2), 105. https://doi.org/10.1001/jama.2019.9523.
29. Hummel, P., Braun, M., & Dabrock Peter. (2020). Own Data? Ethical Reflections on Data Ownership. *Philosophy & Technology.* https://doi.org/10.1007/s13347-020-00404-9.
30. Lanier, J. (2013). *Who owns the future?* New York: Simon & Schuster.
31. Montgomery, J. (2017). Data Sharing and the Idea of Ownership. *The New Bioethics*, *23*(1), 81–86.

32. Thouvenin, F. (2017). Wem gehören meine Daten? Zu Sinn und Nutzen einer Erweiterung des Eigentumsbegriffs. *Schweizerische Juristen-Zeitung*, *113*, 21–32.
33. Pearce, H. (2018). Personality, Property and Other Provocations: *European Data Protection Law Review*, *4*(2), 190–208. https://doi.org/10.21552/edpl/2018/2/8.
34. Fezer, K.-H. (2017). Dateneigentum der Bürger. *Zeitschrift für Datenschutz*, (3), 99–105.
35. Fezer, K.-H. (2017). Dateneigentum. *MultiMedia und Recht*, (1), 3–5.
36. Bundesministerium für Verkehr und digitale Infrastruktur (Hrsg.). (2017, August). „Eigentumsordnung" für Mobilitätsdaten? Eine Studie aus technischer, ökonomischer und rechtlicher Perspektive. https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/eigentumsordnung-mobilitaetsdaten.pdf.
37. Prainsack, B., & Buyx, A. (2017). *Solidarity in Biomedicine and Beyond*. Cambridge: Cambridge University Press.
38. Vayena, E., & Tasioulas, J. (2015). „We the Scientists": a Human Right to Citizen Science. *Philosophy & Technology*, *28*(3), 479–485. https://doi.org/10.1007/s13347-015-0204-0.
39. Derrida, J. (1992). *Given Time: I. Counterfeit Money*. (P. Kamuf, Übers.). Chicago: University of Chicago Press.
40. Hénaff, M. (2010). *The Price of Truth: Gift, Money, and Philosophy*. (J.-L. Morhange, Übers.). Stanford, California: Stanford University Press.
41. Bedorf, T. (2010). Gabe, Recht und Ethik in Hénaffs anthropologischer Genealogie der Anerkennung. *Westend*, *7*, 123–132.
42. Hummel, P., Braun, M., & Dabrock, P. (2019). Data Donations As Exercises Of Sovereignty. In J. Krutzinna & L. Floridi (Hrsg.), *The Ethics Of Medical Data Donation* (S. 23–54). Cham: Springer.
43. Chen, J. H., & Asch, S. M. (2017). Machine Learning and Prediction in Medicine – Beyond the Peak of Inflated Expectations. *New England Journal of Medicine*, *376*(26), 2507–2509. https://doi.org/10.1056/NEJMp1702071.
44. Maughan, T. (2017). The Promise and the Hype of 'Personalised Medicine'. *The New Bioethics*, *23*(1), 13–20. https://doi.org/10.1080/20502877.2017.1314886.
45. Chowkwanyun, M., Bayer, R., & Galea, S. (2018). "Precision" Public Health – Between Novelty and Hype. *New England Journal of Medicine*, *379*(15), 1398–1400. https://doi.org/10.1056/NEJMp1806634.
46. Richter, G., Krawczak, M., Lieb, W., Wolff, L., Schreiber, S., & Buyx, A. (2018). Broad consent for health care–embedded biobanking: understanding and reasons to donate in a large patient sample. *Genetics in Medicine*, *20*(1), 76–82. https://doi.org/10.1038/gim.2017.82.
47. Strech, D., Graf von Kielmansegg, S., Zenker, S., Krawczak, M., & Semler, S. (2020). *„Datenspende" – Bedarf für die Forschung, ethische Bewertung, rechtliche, informationstechnologische und organisatorische Rahmenbedingungen* (Wissenschaftliches Gutachten erstellt für das Bundesministerium für Gesundheit). Berlin. https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/5_Publikationen/Ministerium/Berichte/Gutachten_Datenspende.pdf.
48. Lynch, C. (2008). How do your data grow? *Nature*, *455*(7209), 28–29. https://doi.org/10.1038/455028a.

49. Wilkinson, M. D., Dumontier, M., Aalbersberg, Ij. J., Appleton, G., Axton, M., Baak, A., … Mons, B. (2016). The FAIR Guiding Principles for scientific data management and stewardship. *Scientific Data*, *3*(1), 1–9. https://doi.org/10.1038/sdata.2016.18.
50. Radlanski, P. (2016). *Das Konzept der Einwilligung in der datenschutzrechtlichen Realität* (Bd. 5). Tübingen: Mohr Siebeck.
51. Tinnefeld, M.-T., Buchner, B., & Petri, T. (2012). *Einführung in das Datenschutzrecht: Datenschutz und Informationsfreiheit in europäischer Sicht* (5. Aufl.). München: Oldenbourg.
52. Ernst, S. (2017). Die Einwilligung nach der Datenschutzgrundverordnung. *Zeitschrift für Datenschutz*, (3), 110–113.
53. Augsberg, S. (2016). Big Data im Recht der Transplantationsmedizin – Vom "Ende der Theorie" zum "Ende der Aporie"? *Medizinrecht*, *34*(9), 699–705. https://doi.org/10.1007/s00350-016-4372-4.
54. Augsberg, S., & von Ulmenstein, U. (2018). Modifizierte Einwilligungserfordernisse: Kann das Datenschutzrecht vom Gesundheitsrecht lernen? *GesundheitsRecht*, (6), 341–347.
55. Steinsbekk, K. S., Kåre Myskja, B., & Solberg, B. (2013). Broad consent versus dynamic consent in biobank research: Is passive participation an ethical problem? *European Journal of Human Genetics*, *21*(9), 897–902. https://doi.org/10.1038/ejhg.2012.282.
56. Wee, R. (2013). Dynamic consent in the digital age of biology. *Journal of Primary Health Care*, *5*(3), 259–261.
57. Kaye, J., Whitley, E. A., Lund, D., Morrison, M., Teare, H., & Melham, K. (2015). Dynamic consent: a patient interface for twenty-first century research networks. *European Journal of Human Genetics*, *23*(2), 141–146. https://doi.org/10.1038/ejhg.2014.71.
58. Williams, H., Spencer, K., Sanders, C., Lund, D., Whitley, E. A., Kaye, J., & Dixon, W. G. (2015). Dynamic Consent: A Possible Solution to Improve Patient Confidence and Trust in How Electronic Patient Records Are Used in Medical Research. *JMIR Medical Informatics*, *3*(1), e3. https://doi.org/10.2196/medinform.3525.
59. Budin-Ljøsne, I., Teare, H. J. A., Kaye, J., Beck, S., Bentzen, H. B., Caenazzo, L., … Mascalzoni, D. (2017). Dynamic Consent: a potential solution to some of the challenges of modern biomedical research. *BMC Medical Ethics*, *18*(1), 10. https://doi.org/10.1186/s12910-016-0162-9.
60. DNV GL, Group Research and Development, Precision Medicine Program. (2021). *Dynamic Consent in Clinical Genetics*. Høvik: DNV GL AS. https://www.dnvgl.com/research/precision-medicine/dynamic-consent-whitepaper.html.
61. Medizininformatik-Initiative. (2019). *Stellungnahme der AG Consent der Medizininformatik-Initiative zu patientenindividueller Datennutzungstransparenz und Dynamic Consent*. https://www.medizininformatik-initiative.de/sites/default/files/2019-09/MII_AG-Consent_Stellungnahme-Consent-Modelle_v05.pdf.
62. Albers, M. (2013). Rechtsrahmen und Rechtsprobleme bei Biobanken. *Medizinrecht*, *31*(8), 483–491. https://doi.org/10.1007/s00350-013-3471-8.
63. von Ulmenstein, U. (2020). Datensouveränität durch repräsentative Rechtswahrnehmung Begriffliche Prägung und normative Gestaltung sogenannter „Datentreuhänder". *Datenschutz und Datensicherheit*, *44*(8), 528–534. https://doi.org/10.1007/s11623-020-1319-8.

64. Gutachten der Datenethikkommission der Bundesregierung. (2019). Bundesministerium des Innern, für Bau und Heimat und Bundesministerium der Justiz und für Verbraucherschutz. https://datenethikkommission.de/wp-content/uploads/191128_DEK_Gutachten_bf_b.pdf.
65. Rat für Informationsinfrastrukturen. (2020). *Stellungnahme des Rates für Informationsinfrastrukturen (RfII): Datentreuhandstellen gestalten – Zu Erfahrungen der Wissenschaft* (S. 8). https://www.rdm.kit.edu/downloads/RfII-Stellungnahme_Datentreuhand_2020.pdf.
66. Bizer, J. (1999). Der Datentreuhänder, Lösungsmodell für den Datenzugang der Forschung. *Datenschutz und Datensicherheit*, 392–395.
67. Ihle, P. (2008). Datenschutzrechtliche und methodische Aspekte beim Aufbau einer Routinedatenbasis aus der Gesetzlichen Krankenversicherung zu Forschungszwecken. *Bundesgesundheitsblatt – Gesundheitsforschung – Gesundheitsschutz*, *51*(10), 1127–1134.
68. Horn, N., Riechert, A., & Müller, C. (2017). Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen. In *Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen* (Bd. Teil A, S. 5–58). Leipzig.
69. Richter, F. (2017). Aus Sicht der Stiftung Datenschutz – „Der Einwilligungsassistent und die Chancen eines personal data ecosystem". *Privacy in Germany. Datenschutz und Compliance*, *3*, 122–123. https://doi.org/10.37307/j.2196-9817.2017.03.10.
70. Weichert, T. (2006). Auskunftsanspruch in verteilten Systemen: Zur Einschaltung von Datentreuhändern. *Datenschutz und Datensicherheit – DuD*, *30*(11), 694–699. https://doi.org/10.1007/s11623-006-0194-2.
71. Lind, H.-G., & Suckfüll, H. (2013). *Die Initiative zu einer Deutschen Daten-Treuhand (DEDATE) als Ultima Ratio der Persönlichen Digitalen Datenwirtschaft (PDD)*. Leipzig: Fraunhofer MOEZ. https://www.imw.fraunhofer.de/content/dam/moez/de/documents/Working_Paper/DEDATE-gesamt.pdf.
72. Buchner, B. (2018). Datenmacht. *Wettbewerb in Recht und Praxis*, (10), I.
73. Bisges, M. (2017). Personendaten, Wertzuordnung und Ökonomie – Kein Vergütungsanspruch Betroffener für die Nutzung von Personendaten. *MultiMedia und Recht*, (5), 301–306.
74. Fezer, K.-H. (2018). *Repräsentatives Dateneigentum. Ein zivilgesellschaftliches Bürgerrecht. Studie im Auftrag der Konrad-Adenauer-Stiftung e. V. zum Thema „Einführung eines besonderes Rechts an Daten"*. Sankt Augustin Berlin: Konrad-Adenauer-Stiftung e. V.
75. Unseld, F. (2011). Die Übertragbarkeit von Persönlichkeitsrechten. *Gewerblicher Rechtsschutz und Urheberrecht*, (11), 982–988.
76. Zech, H. (2015). „Industrie 4.0" – Rechtsrahmen für eine Datenwirtschaft im digitalen Binnenmarkt. *Gewerblicher Rechtsschutz und Urheberrecht*, (12), 1151–1160.
77. Reimer, R. (o. J.). Schwärme als Inhaber von Rechten? *WebDok 109/2018*. https://doi.org/10.7328/jurpcb2018338109.
78. Schefzig, J. (2014). Big Data = Personal Data? Der Personenbezug von Daten bei Big Data Analysen, 772–778.

79. Weichert, T. (2013). Die Meinungsfreiheit des Algorithmus. In F. Roggan & D. Busch (Hrsg.), *Das Recht in guter Verfassung? – Festschrift für Martin Kutscha* (S. 147–160). https://doi.org/10.5771/9783845251486-147.
80. Wachter, S., & Mittelstadt, B. (2019). A Right to Reasonable Inferences: Re-thinking Data Protection Law in the Age of Big Data and AI. *Columbia Business Law Review*, *2019*(2), 494–620. https://doi.org/10.7916/cblr.v2019i2.3424.
81. Wachter, S., Mittelstadt, B., & Russell, C. (2017). Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3063289.
82. Mausbach, J. (2018, September 5). DSI Insights: Einwilligung in Forschung ist keine Einbahnstrasse! *inside-it.ch.* Abgerufen 2. Januar 2020, von https://www.inside-it.ch/articles/52128.
83. EuGH, 20.12.2017 – C-434/16 – Antworten eines Prüflings und Anmerkungen des Prüfers als personenbezogene Daten., 2018 NJW 767–769 (EuGH 20. Dezember 2017). Urt.
84. Augsberg, S. (2019). Regelsetzung als staatlich-privat interaktiver Prozess – Vom „Steuerungsdurcheinander" zur Regulierungsstrategie? In F. Möslein (Hrsg.), *Regelsetzung im Privatrecht* (S. 95–120). Mohr Siebeck. https://doi.org/10.1628/978-3-16-156196-2.
85. Mair, N., Pawlowska, I. M., Lins, S., & Sunyaev, A. (2020). Die Zertifizierung nach der DSGVO. *Zeitschrift für Datenschutz*, (9), 445–449.
86. Krüger-Brand, H. E. (2019). Digitale Gesundheitskompetenz: Datensouveränität als Ziel. *Deutsches Ärzteblatt*, *4*, 164–168.
87. Fiske, A., Buyx, A., & Prainsack, B. (2019). Health Information Counselors: A New Profession for the Age of Big Data. *Academic Medicine*, *94*(1), 37–41. https://doi.org/10.1097/ACM.0000000000002395.
88. Makoul, G., & Clayman, M. L. (2006). An integrative model of shared decision making in medical encounters. *Patient Education and Counseling*, *60*(3), 301–312. https://doi.org/10.1016/j.pec.2005.06.010.
89. Elwyn, G., Frosch, D., Thomson, R., Joseph-Williams, N., Lloyd, A., Kinnersley, P., … Barry, M. (2012). Shared Decision Making: A Model for Clinical Practice. *Journal of General Internal Medicine*, *27*(10), 1361–1367. https://doi.org/10.1007/s11606-012-2077-6.
90. Morozov, E. (2013). *To save everything, click here: the folly of technological solutionism.* New York: PublicAffairs.
91. Lehne, M., Sass, J., Essenwanger, A., Schepers, J., & Thun, S. (2019). Why digital medicine depends on interoperability. *npj Digital Medicine*, *2*(1), 1–5. https://doi.org/10.1038/s41746-019-0158-1.
92. Böck, H. (2020). Finnland: Datenleck von Psychotherapie-Klinik für Erpressung genutzt – Golem.de. https://www.golem.de/news/finnland-datenleck-von-psychotherapie-klinik-fuer-erpressung-genutzt-2010-151742.html.
93. van Wynsberghe, A., & Robbins, S. (2014). Ethicist as Designer: A Pragmatic Approach to Ethics in the Lab. *Science and Engineering Ethics*, *20*(4), 947–961. https://doi.org/10.1007/s11948-013-9498-4.
94. Schaar, P. (2010). Privacy by Design. *Identity in the Information Society*, *3*(2), 267–274. https://doi.org/10.1007/s12394-010-0055-x.

95. Porsdam Mann, S., Savulescu, J., Ravaud, P., & Benchoufi, M. (2020). Blockchain, consent and prosent for medical research. *Journal of Medical Ethics*, medethics-2019-105963. https://doi.org/10.1136/medethics-2019-105963.
96. Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using Blockchain for Medical Data Access and Permission Management. In *2016 2nd International Conference on Open and Big Data (OBD)* (S. 25–30). https://doi.org/10.1109/OBD.2016.11.
97. Esposito, C., De Santis, A., Tortora, G., Chang, H., & Choo, K.-K. R. (2018). Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy? *IEEE Cloud Computing*, *5*(1), 31–37. https://doi.org/10.1109/MCC.2018.011791712.
98. Cichosz, S. L., Stausholm, M. N., Kronborg, T., Vestergaard, P., & Hejlesen, O. (2019). How to Use Blockchain for Diabetes Health Care Data and Access Management: An Operational Concept. *Journal of Diabetes Science and Technology*, *13*(2), 248–253. https://doi.org/10.1177/1932296818790281.
99. Beyan, O., Choudhury, A., van Soest, J., Kohlbacher, O., Zimmermann, L., Stenzhorn, H., … Dekker, A. (2020). Distributed Analytics on Sensitive Medical Data: The Personal Health Train. *Data Intelligence*, *2*(1–2), 96–107. https://doi.org/10.1162/dint_a_00032.
100. Blankertz, A. (2020). *Designing Data Trusts. Why We Need to Test Consumer Data Trusts Now*. Berlin: Stiftung Neue Verantwortung e. V. https://www.stiftung-nv.de/sites/default/files/designing_data_trusts_d.pdf.
101. Nissenbaum, H. (2009). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, California: Stanford University Press.
102. Datenethikkommission der Bundesregierung (2019). *Gutachten der Datenethikkommission der Bundesregierung*. Bundesministerium des Innern, für Bau und Heimat. https://datenethikkommission.de/wp-content/uploads/191128_DEK_Gutachten_bf_b.pdf.
103. Mittelstadt, B., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society*, *3*(2), 2053951716679679. https://doi.org/10.1177/2053951716679679.
104. Krafft, T. D., & Zweig, K. A. (2019). *Transparenz und Nachvollziehbarkeit algorithmenbasierter Entscheidungsprozesse*. Berlin: Verbraucherzentrale Bundesverband e. V. https://www.vzbv.de/sites/default/files/downloads/2019/05/02/19-01-22_zweig_krafft_transparenz_adm-neu.pdf.
105. Europäische Kommission (2021). *Proposal for a Regulation on a European approach for Artificial Intelligence*. https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-european-approach-artificial-intelligence.