Eine neue Generation des Datenschutzes? Gegenwärtige Unvollständigkeit, mögliche Lösungswege und nächste Schritte

Andrea Martani und Patrik Hummel

1 Einführung

Es gibt mittlerweile kaum einen Bereich in der Lebenswelt, der noch nicht datafiziert ist. Die Verfügbarkeit großer Datenmengen sowie erheblich gesteigerte Rechenleistungen sind die Grundlage für wegbereitende Informationstechnologien, automatisierte Systeme und Künstliche Intelligenz (KI). In der Wirtschaft werden Daten als neues Rohmaterial für Innovation gesehen, das die Entwicklung von Märkten und Unternehmen grundlegend und fortwährend verändern wird (Mayer-Schönberger und Ramge 2018). Daten sind ebenso die Grundlage für innovative Formen biomedizinischer Forschung, beispielsweise die Analyse elektronischer Patientenakten, und für das Versprechen maßgeschneiderter, patientenzentrierter Versorgung durch die Präzisionsmedizin. Datenverarbeitungsprozesse erreichen hohe und nicht immer für alle Betroffenen nachvollziehbare oder antizipierbare Komplexitätsgrade. Während Vernetzung den Weg für Synergien in Wirtschaft, Politik und persönlicher Sphäre bereitet, kann sie auch unerwünschte Informationsflüsse, erlebte Kontrollverluste, Verletzungen der Privatsphäre und neue Formen von Manipulation und Diskriminierung begünstigen. Verschiedene Stakeholder – ob Konsument/-innen, Patient/-innen, Forscher/-innen, Innovator/-innen, oder Regierungen – bringen jeweils eigene Rechte und Interessen in diese Gemengelage ein. Im vorliegenden Beitrag diskutieren wir mit dem Datenschutzrecht *einen* Bezugspunkt,

A. Martani (✉)
Institut für Bio- und Medizinethik, Universität Basel, Bernoullistrasse 28, Basel 4056, Schweiz
E-Mail: andrea.martani@unibas.ch

P. Hummel
Lehrstuhl für Systematische Theologie II (Ethik), Friedrich-Alexander-Universität Erlangen-Nürnberg, Kochstr. 6, Erlangen 91054, Deutschland
E-Mail: patrik.hummel@fau.de

G. Richter et al. (Hrsg.), *Datenreiche Medizin und das Problem der Einwilligung*,
https://doi.org/10.1007/978-3-662-62987-1_3

um die Bandbreite an nicht immer spannungsfrei miteinander in Beziehung stehenden Ansprüchen zu berücksichtigen und auszutarieren. Unter *Datenschutzrecht* verstehen wir dabei den für Datenverarbeitung relevanten gesetzlichen Rahmen sowie dessen Anwendung, z. B. in der Rechtsprechung. Da sich Technologien und Praktiken der Datenverarbeitung beständig weiterentwickeln, kann Datenschutz nicht stillstehen. Wir werden zunächst die Position beschreiben, dass sich wandelnde Realitäten der Datenverarbeitung neue *Generationen* von Datenschutzrecht erfordern (2.). Im Laufe der Diskussion wird unser Augenmerk darauf liegen zu verstehen, was eine solche *Generation* auszeichnet und aus welchen Gründen eine *neue* Generation gefordert werden könnte. Dabei argumentieren wir, dass sich das Datenschutzrecht aktuell mit einer Reihe von offenen Grundsatzfragen konfrontiert sieht, welche sowohl den Weg in Richtung einer nächsten Generation weisen als auch suggerieren, dass Reflexionsbedarf im *Status quo* besteht. Diese Grundsatzfragen entfalten wir entlang drei konzeptioneller Knotenpunkte: der *Gegenstandsbereich (3.1)*, der *Schutzgegenstand* (3.2) und das *Paradigma (3.3)* des Datenschutzrechts. Im Anschluss fokussieren wir die biomedizinische Forschung als einen Kontext, in dem sich weitere bereichsspezifische Fragen bei der Weiterentwicklung des Datenschutzes stellen (4). Schließlich werden wir auf Basis dieser Diskussion Hypothesen formulieren, wie der Übergang zu einer neuen *Generation* ermöglicht werden könnte.

2 Ist es notwendig, Datenschutz neu zu denken?

Die Auffassung, dass der datenschutzrechtliche Rahmen mangelhaft ist, ist nicht neu. Seit den ersten Datenschutz-Gesetzgebungen in den 1970er-Jahren haben technologische und gesellschaftliche Entwicklungen diesen Rahmen immer wieder herausgefordert, infrage gestellt, und die fortwährende Notwendigkeit seiner Weiterentwicklung unterstrichen. Mayer-Schönberger (1997) identifiziert aufeinanderfolgende *Generationen* des Datenschutzes, wobei sich der Übergang von einer zu der nächsten immer aus der Unzulänglichkeit der vorausgehenden ableitet.[1] So sei das Ziel der ersten Generation des Datenschutzes in den 70er-Jahren gewesen, zunehmend expansive Formen der Datenverarbeitung *zu bändigen*, für die damals noch eine verhältnismäßig kleine Gruppe von Akteuren (vor allem Staaten oder große Unternehmen, die sich die ersten Computer leisten konnten) verantwortlich waren. Mit zunehmender Anzahl der Datenbanken und -verarbeiter sowie der steigenden Bedeutung von Datenverarbeitung in verschiedenen

[1]Neben Mayer-Schönbergers Position gibt es auch andere Interpretationen des Generationenbegriffs mit Bezug zum Datenschutz. Poullet (2005, 2010) unterscheidet z. B. zwischen drei Generationen, die erste bestimmt durch Art. 8 der Europäischen Menschenrechtskonvention, die zweite durch die Datenschutzkonvention 108 des Europarats und die Datenschutzrichtlinie der EU (95/46/EG) sowie eine mögliche dritte durch die Datenschutzrichtlinie für elektronische Kommunikation der EU (2002/58/EG).

Lebensbereichen wurde die Herangehensweise der ersten Generation aufgegeben und eine neue Generation entwickelt. Diese konzentrierte sich laut Mayer-Schönberger mehr auf die Rechte des Individuums und seine Privatsphäre. Ziel war die Befähigung einzelner Personen, eigene Abwehrlinien gegen unerwünschte Datenverarbeitung und Verletzungen von Datensicherheit einziehen zu können. Aber auch diese Herangehensweise gelangte letztlich an ihre Grenzen angesichts eines kontinuierlichen Datenflusses, der für viele Aktivitäten (z. B. die Leistungserbringungen des Sozialstaats) zentral geworden war. Deshalb wurde eine dritte Generation des Datenschutzes kreiert, in der das Prinzip der informationellen Selbstbestimmung zentral wurde, damit Personen selbst (mit-)bestimmen können, unter welchen Bedingungen ihre Daten verarbeitet werden. Nach kurzer Zeit war jedoch offensichtlich, dass die praktische Umsetzung der informationellen Selbstbestimmung durch die schwache Verhandlungsposition der einzelnen Personen gegenüber großen datenverarbeitenden Institutionen verhindert wurde. Dies hatte das Entstehen einer vierten Generation des Datenschutzes durch Gesetzgebungsakte wie die Europäische Datenschutzrichtlinie (Richtlinie 95/46/EG) in den 90er-Jahren zur Folge. Wie wir sogleich erörtern werden, sehen manche auch die kürzlich eingeführte Datenschutz-Grundverordnung (DSGVO) in dieser Tradition.

Unabhängig davon, ob man den Hypothesen über die jeweiligen Ursachen der Übergänge zu neuen Generationen des Datenschutzes zustimmt, hat es zwei Vorteile, seine Entwicklung in generationeller Hinsicht zu interpretieren. Erstens hat der Begriff *Generation* ein gewisses evokatives Potenzial: Er hebt sowohl den provisorischen als auch den evolutiven, sich fortwährend entwickelnden Charakter des Datenschutzes hervor. Datenschutzregelungen und ihre Paradigmen sind nicht in Stein gemeißelt, sondern stellen einen (oft unvollkommenen) Versuch dar, zeitgemäße Vorschriften zu kodifizieren, um den Risiken und den problematischen Aspekten der Datenverarbeitung zu einem gegebenen Zeitpunkt Rechnung zu tragen. Im Laufe der Zeit können neue Herausforderungen entstehen, sodass die vorher adäquaten Regelungen immer wieder neu angepasst werden müssen. An einem gewissen Punkt in diesem Ablauf werden tiefgreifendere Modifikationen der früheren Ordnung unerlässlich, was einen umfassenden Modellwechsel erfordert. Zweitens hat eine generationelle Interpretation des Datenschutzes auch den Vorteil, dass sie uns daran erinnert, wie die Angemessenheit des datenschutzrechtlichen Rahmens in der Vergangenheit bereits infrage gestellt wurde. Dies hemmt die Neigung, die derzeitige Situation als außergewöhnlich zu betrachten. Die Herausforderungen unseres digitalen Zeitalters mögen präzedenzlos sein, aber das trifft nicht minder auf jedes andere Zeitalter zu, das von abrupten technologischen Innovationen geprägt wurde. Eine generationelle Interpretation der Entwicklung des Datenschutzes könnte dann der Tendenz entgegenwirken, die Neuheit und Komplexität der jetzigen Herausforderungen als Anlass für zögerliche oder überhastete Anpassungen des Datenschutzes auf veränderte Rahmenbedingungen in unserer digitalen Umwelt zu nehmen.

Obwohl Herausforderungen für die rechtliche Steuerung von Datenverarbeitung in vielen Sektoren entstanden sind, wirft der Bereich der biomedizinischen Forschung

spezifische Fragen auf. In diesem Kontext war das Verwenden von Daten traditionell mit der Idee verbunden, dass sie für einen spezifischen und klar definierten Zweck, wie z. B. das Testen einer bestimmten Hypothese, gesammelt und verarbeitet werden. Hintergrund ist hier, dass forschungsrechtliche und -ethische Normen immer schon die Darstellung von Forschungszwecken verlangt haben, um Probanden hinreichend über das jeweilige Projekt aufzuklären und so eine gehaltvolle Einwilligung zu ermöglichen. Deshalb ist biomedizinische Forschung mit dem sogenannten „Zweckbindungsprinzip“[2] des Datenschutzrechts immer gut kombinierbar gewesen. Nach diesem Prinzip müssen Daten für einen spezifischen und vordefinierten Zweck, welcher wiederum den betroffenen Personen klar offengelegt und erklärt werden muss, gesammelt und verarbeitet werden.

Biomedizinische Forschung ist jedoch neuerdings immer weniger mit solchen Annahmen vereinbar. Auf der einen Seite ist die Anzahl der Big-Data- und KI-basierten Forschungsaktivitäten (Zhu und Zheng 2018) gestiegen, in denen das Definieren des spezifischen Zwecks der Datensammlung und -verarbeitung schwierig ist. Auf der anderen Seite stützen sich immer mehr Studien auf die Weiterverwendung von Daten, die zunächst nicht für Forschungszwecke gesammelt wurden (z. B. in der Gesundheitsversorgung oder für statistische Zwecke). Unter diesen Umständen gestaltet sich das alte Paradigma des Einholens der informierten Einwilligung von jeder Person, deren Daten verarbeitet werden, sehr aufwendig. Darüber hinaus hat die alte Annahme, dass Anonymisierung grundsätzlich eine valide Alternative zur Einwilligung sein kann,[3] wenn diese nicht einfach einzuholen ist, an Glaubwürdigkeit verloren (Ohm 2009). Schließlich hat zunehmende Datafizierung in bestimmten Bereichen die partizipative Dimension der Forschung verstärkt und eine Reflexion auf Ziele der Wissenschaft motiviert.[4] In diesem Zuge sind die Erwartungen bezüglich der Kontrolle über die in der Forschung verwendeten personenbezogenen Daten gestiegen. Gleichzeitig ist mit dem gestärkten Grad an Partizipation zumindest potenziell der Anspruch verbunden, Daten spenden zu können (Hummel et al. 2019).

Nun könnte man argumentieren, dass bereits eine neue Generation des Datenschutzes eingeläutet wurde, die fähig ist mit den oben genannten Herausforderungen umzugehen.[5] Im Jahr 2016 erließ die Europäische Union die DSGVO, welche das erste supranationale Rechtsinstrument mit direkter Anwendbarkeit in verschiedenen Staaten verkörperte und dadurch endlich die transnationale Natur der Datenverarbeitung widerspiegelte. Darüber hinaus gab die DSGVO den Datenschutzbehörden breitere Überwachungsbefugnisse und führte empfindliche Geldstrafen als Instrument ein, um Compliance zu gewährleisten

[2]Siehe z. B. Brouwer (2011). Das Zweckbindungsprinzip hat eine lange Tradition im Datenschutz und wurde in der DSGVO nochmals unterstrichen (Art. 5 Abs. 1. lit. b).

[3]Diese Annahme ist als „consent or anonymise approach“ bekannt (Mostert et al. 2016).

[4]Als Beispiel seien die sogenannten „citizen science“ Initiativen in ihren verschiedenen Formen (Shirk et al. 2012) angeführt, die aber auch weiterer Reflexion und Gestaltung bedürfen (Guerrini et al. 2018).

[5]Diese These wird z. B. von Kiss und Szőke (2015) vertreten.

(Albrecht 2016). Nach einer anfänglichen Befangenheit aufgrund der ersten Entwürfe der Verordnung (Dove et al. 2014) wurde die rechtskräftige Fassung gelobt, weil sie vorteilhafte Normen für die Forschung enthielt, wie die Freistellung „from storage limitation periods and the duty to notify data subjects about processing" oder die Möglichkeit einer generellen Einwilligung *(broad consent)* für die Datenverarbeitung in der Forschung (Dove et al. 2016).

Kann man dann sagen, dass die DSGVO den definitiven Übergang zu einer neuen Generation des Datenschutzes markiert? Dies ist eine schwierige Frage, vor allem da nach dem Inkrafttreten der Verordnung (25. Mai 2018) einige Jahre abgewartet werden sollten, bevor man voreilige Schlüsse zieht. Aber einige vorläufige Beobachtungen lassen sich bereits formulieren. Auf der einen Seite könnte man argumentieren, dass bereits die bloße Aufmerksamkeit, welche die DSGVO auf die Erarbeitung von angemessenen und sicheren Datenverarbeitungsverfahren gelenkt hat, schon ein epochaler Erfolg ist. Auf der anderen Seite bleiben Unklarheiten. In Bezug auf Datenverarbeitung für die Forschung klärt die DSGVO z. B. nicht (vollständig), inwiefern und ggf. mit welcher Ausgestaltung alternative Formen der Einwilligung (wie eine Generaleinwilligung bzw. ein *broad consent*) legitim sind, oder ob in manchen Fällen der „Forschungszweck" als Legitimationsgrundlage der Daten(weiter)verarbeitung vom Erfordernis einer Einwilligung der betroffenen Person[6] befreit (Mondschein und Monda 2019). Darüber hinaus könnten die Stärkung des Rechts auf Löschung (auch bekannt als „Recht auf Vergessenwerden", Art. 17 DSGVO) und die Anreize, Daten zu anonymisieren (als Voraussetzung für die Exemtion vom Anwendungsbereich der DSGVO) und zu pseudonymisieren (als vorgeschlagene Schutzmaßnahme, z. B. in der Verarbeitung von Daten für Forschungszwecke) mit dem Reproduzierbarkeitsbedarf der Wissenschaft (verhindert durch die Datenlöschung), ihrem Exaktheitsbedarf (potenziell gefährdet durch Datenverknüpfungsfehler, die durch Pseudonymisierung begünstigt werden können) und der Rückgabe klinisch relevanter Ergebnisse (durch die Datenanonymisierung kompromittiert) kollidieren.[7]

Aus diesen Gründen wurde die DSGVO zurecht als „a bit of an unusual hybrid of old and new" (Mayer-Schonberger und Padova 2015, S. 324) beschrieben. Diese Beobachtungen zur DSGVO – und ebenso die anderen Datenschutzgesetze, die seither beschlossen wurden[8]

[6]Damit ist die sogenannte *research exemption* (siehe auch Abschn. 4.1) angesprochen. Es wird in der Rechtswissenschaft kontrovers diskutiert, inwiefern Mitgliedstaaten „may limit a data subjects right to control the use of their data in research by removing the consent requirement" (Staunton et al. 2019, S. 1161). Art. 9 Abs. 2 lit. j und Art. 89 könnten dies ermöglichen, v.a. wenn es sich um Datenweiterverwendung (bzw. Sekundärnutzung) handelt, z. B. bei genetischen Daten aus einer Biobank. Siehe auch Abschn. 4.2.

[7]Solche Sorgen werden z. B. von Negrouk und Lacombe (2018) formuliert.

[8]Die DSGVO, obwohl in der ganzen EU direkt anwendbar, enthält viele Öffnungsklauseln, die den Mitgliedstaaten erlauben, weiter zu regulieren. Das haben u.a. Deutschland (Datenschutz-Anpassungs- und Umsetzungsgesetz EU vom 30. Juni 2017) und Dänemark (Act No. 502 vom 23. Mai 2018) bereits gemacht.

– sind aber nicht der einzige Grund, warum es offen erscheint, ob bereits eine neue Generation des Datenschutzes entstanden ist. Während Mayer-Schönbergers Framing verschiedener Datenschutzgenerationen hauptsächlich die Gesetzgebung fokussiert, ist zu berücksichtigen, dass Datenschutz bzw. Generationen desselben nicht ausschließlich auf Rechtstexte reduziert werden können. Eine weitere entscheidende Variable ist „Tradition", welche sich aus gerichtlichen Präzedenzfällen und etablierten Handelsbräuchen außerhalb der juristischen Sphäre im engen Sinn entwickelt hat, z. B. in der Industrie. Wie in der Rechtswissenschaft betont wurde (Sacco 1991), wird das Recht (im weiteren Sinne) nicht nur durch Gesetze und Gerichtsurteile geschaffen: Es ist ein komplexes Ergebnis aus unterschiedlichen Rechtsformanten, darunter feststehende Handelsbräuche, Interpretationen der Beamten, Verwaltung und Rechtslehre. Außerdem werden gesellschaftsfähige Normen auch durch *de facto* akzeptierte Praktiken beeinflusst, welche als „mute law" bezeichnet werden (Sacco 1995, 2015). Während ein Gesetz in einer verhältnismäßig kurzen Zeit verändert werden kann, ist das Modifizieren der anderen Rechtsformanten, welche die juristische Ordnung mitbestimmen, langwieriger. Sie können dann dafür sorgen, dass Konzepte, welche sich in der Lehre, der Rechtsprechung und der Interpretation etabliert haben und womöglich breite gesellschaftliche Akzeptanz genießen, abrupte Gesetzesänderungen überdauern und die Umsetzung neuer Regeln dauerhaft prägen. Im Datenschutz haben sich beispielsweise Begriffe wie das Zweckbindungsprinzip in der *Tradition* des Datenschutzes so ‚fossilisiert', dass selbst mögliche Alternativen als vermeintliche Variationen von (oder Exemtionen zu) diesem Prinzip verstanden werden. Ähnliches gilt für den Begriff der *Privacy*, dessen Wurzeln zunächst tief in einer Konzeption verhaftet erscheinen, welche die betroffene Person als unabhängig und atomistisch versteht. Ein solches Bild legt nahe, dass Privatsphäre nur von Attacken auf ‚bestimmbare' Daten und auf das Individuum bezogene Daten geschützt werden muss. Konzepte wie „group privacy" (Floridi 2017) mögen dann auf den ersten Blick lediglich als bloße akademische Spekulationen erscheinen.

Es bleibt somit zunächst offen, wie die DSGVO in der Reihe von Mayer-Schönbergers Unterscheidung verschiedener Generationen des Datenschutzes zu betrachten ist. Im Folgenden entwickeln wir einen Vorschlag, wie der Begriff einer neuen Generation des Datenschutzes weiter konkretisiert werden könnte und welche Fragen zu klären sind, um den Übergang zu einer neuen Generation zu markieren.

3 Konzeptionelle Knotenpunkte einer neuen Generation des Datenschutzes

Um zu beleuchten, worin der Übergang zu einer neuen Generation des Datenschutzes bestehen könnte, stellt sich zunächst die Frage, worin genau die datenschutzrechtlichen Herausforderungen heutiger Formen von Datenverarbeitung bestehen. Wir argumentieren, dass diese Frage im Zusammenhang mit mindestens drei konzeptionellen

Grundsatzfragen des Datenschutzes betrachtet werden muss: Was ist der *Gegenstandsbereich* des Datenschutzes, d. h. für die Regelungen welcher Vorgänge ist er zuständig (Abschn. 3.1)? Was ist der relevante *Schutzgegenstand*, d. h. was wird geschützt (Abschn. 3.2)? Und welches *Paradigma* leitet seine Formulierung, Präzisierung und Anwendung (Abschn. 3.3)?[9] Um Datenschutz für diese Herausforderungen zu rüsten und mit Mayer-Schönberger von einer neuen Generation sprechen zu können, erscheinen daher Anpassungen entlang dieser konzeptionellen Knotenpunkte nötig.

3.1 Ein erweiterter Gegenstandsbereich?

Angesichts neuer Realitäten der Datenverarbeitung, der Verknüpfung von Daten aus verschiedenen Lebensbereichen sowie der Allgegenwärtigkeit datengetriebener Entscheidungsfindung erscheint es denkbar, dass der *Gegenstandsbereich* des Datenschutzes, d. h. Aufgabe und Zuständigkeit, überdacht werden muss. Im Folgenden bezeichnen wir als die *Unvollständigkeitsthese* den Standpunkt, dass der *Gegenstandsbereich* des Datenschutzes aktuell zu eng gefasst ist und einer Erweiterung bedarf, um den Schutz von Datensubjekten zu gewährleisten.

Eine prominente, aktuelle Verteidigung der Unvollständigkeitsthese findet sich bei Wachter und Mittelstadt. Datenschutz, so Wachter und Mittelstadt (2019, S. 498), soll die Privatheit, Identität, Reputation und Autonomie der Individuen schützen, kann diesen Zweck angesichts neuer Risiken durch inferenzielle Datenanalyse jedoch nicht erfüllen. Um diese These eingehender darzustellen und zu fundieren, unterscheiden Wachter und Mittelstadt zwischen Daten und *inferences,* die auf Basis dieser Daten gezogen werden. *Inferences* sind definiert als „information relating to an identified or identifiable natural person created through deduction or reasoning rather than mere observation or collection from the data subject“ (Wachter und Mittelstadt 2019, S. 515). Die DSGVO schützt zwar Personendaten, also „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person“ (Art. 4 Nr. 1 DSGVO) beziehen. Ferner schützt sie die „Verarbeitung besonderer Kategorien personenbezogener Daten“ (Art. 9 DSGVO), z. B. Gesundheitsdaten. Wachter und Mittelstadt weisen jedoch darauf hin, dass Individuen nur wenig Kontrolle darüber zugesprochen bekommen, wie ihre Personendaten zur Ableitung von *inferences* verwendet werden (Wachter und Mittelstadt 2019, S. 499). Sie unterscheiden in ihrer Diskussion zwischen *Inputs* in Datenverarbeitung und *Outputs* aus Datenverarbeitung, z. B. die Ableitung von Daten, Profiling, und datengetriebene Entscheidungsfindung. Wachter und Mittelstadt weisen darauf hin,

[9]Die Begrifflichkeiten *Gegenstandsbereich*, *Schutzgegenstand* und *Paradigma* werden im Zusammenhang mit datenschutzrechtlichen Regelungen nicht immer einheitlich verwendet (vgl. z. B. Veil 2019; Bock 2019). Wir verstehen sie jeweils im Sinne der soeben angeführten Paraphrasierungen.

dass gegenwärtiges Datenschutzrecht primär an den *Inputs* in Datenverarbeitung ansetzt. Die wenigen Mechanismen im europäischen Datenschutz, die sich auf *Outputs* beziehen, sind wesentlich schwächer (Wachter und Mittelstadt 2019, S. 514). Während die DSGVO prinzipiell so verstanden werden könnte (Wachter und Mittelstadt 2019, Kapitel 5), dass sie wenigstens zu gewissem Grad auch *inferences* reguliert (z. B. Artikel 13–17, 21–22),[10] bleibt deren rechtlicher Status insgesamt unscharf und lückenhaft. Als Beispiel diskutieren Wachter und Mittelstadt (2019, S. 570–572) das Recht auf Anfechtung automatisierter Entscheidungen (Artikel 22). So suggeriert der EuGH, dass Resultate von Verarbeitungsprozessen nur insofern datenschutzrechtlich problematisierbar sind, als falsche und/oder unvollständige Daten eingegeben wurden (oder die Verarbeitung aus anderen Gründen unrechtmäßig ist). Davon abgesehen enthält das Datenschutzrecht alleine jedoch keine Richtgrößen zur Beurteilung einer Anfechtung datengetriebener Entscheidungsfindung. Anfechtung bleibt so ein „mere procedural right" und bloße „empty shell" (Wachter und Mittelstadt 2019, S. 571). Überhaupt setzt die Anwendung der DSGVO auf *inferences* voraus, diese als Personendaten oder sensitive Daten zu klassifizieren. Selbst dann, so resümieren Wachter und Mittelstadt, würden *inferences* lediglich als „economy class" Personendaten behandelt, die weniger geschützt sind als durch Datensubjekte bereitgestellte Personendaten oder sensitive Daten (Wachter und Mittelstadt 2019, S. 611).

Ein damit verbundenes Problem (auf das wir in Abschn. 3.2 ebenfalls eingehen) ist, dass die Unterscheidung zwischen Personendaten und nicht-Personendaten, oder zwischen sensitiven und nicht-sensitiven Daten, in Big-Data-Kontexten nicht tragfähig erscheint: Nicht-personenbezogene oder -sensitive Daten können personenbezogen oder sensitiv werden, sobald sie zur Ableitung personenbezogener oder sensitiver Attribute verwendet werden – ohne dass sich der Inhalt der Daten verändert (Wachter und Mittelstadt 2019, S. 564). Ebenso können vermeintlich neutrale Daten zu Daten werden, welche Verletzungen der Privatsphäre von Datensubjekten und/oder Schädigungen sowie Diskriminierung Tür und Tor öffnen (Wachter und Mittelstadt 2019, S. 615–616). Auf solche Kategorien fußende Regelungsmechanismen sind daher veraltet und ineffektiv, da sie nachgelagerte Verwendung und damit verbundene Änderungen in der Kategorisierung von Daten nicht ausreichend berücksichtigen (Wachter 2019, S. 7). Schließlich illustrieren Wachter und Mittelstadt anhand einer Reihe von Fallbeispielen, dass die europäische Rechtsprechung, insbesondere der Europäische Gerichtshof, dazu tendiert, Daten beim *Input* in Datenverarbeitung wesentlich größeren Stellenwert als den *Outputs* von Datenverarbeitung beizumessen.

Um den herausgearbeiteten Unzulänglichkeiten im Datenschutz beizukommen, fordern Wachter und Mittelstadt ein neues Datenschutzrecht, das Lücken in der

[10]Die angesprochenen Artikel definieren Informationspflichten (Art. 13-14), Auskunftsrechte (Art. 15), Rechte auf Berichtigung (Art. 16), Löschung (Art. 17), Widerspruch (Art. 21) sowie Rechte im Zusammenhang mit automatisierten Entscheidungen (Art. 22).

Zurechenbarkeit, Haftung und Verantwortung von datengetriebenen Vorgängen schließt: ein *right to reasonable inferences*. Dieses Recht soll *inferences* mit besonders hohem Risiko regulieren, d. h. solche *inferences*, die in die Privatsphäre eindringen, Reputationsrisiken bergen, oder schwer verifizierbar sind. Für solche *inferences* würde das *right to reasonable inferences* von Datenverarbeitern *ex ante* folgende Erklärungen verlangen, um eine Einschätzung der *reasonableness* zu ermöglichen: „(1) why certain data are a normatively acceptable basis to draw inferences; (2) why these inferences are normatively acceptable and relevant for the chosen processing purpose or type of automated decision; and (3) whether the data and methods used to draw the inferences are accurate and statistically reliable" (Wachter und Mittelstadt 2019, S. 581). In Fällen, in denen *inferences unreasonable* erscheinen, sollen Individuen zu deren Anfechtung befähigt werden.

Diese Forderungen sind unter die *Unvollständigkeitsthese* zu fassen, da sie gegenwärtiges Datenschutzrecht als zu eng gefasst kritisieren und neue Regelungen fordern. Wie im etablierten Datenschutzrecht scheint Bedingung (1) zu regeln, welche Daten verarbeitet werden können, löst sich dabei jedoch von den fehlgehenden Klassifizierungsversuchen, die Grundlage momentaner Regulierung sind. Demgegenüber knüpfen der Fokus auf *inferences* sowie die geforderten Mechanismen zur Anfechtung primär an der Verwendung der Daten sowie deren Auswirkungen und nur sekundär an der Herkunft der Daten an (Wachter und Mittelstadt 2019, S. 616). Bedingungen (2) und (3) sind schließlich dazu intendiert, den Gegenstands- und Aufgabenbereich des Datenschutzrechts auf *inferences* und deren Adäquatheit zu erweitern.

Als Herausforderungen für Wachter und Mittelstadt können folgende Punkte angesprochen werden. Auf der einen Seite kritisieren sie gegenwärtige Kategorisierungen im Datenschutzrecht, z. B. Personendaten versus Nicht-Personendaten, oder sensitive versus nicht-sensitive Daten. Auf der anderen Seite führen sie selbst eine ganze Reihe von Unterscheidungen in die Diskussion ein, z. B. Hochrisiko versus nicht-Hochrisiko, *reasonable* versus *unreasonable*, verifizierbare Daten versus unverifizierbare Vorhersagen und akzeptable versus inakzeptable Grundlagen für *inferences*. Man könnte befürchten, dass einige dieser Klassifizierungen ganz ähnliche Probleme aufwerfen. So könnte sich beispielsweise die Risikobewertung eines *inference* in verschiedenen Kontexten von niedrig zu hoch verändern. Ebenso könnten manche Daten in einem Kontext akzeptable Grundlage für *inferences*, in anderen Kontexten jedoch inakzeptabel sein. Ein Beispiel: Die Ableitung der Postleitzahl des Wohnsitzes einer Person mag zunächst als ein vergleichsweise harmloser *inference* erscheinen. In Big-Data-Kontexten kann sich dies jedoch schnell ändern. Paradigmatisch sei auf die Forschung von Latanya Sweeney (Sweeney 2000; Sweeney et al. 2017; Yoo et al. 2018) verwiesen, die mehrfach gezeigt hat, wie bereits wenige solcher Datenpunkte zusammengenommen eine Person eindeutig identifizieren und Verknüpfungen mit anderen Datensätzen erlauben, z. B. mit öffentlich einsehbaren, prima facie anonymisierten Forschungs- und Gesundheitsdaten.

Der initial harmlose *inference* der Postleitzahl erhält in einem solchen Szenario ein hohes Risikopotenzial.

Selbstverständlich muss bei diesen Bedenken berücksichtigt werden, dass Wachter und Mittelstadt selbst explizit machen, dass die genauen Bedeutungen dieser Unterscheidungen kontextsensitiv erörtert werden und sozial akzeptable Standards insbesondere im Hinblick auf *reasonableness* ausbuchstabiert werden müssen (Wachter 2019, S. 7). Ein wesentlicher Teil ihrer Position weist somit über unvollständiges Datenschutzrecht hinaus und hebt die Bedeutung von Aushandlungsprozessen zwischen Datensubjekten, -verarbeitern und Gesellschaft hervor. Zentrale Grundbegrifflichkeiten werden in konkreten Anwendungsszenarien und –kontexten situativ spezifiziert, in denen Daten verarbeitet, *inferences* gezogen und Entscheidungsprozesse dadurch beeinflusst werden. Eine solche Offenheit und Kontextsensitivität wirft dabei mindestens zwei Fragen auf: Erstens wäre zu diskutieren, ob uns Prozesse der Ausbuchstabierung und diskursiven Erörterung des Umfangs von Datenschutz sowie der Bewertungsmaßstäbe nicht schon im *Status quo*, d. h. im aktuellen und vermeintlich unvollständigen Datenschutzrecht genauso offen stehen wie im Modell von Wachter und Mittelstadt. Zweitens stellt sich die Frage, ob die Bedeutsamkeit der sozial-diskursiven Ausbuchstabierung von Grundbegrifflichkeiten und Bewertungsmaßstäben nicht suggeriert, dass wir bei der Berücksichtigung und dem Schutz der Grundrechte und Interessen von Datensubjekten über wesentlich *mehr* nachdenken müssten als über Datenschutz. Diese Anfrage fördert eine Ambiguität in der Unvollständigkeitsthese zutage: Sie kann verstanden werden als die Behauptung, dass aktuelles Datenschutzrecht inadäquat ist und der Verbesserung bedarf. Aber sie kann ebenso als Hinweis darauf gelesen werden, dass Datenschutz nur ein Teil des Unterfangens sein kann. Datenschutz muss ergänzt werden, und zwar nicht nur durch andere gesetzliche Regelungen außerhalb des genuinen Datenschutzrechts, sondern durch gesellschaftliche Diskurse, die Maßstäbe – wie z. B. *reasonableness* – kontinuierlich erörtern sowie neu verhandeln. Insofern Wachter und Mittelstadt eine Erweiterung des Gegenstands- und Aufgabenbereichs des Datenschutzrechts fordern, scheinen sie die erste Lesart der Unvollständigkeitsthese zu vertreten. In diesem Fall kann debattiert werden, inwieweit sich ihre neu eingeführten datenschutzrechtlichen Kategorien besser schlagen als die bisherigen. Insofern sie nun die Signifikanz sozialer Aushandlungsprozesse betonen, scheinen sie vor allem die zweite Lesart der Unvollständigkeitsthese zu unterstreichen. Beide Lesarten sind miteinander konsistent und es ist keineswegs abwegig beide zu verfolgen. Dies und das konzeptionelle Verhältnis beider Lesarten explizit zu machen wäre jedoch hilfreich um nachvollziehen zu können, in welchem Sinne Datensubjekte zur Formulierung und Durchsetzung neuartiger Ansprüche berechtigt sind bzw. sein sollten und inwieweit es gerade das Datenschutzrecht ist, das als systematischer Ort zur Einführung und Garantie solcher Ansprüche fungieren sollte.

Der diskutierte Vorschlag der Verankerung eines *right to reasonable inferences* im Datenschutzrecht illustriert ganz unabhängig davon, ob man ihn letztlich verteidigt oder zurückweist, wie ein erweiterter Gegenstandsbereich ein entscheidender Schritt beim Übergang zu einer neuen Generation des Datenschutzes sein könnte.

3.2 Ein veränderter Schutzgegenstand?

Wie gerade erwähnt basiert Datenschutz traditionellerweise auf Abgrenzungen zwischen unterschiedlichen Kategorien von Daten. Die wichtigste davon ist die Unterscheidung zwischen personenbezogenen und nicht-personenbezogenen Daten (auch bekannt als Sachdaten). Es wird oft angenommen, nur personenbezogene Daten seien der relevante Schutzgegenstand des Datenschutzes, weil nur personenbezogene Daten Informationen enthalten, welche die individuelle Privatsphäre und die Selbstbestimmung der Personen betreffen. Informatiker/-innen und Rechtswissenschafter/innen sind lange davon ausgegangen, dass der Personenbezug von Daten durch Anonymisierung entfernt werden kann (Ohm 2009) und diese somit nicht mehr geschützt werden müssen, da Bezug und Auswirkungen auf identifizierbare Personen ausgeschlossen werden können. Dazu kommt die Tatsache, dass eine Unterscheidung zwischen personenbezogenen und nicht-personenbezogenen Daten eine intuitive und semantische Anziehungskraft hat, vor allem in der heute geläufigsten Wissenschaftssprache, nämlich Englisch. Tatsächlich heißt „personal“[11] sowohl ‚privat/intim' – wie in „she resigned from this job for personal reasons“ – als auch ‚eigen/individuell' – wie in „I've decided to hire a personal fitness trainer“[12]. Dadurch mag auch die Semantik des Wortes „personal“ implizit die Annahme stützen, dass es einen selbstverständlichen Unterschied gibt zwischen den Daten, die ‚privat/intim' oder ‚eigen/individuell' sind und denen, die es nicht sind.

Dennoch werfen heutige Technologien der Datenverarbeitung die Frage auf, ob es zweckmäßig ist, dass nur personenbezogene Daten als Objekt des Datenschutzrechts verbleiben. Diesbezüglich stellen sich zwei unterschiedliche Fragen, die erste eher empirisch, die zweite eher normativ: (1) Ist es überhaupt noch *möglich,* personenbezogene von nicht-personenbezogenen Daten zu unterscheiden? (2) Wäre es *wünschenswert* zwischen personenbezogenen und nicht-personenbezogenen Daten zu unterscheiden und nur Erstere zum Schutzgegenstand des Datenschutzrechts zu zählen?

In Bezug auf die erste Frage ist festzustellen, dass es empirisch mehr und mehr zweifelhaft ist, ob man noch personenbezogene von nicht-personenbezogen Daten unterscheiden kann. Personenbezogene Daten werden traditionellerweise definiert als

[11] „Personal data“ ist der englische Terminus für „personenbezogene Daten“.

[12] Beispiele und Bedeutungen aus dem *Macmillan dictionary online*: https://www.macmillandictionary.com/dictionary/british/personal_1 (letzter Zugang am 15. Mai 2020).

Informationen, die sich auf eine bestimmte oder bestimmbare Person beziehen.[13] Dementsprechend gibt es zwei unterschiedliche Hauptkriterien, die Informationen erfüllen müssten, damit sie als personenbezogene Daten erachtet werden können: erstens, dass sie sich auf eine Person beziehen; zweitens, dass diese Person bestimmbar ist. Obwohl diese zwei Kriterien *prima facie* streng und spezifisch erscheinen, gibt es Hinweise, dass eine zunehmende Menge von Informationen beide Kriterien erfüllen kann, sodass Datenschutzrecht geradezu das „law of everything" werden könnte (Purtova 2018). Die jüngste europäische Rechtsprechung hat zum Teil die Idee unterstützt, dass ein Personenbezug besteht, „wenn die Information aufgrund ihres *Inhalts*, ihres *Zwecks* oder ihrer *Auswirkungen* mit einer bestimmten Person verknüpft ist."[14] Purtova suggeriert im Hinblick auf die Auswirkung dieses wichtigen Urteils provokanterweise, dass prinzipiell auch Wetterinformationen diese Kriterien erfüllen können und dann als personenbezogene Daten gelten müssten.[15] Abgesehen von diesem hyperbolischen Beispiel besteht sicherlich ein konkretes Risiko einer Über-Erweiterung des Begriffes „personenbezogene Daten", sodass jede Unterscheidung zu nicht-personenbezogenen Daten faktisch unmöglich wird. Manche argumentieren (Dalla Corte 2019), dass eine Abhilfe zu dieser möglichen Über-Erweiterung in der bereits existierenden Rechtsprechung und Rechtslehre gefunden werden könne und neue Gesetzgebung deshalb nicht notwendig sei. In jedem Fall bleibt die Tatsache, dass eine neue Generation des Datenschutzes definieren muss, wie umfangreich sein Schutzgegenstand sein soll (oder sogar sein kann).

Aber selbst wenn eine Unterscheidung zwischen personenbezogenen und nicht-personenbezogenen Daten tragfähig und die Klasse von Personendaten enger zu fassen wäre als von Purtova befürchtet, gibt es in Bezug auf die zweite Frage Argumente, die eine Erweiterung des Datenschutzrechts auf *mehr* als nur personenbezogene Daten im klassischen Sinn nahelegen: Personen und ihre jeweilige Privatsphäre müssen auch von der Verarbeitung von Daten geschützt werden, die nicht-personenbezogen oder anonymisiert sind oder die sich auf andere Personen (und nicht die von der Verarbeitung betroffene Person) beziehen. Der Grund dafür ist, dass Erkenntnisse, welche durch

[13]Siehe z. B. sowohl Art. 2 lit. a der alten Datenschutzrichtlinie (Richtlinie 95/46/EG) als auch Art. 4 Nr. 1 DSGVO.

[14]EuGH, Rechtssache C-434/16, Peter Nowak v. Data Protection Commissioner, ECLI:EU:C:2017:994, Urteil vom 20. Dezember 2017. Hervorhebung der Autoren.

[15]So beschreibt die Autorin ein Smart City Projekt in den Niederlanden, in dem ein Stadtviertel mit zahlreichen Sensoren ausgestattet wurde, um so viele Daten wie möglich zu sammeln und auf dieser Basis deviantes Verhalten der Besucher des Viertels besser verstehen und eventuell korrigieren zu können. In diesem Kontext argumentiert Purtova, dass die von einigen dieser Sensoren gesammelten Wetterinformationen die Kriterien erfüllen könnten, sich auf eine bestimmbare Person zu beziehen: „this information is collected in a database that is likely to be used for a *purpose* to assess and influence their [i.e. the visitors of the area] (deviant) behaviour, and hence it is information *relating to* people in purpose" (Purtova 2018, S. 58).

nicht-personenbezogene Daten oder durch Daten gewonnen werden, die sich auf andere Personen beziehen, eine oft noch größere Gefahr für den Einzelnen darstellen können als die Bearbeitung seiner bzw. ihrer eigenen (d. h. auf sich selbst bezogenen) Daten (Loi 2019). Ein Beispiel hierfür wäre eine hypothetische Marktforschung (basierend auf Daten von *n* anderen Personen), die zeigen würde, dass Kunden, die gewisse Dinge während einer gewissen Zeitspanne kaufen, bereit wären einen höheren Preis zu zahlen. Nach einer solchen hypothetischen Entdeckung wäre *jede andere* Person, die potenziell in dieser Zeitspanne einkauft, von der initialen Datenverarbeitung betroffen – und nicht nur die Personen, auf welche sich die in der Marktforschung verwendeten Daten beziehen. Das heißt, Personen könnten also von der Verarbeitung von Daten, die weder ‚privat/intim' noch ‚eigen/individuell' sind, beeinträchtigt werden.[16] Aus diesem Grund sollte u.U. der „nominalist approach" (Floridi 2017) des derzeitigen Datenschutzrechts überdacht werden, der grundsätzlich individuelle Rechte zuspricht und Personen nur Schutz bietet, wenn ihre eigenen Daten bearbeitet werden.

3.3 Ein Paradigmenwechsel?

Neben dem Gegenstandsbereich und dem Schutzgegenstand wird eine zukünftige Datenschutzgeneration möglicherweise auch zentrale Paradigmen überdenken müssen. Traditionell orientiert sich Datenschutz (zumindest in Europa) an Privatheit, Grundrechten und informationeller Selbstbestimmung. So ist beispielsweise ein in der DSGVO formuliertes Ziel, „die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten" (Art. 1 DSGVO) zu schützen. In diesem Zusammenhang stellt sich zunächst die Frage, durch welche *Art von Rechten* diese Ziele und Zwecke verfolgt werden. Eine kontrovers diskutierte Idee ist es, Datenschutz mit Kategorien des Eigentums zu verknüpfen. Zurück geht diese Idee auf US-amerikanische Diskurse, wobei sie sich in jüngerer Zeit auch in Europa verbreitet hat (Purtova 2012). Befürworter der Propertisierung personenbezogener Daten formulieren eine ganze Reihe verschiedener Forderungen (Hummel et al. 2020). Unter anderem kritisieren sie, dass derzeitige Datenschutzrechte keine vollständige Kontrolle über Daten gewährleisten. Individuen können Daten beispielsweise nicht veräußern. Demgegenüber könnten Eigentumsrechte an Daten die Übertragung und Herausgabe von Daten sowie die Abwehr Dritter (Purtova 2017, S. 6–8; Thouvenin 2017, S. 25–27) ermöglichen und durchsetzen. Daten als Eigentum zu behandeln, so die Befürworter, würde die Anwendung traditioneller und bewährter Regelungen des Eigentumsrechts erlauben und könnte Datenaustausch für diejenigen erleichtern, die dies wünschen, ohne Datenschutz für diejenigen aufzuweichen, die ihre Daten nicht teilen möchten.

[16]Eine ähnliche Position wird auch von Poullet (2018, S. 776, Fn. 9) vertreten.

Der Vorschlag eines Dateneigentums hat besonders im medizinischen Bereich Begeisterung ausgelöst (Kish und Topol 2015). Auch wenn dies reizvoll erscheint, sind einige Fragen im Hinblick auf den Übergang zu einem Eigentums-Paradigma für personenbezogene Daten aufgeworfen worden, z. B. wie Eigentumsregeln auf Daten als neuen Gegenstandsbereich angepasst werden könnten (Thouvenin et al. 2017) oder ob ein Eigentum an personenbezogenen Daten den Schutz der Privatsphäre *de facto* stärken oder schwächen würde. So mag die Möglichkeit Daten veräußern zu können zunächst wie ein Zugewinn über Schutz und Gestaltung der Privatsphäre erscheinen; sind Daten jedoch einmal veräußert, ist nicht mehr klar, inwieweit der/die Ex-Eigentümer/-in noch Ansprüche an und um ihre Verarbeitung formulieren und durchsetzen kann.

Dateneigentum kann als revisionistischer[17] Vorschlag in Bezug auf die Frage verstanden werden, durch welche Art von Recht Datenschutz praktisch werden sollte. Eine weitere Grundsatzfrage betrifft die Spezifizierung der *Zielsetzungen*, die durch Datenschutz verfolgt werden. In Debatten über durch Datafizierung tangierte Grundrechte und Interessen treten vermehrt Begriffe von *Souveränität* in Erscheinung. Historisch gesehen bezeichnet Souveränität den Anspruch auf absolute Macht in Bezug auf einen Gegenstandsbereich, z. B. die Macht eines souveränen Nationalstaates über sein Territorium. Datensouveränität (Hummel et al. 2018), digitale Souveränität (Pinto 2018) oder Cyber-Souveränität (Baezner und Robin 2018) übertragen dieses Konzept mit ganz verschiedenen Schwerpunkten und Konnotationen (Couture und Toupin 2019; Hummel et al. 2021a) auf den digitalen Raum. Beispielsweise wird Datensouveränität dann möglich, wenn die jeweilige Akteure in der Lage sind , Macht- und Kontrollansprüche rund um ihre Daten und deren Verarbeitung zu artikulieren und durchzusetzen. Derartige Ansprüche können von Einzelpersonen, Organisationen oder Staaten ausgehen. Dabei hält nicht jeder Kontrollanspruch einer genauen Überprüfung stand. Ansprüche können kritisiert werden, in Spannung zu anderen stehen und erfordern daher eine diskursive Aushandlung und Bewertung ihrer Autorität und Legitimität.

Der Deutsche Ethikrat (2017) versteht Datensouveränität als die Fähigkeit des Einzelnen zu informationeller Freiheitsgestaltung. Er weist die Bedeutung von Paradigmen wie Privatheit, Grundrechte und Selbstbestimmung nicht von der Hand. Aber im Unterschied zu primär negativen Rechten zum Ausschluss anderer von der eigenen, intimen informationellen Sphäre beinhaltet informationelle Freiheitsgestaltung den Anspruch selbst zu bestimmen und zu gestalten, wie man mit anderen in informationelle Beziehungen tritt. Die Idee informationeller Freiheitsgestaltung schließt daher positive Ansprüche auf die Befähigung zur Ausübung gehaltvoller Kontrolle über die eigenen Daten ein.

[17]Vgl. demgegenüber Victor (2014), der argumentiert, dass Dateneigentum keine Zukunftsmusik mehr ist, sondern die DSGVO bereits den Beginn eines Übergangs zu einem eigentumsähnlichen Paradigma markiert.

Eine spannende Frage, die hier nicht abschließend geklärt werden kann, betrifft das Verhältnis zwischen dem datenschutzrechtlichen Rahmen der DSGVO und dem Leitkonzept der *Datensouveränität,* z. B. ob Letzteres eine Erweiterung oder Verschärfung des Ersteren erfordern würde. Auf der einen Seite könnte man Datensouveränität als Entfaltung der in Art. 1 DSGVO angesprochenen Grundrechte und Grundfreiheiten verstehen. Auf der anderen Seite enthält die DSGVO Erlaubnistatbestände (beispielsweise Art. 9 Abs. 2lit. j DSGVO), durch die zumindest in bestimmten Datenverarbeitungskontexten individuelle Kontrollansprüche nicht an erster Stelle stehen.

4 Spezifische Herausforderungen im Hinblick auf biomedizinische Forschung

Während sich die oben genannten Grundsatzfragen auf Datenschutz im Allgemeinen beziehen, wenden wir uns jetzt zwei spezifischen Herausforderungen zu, welche die Bearbeitung von Daten in der biomedizinischen Forschung betreffen. Zunächst werden wir uns mit der Frage beschäftigen, ob es sinnvoll ist, *Ausnahmenormen* für die Forschung zu definieren. Danach diskutieren wir die *informierte Einwilligung* als Voraussetzung der Datenverarbeitung in biomedizinischer Forschung.

4.1 Ausnahmenormen für die Forschung?

Derzeit ist die Datenverarbeitung für biomedizinische Forschungszwecke durch spezielle datenschutzrechtliche Bedingungen reguliert. Die DSGVO sieht z. B. die Verarbeitung von Daten für Forschungszwecke als einen legitimen Grund vor, der die Verarbeitung sensibler Daten – wie Gesundheitsdaten oder genetische Daten – ermöglicht.[18] Darüber hinaus enthält die DSGVO weitere spezielle Regeln für die Weiterverwendung von Daten für Forschungszwecke[19] und kreiert dadurch eine sogenannte „research exemption", d. h. Derogationen von den normalen Regeln für die Datenverarbeitung, wenn diese für Forschungszwecken erfolgt (Shabani und Borry 2018; Staunton et al. 2019).

Spezielle Regeln für die Bearbeitung von Daten für Forschungszwecke können theoretisch von Vorteil sein. Auf den ersten Blick kann eine „research exemption" ein Subset von Normen schaffen, das spezifisch für die Forschung modelliert ist und so eine vereinfachte Datenverarbeitung ermöglichen. Bei näherer Betrachtung entstehen jedoch Fragen, ob es sinnvoll ist, einen solchen Ausnahmestatus in der Gesetzgebung vorzusehen.

[18] Art. 9 Abs. 2 lit. j DSGVO.

[19] Siehe Art. 5 Abs. 1 lit. b, Art. 5 Abs. 1 lit. e, Art. 9 Abs. 2 lit. j, Art. 14 Abs. 5 lit. b, Art. 17 Abs. 3 lit.d, Art 21 Abs. 6, Art. 89.

Als erste Schwierigkeit ist der Anwendungsbereich dieser Ausnahmenormen für die Forschung nicht immer scharf abzugrenzen. Wenn er als sehr umfassend interpretiert wird, sodass z. B. auch Marktforschung abgedeckt wird,[20] könnten Ausnahmenormen gerade für kommerzielle Ziele ausgenutzt werden und – anstatt für Forschung vorbehalten zu bleiben – auch für Verarbeitungsprozesse gelten, bei denen primär individuelle und private Interessen des Datenverarbeiters im Vordergrund stehen. Doch auch bei demgegenüber rigoroser Interpretation des Geltungsbereichs (d. h. nur für *biomedizinische* oder mindestens *gesundheitsbezogene* Forschung) bleiben Herausforderungen.

Zunächst suggeriert bereits die Wahl der Worte und Konzepte einen ganz bestimmten Fokus. Wenn im Zusammenhang mit Datenschutzregeln und sektorspezifischen Normen für die Forschung von „research exemption" (Shabani und Borry 2018), „research exception" (Dove 2018) oder wie wörtlich in der DSGVO[21] von „derogations" (englische Fassung) und „Ausnahmen" (deutsche Fassung) die Rede ist, so suggeriert dies, dass die Voraussetzungen für Datenverarbeitung für (biomedizinische) Forschungszwecke im Vergleich zu anderen Verarbeitungszwecken und -bereichen als eher gelockert interpretiert werden können. Aus dieser Perspektive scheinen einerseits bestimmte *prima facie* bindende Anforderungen an Datenverarbeitung zu bestehen, die schließlich bei bestimmten Zwecken und Arten von Verarbeitungsprozessen suspendiert werden. Ruyter et al. (2010) kritisieren, dass dieses Verständnis bereits in der Konzeptualisierung der Ausgangslage eine Tendenz einführt: „[t]he language of 'exemption' denotes deviance from a common obligation (in this case the data protection principles) from which one needs to be excused. It follows that exemptions should be exceptional, and deviations are most commonly considered to be undesirable and regrettable" (Ruyter et al. 2010, S. 288). Stattdessen fordern sie, für bestimmte Verarbeitungszwecke von einer alternativen, „equally acceptable route to achieve protection" (Ruyter et al. 2010, S. 310) zu sprechen, die z. B. Einwilligung in Verarbeitung nicht notwendig erfordert.

Konzeptionelle Fragen wie diese können praktische Konsequenzen nach sich ziehen. Auch wenn dem *Buchstaben des Gesetzes* und der *Rhetorik* nach Erleichterungen formuliert sind, bleibt die Möglichkeit, dass *operative Normen*[22] für die Datenbearbeitung in der biomedizinischen Forschung resultieren, die *trotz* oder womöglich *wegen* diesem Sonderstatus zum Teil rigorosere Anforderungen mit sich bringen. Weichert (2020,

[20]Eine Stellungnahme der Article 29 Working Party (2013) scheint in diese Richtung zu gehen (Article 29 Data Protection Working Party 2013, S. 46; vgl. jedoch ibid., Fn. 113).

[21]Art. 89 Abs. 2.

[22]Forschung in der Rechtswissenschaft hat betont, dass es einen wesentlichen Unterschied gibt "between operational rules and the formulas which jurists have deemed to describe those operational rules" (Sacco 1991, S. 378). Manchmal wird dieser Unterschied als Gegensatz zwischen „law in the books" und „law in action" beschrieben. Unsere These hier ist, dass das „law in action" des Datenschutzes in der biomedizinischen Forschung *de facto* strenger sein kann, als das „law in the books" mit seinen Ausnahmenormen für die Forschung suggerieren würde.

S. 22) nennt z. B. eine Liste von mehr als zehn detaillierten Maßnahmen,[23] denen ein Forschungsprojekt folgen müsste, um von den privilegierten Datenschutznormen zu profitieren.[24] Ausnahmenormen für die Forschung – obwohl sie oft darauf gemünzt sind, dass die Verarbeitung von Daten für Forschungszwecke vereinfacht wird – können das gegenteilige Ziel erreichen, gerade dann, wenn sie zusätzliche Datenschutzmaßnahmen voraussetzen. Bei der Bewertung bereichsspezifischer Regulierung sind daher ihre konkreten Effekte zu berücksichtigen. Ist es durch sie einfacher, die jeweiligen datenschutzrechtlichen Anforderungen zu erfüllen? Wird der Zeitrahmen von der Planung von Verarbeitungsvorgängen bis zu deren Durchführung durch die bereichsspezifischen Regelungen verkürzt oder verlängert? Ist der bürokratische Aufwand verringert oder erhöht? Die Adressierung dieser empirischen Fragen liegt jenseits des Gegenstandsbereichs des vorliegenden Beitrags. Von Bedeutung für unsere Zwecke ist lediglich der Hinweis, dass bereichsspezifische Lockerungen Vereinfachung auf der operativen Ebene nicht garantieren.

In der Tat ist es offensichtlich, dass die Datenschutzbestimmungen einer biomedizinischen Studie von einer hohen Anzahl von verschieden Kontrollorganen – u. a. Ethikkommissionen,[25] Förderinstitutionen und Datenschutzbeauftragten – überprüft werden, denen „normale“ Datenverarbeiter gar nicht oder nicht im selben Maße unterstehen. Eine Möglichkeit zur Verringerung der letztgenannten Asymmetrie könnte selbstverständlich in dem Ansatz bestehen, auch große datenverarbeitende Unternehmen – welche eine *rigorosere* oder *restriktivere* Interpretation der Ausnahmenormen von deren Geltungsbereich ausschließen würde – durch spezifische „Data Science“ Ethikkommissionen und weitere Instrumente zu begleiten und ggf. zu regulieren (Schneble et al. 2020).

Für eine Vertiefung, wie sich der Buchstabe des Gesetzes und seine praktische Umsetzung im Datenschutz unterscheiden, siehe Koops (2014).

[23]In diesem Text befürwortet der Autor eine restriktive Interpretation der von ihm definierten „datenschutzrechtlichen Forschungspriviligierung“, welche nur für „unabhängige Forschung“ gelten müsste: „Dies [die datenschutzrechtliche Forschungspriviligierung] gilt nur für unabhängige Forschung […] Wissenschaftliche Untersuchungen, die zu Organisations-, Aufsichts- und Kontrollzwecken vorgenommen werden, sind also ebenso wenig privilegiert wie Werbeforschung. Das Gleiche gilt für auf die Entwicklung neuer Produkte ausgerichtete Forschung (z. B. der Pharmaindustrie) und rein oder vorrangig kommerzielle Absatz- oder Markt- und Meinungsforschung“ (Weichert 2020, S. 19–20).

[24]Vgl. auch Rossnagel (2019, S. 161).

[25]In der Schweiz wurde 2020 ein Review durchgeführt, dessen Ziel es u.a. war festzustellen, welche Probleme am häufigsten in den Anträgen auf Genehmigung durch eine Ethikkommission vorliegen (Bergstraesser et al. 2020). Ein Resultat war, dass die große Mehrheit der Vorbehalteder Ethikkommissionen Datenschutzaspekte betreffen.

Zweitens schaffen solche Ausnahmenormen eine zusätzliche Ebene von Regeln, die mit allgemeineren Datenschutzbedingungen kombiniert und koordiniert werden muss. Dies kann vor allem für Forscher/-innen ohne vertiefte juristische Kenntnisse herausfordernd sein, insbesondere solange sich die Rechtspraxis noch im Wandel befindet. Nur größere Studien haben normalerweise genügend finanzielle Ressourcen, um passende Rechtsberatung hinzuzuziehen, damit sie die Ausnahmenormen anwenden, sie auf die allgemeineren Datenschutzrichtlinien abstimmen und ein verlässlich regelkonformes Projekt verwirklichen können. Anwaltskanzleien wiederum profitieren von der Komplexität des Datenschutzrechts und erlangen in diesem Kontext Marktmacht und Deutungshoheit (Purtova 2014). Koops resümiert gar: „data protection lawyers can be suspected of having an interest in complexity as it provides them with work“ (Koops 2014, S. 254).

Drittens ist die genaue Grenze zwischen Datenverarbeitung für die Forschung und für nicht-forschungsbezogene Zwecke in Big-Data-Kontexten immer schwieriger aufrechtzuerhalten. Dadurch wird zunehmend zweifelhafter, inwieweit die derzeit existierenden Ausnahmenormen für die Forschung auf Grenzfälle und innovative Projekte zutreffen. Ein aktuelles Beispiel sind die Contact-Tracing Apps, die entwickelt werden, um die COVID-19-Pandemie zu bekämpfen (Gasser et al. 2020). Diese zielen sicherlich primär auf die öffentliche Gesundheit ab. Es ist aber ebenfalls absehbar, dass die dadurch erhobenen Daten auch für Forschungszwecke verwendet werden (McLennan et al. 2020). Diesbezüglich können Ausnahmenormen für die (biomedizinische) Forschung zwar Chancen bieten, aber auch für Rechtsunsicherheit sorgen, ob (und ab wann) innovative Studien solchen Ausnahmenormen oder den allgemeineren und nicht bereichsspezifischen Datenschutzbestimmungen entsprechen müssen.

Operationales Resultat von *exemptions*, *exceptions* und *derogations* könnte also insgesamt sein, dass ein erhebliches Maß an Aufmerksamkeit auf deren Anwendungsbedingungen gelegt wird, gleichzeitig Unklarheiten im Hinblick auf verschiedene Ebenen des Datenschutzrechts aufgeworfen werden und schließlich gerade innovative Projekte an der Schnittstelle zwischen Forschung und anderen Sektoren von solchen Unsicherheiten betroffen sind. Gleichzeitig scheinen andere Formen und Legitimationsgrundlagen von Datenverarbeitung jenseits dieser Erlaubnistatbestände, z. B. Datenverarbeitung in Online-Kontexten auf Basis von „blinde[m] Akzeptieren“ (Plaut und Bartlett 2012) von obskuren *Terms & Conditions*, auf keinem vergleichbaren Prüfstand zu stehen.[26]

[26]Siehe z. B. Monteleone (2015) für eine Kritik der „privacy policies“ von Webseiten, die ein Gefühl von Datenschutz kreieren, dies jedoch mittels „written, detailed and usually long and highly complex texts; […] they consist of separate texts hardly accessible or displayed in a slightly visible part of a website. Internet users are asked to consent to the conditions described in the privacy policies by ticking a "yes" box at the end of the statements; more often, this box is simply

4.2 Informierte Einwilligung?

Aus ethischer Sicht ist die Notwendigkeit der Einholung informierter Einwilligung als Grundlage zur Einbindung in biomedizinische Forschung durch eine Bandbreite von Erwägungen motiviert. So sollen Einwilligungsmechanismen beispielsweise potenzielle Probanden vor Übergriffen schützen, Autonomie ermöglichen und Vertrauen in Forschungsprozesse aufrechterhalten (Eyal 2019). In Anlehnung an eines der oben dargestellten Paradigmen kann informierte Einwilligung auch als Ausübung persönlicher Souveränität gesehen werden: „consent and personal sovereignty go hand in hand: A zone of personal inviolability and control is manifested in respect for the ability to give and withhold consent" (Miller 2010, S. 380–381).

Während diese ethischen Erwägungen klar für informierte Einwilligung als essentielle Voraussetzung für biomedizinische Forschung sprechen, gibt es Debatten darüber, ob sie kategorisch und für jede Art von Forschungsprojekt finden sollten. Populationsbezogene Beobachtungsstudien, die durch Auswertung von Befunden, Statistiken und Krankenakten beträchtlichen Nutzen für eine Gesellschaft generieren (vgl. der Beitrag von Jungkunz et al. im vorliegenden Band), beeinträchtigen die Privatsphäre von Individuen und deren Kontrollansprüche rund um ihre Daten wenn überhaupt nur minimal (vgl. Porsdam Mann et al. 2016; Cohen 2018). Pragmatische und auch methodische Gründe können dem Einholen informierter Einwilligung in solchen Szenarien im Wege stehen. Miller (2010) argumentiert, dass in solchen Fällen Klarheit über den genauen Gegenstandsbereich persönlicher Souveränität verlangt ist. Er verteidigt die Position, dass informierte Einwilligung bei nicht-interventioneller Forschung, die z. B. ausschließlich auf der Analyse von Patientendaten basiert, unter bestimmten Bedingungen verzichtbar sein kann. Wenn solche Forschungsaktivitäten das Gemeinwohl befördern, ohne individuelle Rechte unverhältnismäßig zu beeinträchtigen, ist ein Verzicht auf Einwilligung insbesondere dann denkbar, wenn folgende Punkte zutreffen: „(1) the proposed research is socially valuable; (2) there are severe practical impediments to soliciting consent or requiring consent would be likely to compromise the scientific validity, and consequently the value, of research; and (3) adequate safeguards for access by researchers are implemented to minimize the intrusion on privacy" (Miller 2010, S. 400).

Big-Data-basierte biomedizinische Forschung wirft bestimmte Herausforderungen für das Konzept informierter Einwilligung auf. So wird beispielsweise ähnlich wie im Kontext des Biobankings (Richter und Buyx 2016) darauf hingewiesen, dass Daten-

positioned beside a link (hyperlink), which refers to another page (hypertext) containing the privacy policy: clicking the box presumes you have read the policies" (Monteleone 2015, S. 80). Es bleibt abzuwarten und empirisch zu untersuchen, ob die DSGVO die Herangehensweise von Datenverarbeitern in dieser Hinsicht verändern wird.

subjekte nicht immer hinreichend über Zwecke und Konsequenzen der Forschungsaktivitäten aufgeklärt werden können, da diese nicht notwendigerweise absehbar sind (Mittelstadt und Floridi 2016, S. 311–316; Deutscher Ethikrat 2017, S. 136–138). Die gerade skizzierten Ziele von Mechanismen informierter Einwilligung sind daher in Big-Data-Forschung schwer zu erreichen, die gerade auf der De- und Rekontextualisierung, der Zusammenführung von Daten verschiedener Arten und Quellen, der Suche nach unvorhersehbaren Korrelationen, dem Ziehen von Rückschlüssen auf Individuen wie auch Populationen und der Nutzung von Anwendungen maschinellen Lernens basiert.

Angesichts dieser Herausforderungen scheinen mindestens zwei Ansätze möglich. Erstens können wir Millers Standpunkt zu bestimmten Formen nicht-interventioneller Forschung folgen und argumentieren, dass informierte Einwilligung in manchen Szenarien datenintensiver biomedizinischer Forschung nicht nötig ist. So können wir annehmen, dass Bedingung (2) – informierte Einwilligung im klassischen Sinne erscheint wenig praktikabel – zuweilen erfüllt sein wird, beispielsweise aufgrund der soeben erwähnten Offenheit von konkreten Verarbeitungszwecken und Konsequenzen. Die Euphorie (Chen und Asch 2017) um datengetriebene Medizin, personalisierte Versorgung und klinische KI suggeriert ferner, dass Bedingung (1) – beträchtlicher gesellschaftlicher Nutzen – zumindest prinzipiell erfüllbar ist. Zwar kippt diese Euphorie zuweilen in Hype (Maughan 2017) und es ist keineswegs sicher, dass sich die Hoffnungen auch erfüllen. Aber angenommen dies gelingt und wir stellen ferner sicher, dass auch Bedingung (3) – Implementierung von Sicherungsmechanismen zur Minimierung von Verletzungen der Privatsphäre – erfüllt ist, hätten wir möglicherweise eine solide Grundlage, um Einwilligungserfordernisse in diesen Fällen zu lockern.[27]

Eine zweite Strategie wäre es, das Bekenntnis zur informierten Einwilligung als essentielle Voraussetzung von jeder Form von biomedizinischer Forschung hochzuhalten, jedoch über neue Formen solcher Einwilligung nachzudenken, die der Realität von Big Data und KI angemessen sind. So sind zwischen klassischer informierter Einwilligung in jeden einzelnen Verarbeitungsvorgang und dem Verzicht auf Einwilligungserfordernisse Mittelwege denkbar. (2) könnte dann zum Anlass genommen werden,

[27]Selbstverständlich gibt es weitere Begründungsmuster, die ähnliche Konklusionen stützen. Dove & Chen (2020) problematisieren beispielsweise aus rechtswissenschaftlicher Perspektive die von ihnen als „consent misconception“ bezeichnete Annahme, dass „research ethics consent“ einen „data processing consent“ impliziert– sowohl im Hinblick auf (i) den Grad der Erforderlichkeit als auch (ii) auf den vom Subjekt intendierten Gegenstandsbereich seiner/ihrer Einwilligung: „failure to make this distinction between research ethics consent and data processing consent explicit will exacerbate a misconception among participants and researchers alike such that the participants' consent to participate in a research project de facto equates to a consent to (also) process their personal data. We term this 'consent misconception', a scenario whereby because consent is the favoured mechanism and key ethico-legal norm in research ethics governance, it is perceived that it must also be the case for data protection purposes“ (Dove und Chen 2020, S. 12).

innovative Strukturen und Mechanismen zum Einholen, Erteilen, Verweigern und Widerruf informierter Einwilligung zu geben (Kaye et al. 2015; Ploug und Holm 2015, 2016; Budin-Ljøsne et al. 2017).

Dies ist nicht der Ort, um diese beiden Ansätze abschließend zu bewerten. Wir möchten lediglich auf eine Schwierigkeit in der Motivation des ersten Ansatzes, d. h. in den angesprochenen Kontexten *keine* informierte Einwilligung zu fordern, hinweisen. Dessen Rechtfertigung basiert im Wesentlichen auf einer Kombination von Impraktikabilität und Unsicherheit. So kann beispielsweise zum Zeitpunkt der möglichen Aufnahme von Individuen in bestimmte Forschungsprojekte offen sein, welche Zwecke durch die Datenverarbeitung genau verfolgt werden. Dadurch erscheint Bedingung (2) erfüllt, d. h. informierte Einwilligung im klassischen Sinne ist wenig praktikabel. Zu beachten ist jedoch, dass genau dieselben Erwägungen (1) und (3) unterlaufen oder zumindest Fragen aufwerfen: Wenn Verarbeitungszwecke und zukünftige Verwendung von Daten bzw. Ergebnissen unklar sind, warum sollte gerade unter solchen Umständen hinreichend hohe Sicherheit bezüglich des gesellschaftlichen Werts und der Effektivität von Sicherungsmechanismen gegen Verletzungen der Privatsphäre bestehen? Fragen wie diese mag man daher zum Anlass nehmen, statt der Beschränkung oder Aufgabe von Einwilligungserfordernissen eher den zweiten Ansatz zu verfolgen und die Anpassung und Weiterentwicklung von Einwilligungsprozessen voranzutreiben, welche die Präferenzen der Subjekte kontinuierlich einholen, abbilden und bei Verarbeitungsanfragen umsetzen und dabei in der neuen Realität datenintensiver biomedizinischer Forschung sowohl anwendbar als auch gehaltvoll sind (Hummel et al. 2021b).

5 Fazit

Ausgangspunkt unserer Untersuchungen war die Beobachtung, dass sich Technologien und Praktiken der Datenverarbeitung beständig weiterentwickeln und dabei Herausforderungen für den Datenschutz aufwerfen. Wir sind der Hypothese nachgegangen, dass Datenschutz aus diesem Grund der Anpassung und Erneuerung bedarf. Insbesondere haben wir Mayer-Schönbergers Deutung der Evolution von Datenschutz als Sequenz aufeinanderfolgender *Generationen* beleuchtet. Seine Deutung hebt die Gestaltbarkeit, Unabgeschlossenheit sowie das Erfordernis fortwährender, zuweilen tiefgreifender Weiterentwicklung des Datenschutzes hervor. Wir haben daraufhin entfaltet, was es aus unserer Sicht konkret heißen würde, im Kontext der eingangs skizzierten Begebenheiten zu einer *neuen Generation* des Datenschutzes überzugehen.

Mit Wachter und Mittelstadt wäre erstens auf den *Gegenstandsbereich* des Datenschutzes zu reflektieren. Dabei sind wir in Bezug auf die Frage neutral geblieben, *ob* Datenschutz um ein *right to reasonable inferences* erweitert werden sollte. Stattdessen ist es eben jene Grundsatzfrage um den *Gegenstandsbereich* – in diesem Fall der Erweiterung auf *inferences* als einer der möglichen *Outputs* von Datenverarbeitung – die einer Klärung bedarf. Als offene Frage haben wir markiert, ob in diesem Zusammenhang

wirklich eine Erweiterung des *Datenschutzes* gedacht werden muss, oder ob die Problemstellungen nicht unterstreichen, dass gerade mehr als *Daten*schutz nötig ist, um Datens*ubjekte* zu schützen.

Zweitens erscheint Personenbezug zur Spezifikation des *Schutzgegenstands* problembehaftet: Zum einen erscheint der Begriff des Personenbezugs potenziell enorm weit, zum anderen können auch Verarbeitungsprozesse von Daten *ohne* Personenbezug im engeren Sinne zu Beeinträchtigungen der Rechte und Freiheitsvollzüge von Individuen führen. Es stellt sich daher neben den Erwägungen zum *Gegenstandsbereich* die Frage, ob auch andere Datensorten als personenbezogene Daten *Schutzgegenstand* des Datenschutzes sein sollten.

Drittens sind leitende *Paradigmen* des Datenschutzrechts wie Privatheit, die Wahrung von Grundrechten und informationelle Selbstbestimmung im Hinblick auf neue Realitäten der Datenverarbeitung und datengetriebener Entscheidungsfindung weiterzudenken und ggf. zu ergänzen. Dies betrifft u. a. die Art von Rechten, über die Ansprüche rund um den Schutz von Daten artikuliert werden, und die in den Augen mancher um Eigentumsrechte erweitert werden sollten. Ebenso sind neue Zielgrößen wie Datensouveränität zu bewerten und mit dem bestehenden Rahmen in Beziehung zu setzen.

Im Anschluss haben wir uns zwei Themenkomplexen zugewandt, die insbesondere bei der datenschutzrechtlichen Betrachtung biomedizinischer Forschung dringlich sind, bevor eine neue *Generation* des Datenschutzrechts erdacht und implementiert werden kann. Erstens wäre zu erörtern, ob die momentane Exzeptionalität von Forschung gegenüber anderen Arten der Datenverarbeitung sinnvoll ist. Zweitens stellt sich die Frage, ob und wie die Bedeutung informierter Einwilligung bei der Durchführung von Forschungsvorhaben neu zu bewerten ist.

Während wir notwendige Grundsatzfragen zur Neuausrichtung identifiziert haben, war unser Ziel nicht, diese zu klären. Manche Herausforderungen bei der Steuerung datenintensiver Anwendungen mögen durch minimalinvasive, gezielte Anpassungsschritte in der Rahmenordnung lösbar sein. Die aufgeworfenen Fragestellungen hingegen betreffen die konzeptionellen Grundpfeiler, auf denen eine solche Ordnung aufgebaut ist, und die angesichts extensiver Formen der Datenverarbeitung ihre Tragfähigkeit neu beweisen bzw. einer angepassten Architektur weichen müssen. Dies unterstreicht aus unserer Sicht die Relevanz von Mayer-Schönbergers Deutung der Evolution von Datenschutzgesetzgebung als Sequenz aufeinanderfolgender Generationen, welche die Schwächen vorhergehender Arrangements durch Neuausrichtung und Erweiterung zu überwinden versuchen. Angesichts gänzlich neuartiger, datenbasierter Entscheidungsmechanismen und gesellschaftlicher Koordinationsprozesse scheint die Zeit für einen Generationenwechsel gekommen, der durch die DSGVO möglicherweise angestoßen, kaum jedoch vollendet wurde.

Der nächste Schritt besteht darin auszuhandeln, durch wen und in welcher Form solche Prozesse vorangetrieben und ausgestaltet werden sollen. Wir vertreten in dieser Hinsicht den Standpunkt, dass eine neue Generation des Datenschutzes nicht nur mittels neuer Gesetzgebung durch nationale oder supranationale Entitäten

erfolgt. Die DSGVO ist nach wie vor zu neu und hat zu viel gesetzgeberischen Aufwand erfordert, als dass eine erneute Novelle des Datenschutzes oder gar eine radikal neue Gesetzgebung – gerade auf europäischer Ebene – mittelfristig realistisch ist. Ferner kann Gesetzgebung zwar Veränderungen initiieren, stellt jedoch nur einen Teil des Regelungsapparats dar. Andere sind Rechtsprechung, Rechtslehre, Interpretationen der Beamten sowie der öffentlichen und privaten Akteure, welche den bzw. einen spezifischen Rechtsbereich prägen (z. B. Datenschutzbeauftragte und große datenverarbeitende Unternehmen für den Datenschutzbereich). Veränderungen bzw. eine Evolution im Sinne eines Übergangs zu einer anderen Generation dieser Bandbreite an Komponenten beansprucht eine wesentlich längere Zeit, als für die Änderung eines Gesetzes gebraucht wird. Stefano Rodotà betont dies mit spezifischem Bezug zur Rechtsprechung, wenn er im Hinblick auf eine neue Konzeption (oder gar *Generation*) des Eigentums im Nachgang der Französischen Revolution erklärt, dass Gesetzesänderungen (bzw. das Inkrafttreten des Code Civil) alleine für den Übergang zu einer neuen Konzeption des Eigentums noch nicht ausreichen:

> „Beginnen wir damit, dass sich in der Arbeit der Gerichte das Alte und das Neue ständig miteinander vermischen. Mindestens 20 Jahre lang beurteilten die Gerichte weiterhin Klagen, die vor dem Inkrafttreten des Code Civil entstanden. Wir müssen uns daher nicht nur mit der traditionell konservativen Denkweise der Juristen und mit der Tatsache befassen, dass die Richter ihr intellektuelles Gepäck nicht plötzlich aufgeben konnten: Ebenso muss man berücksichtigen, dass die Phase nach der Kodifizierung [der neuen Eigentumsordnung durch den Code Civil] eine Übergangsphase ist, die gerade durch die Verwendung von Normen und juristischen Kategorien gekennzeichnet ist, die sich in ihrer Inspiration stark unterscheiden." (Rodotà 2013, S. 122–123, unsere Übersetzung)[28]

Übergänge von einer Generation zur anderen sind nicht abrupt, sondern entfalten sich im Rahmen eines kontinuierlichen Prozesses. In der Tat wird die bereichsspezifische Governance neben Gerichten, Staaten und Regierungen durch eine Reihe von weiteren Akteuren beeinflusst (Börzel und Risse 2010). So wird beispielsweise darauf hingewiesen, dass die praktische Anwendung, Ausgestaltung und Interpretation von Datenschutzmechanismen maßgeblich von großen Anwaltskanzleien mitgeprägt werden wird, welche strategische Beratungsleistungen, internationale Vernetzung und Diskurs sowie die Dokumentation von *best practices* katalysieren (Purtova 2014). Eine durch und durch neuartige Generation des Datenschutzes kann daher nur unter Einbindung der ganzen

[28]"Cominciamo col dire che, nell'opera delle corti, vecchio e nuovo si mescolano continuamente. Per almeno vent'anni, i tribunali continuano a giudicare di cause anteriori all'entrata in vigore del Code civil. Non solo, dunque, bisogna fare i conti con la tradizionale mentalità conservatrice dei giuristi e con il fatto che certo i giudici non potevano di colpo abbandonare il loro bagaglio intellettuale: si deve anche tener presente che la fase successiva alla codificazione è, da questo punto di vista, un periodo di transizione, caratterizzata appunto dal ricorso a norme ed a categorie giuridiche profondamente divergenti nell'ispirazione."

Bandbreite an Akteuren gelingen, die an der Entwicklung, Verfeinerung, Anwendung und operationalen Ausgestaltung des Datenschutzrahmens beteiligt sind – ein Diskurs, so glauben wir, in dem die in diesem Beitrag umrissenen konzeptionellen Knotenpunkte der Reflexion bedürfen.

Danksagung Die Autoren möchten Georg Starke, Matthias Braun, Serena Bischoff, Martin Jungkunz, Wulf Loh, David Samhammer und Maike Tischendorf für ihre kritischen Hinweise und ihr hilfreiches Feedback herzlich danken. AM ist dem Schweizerischen Nationalfonds zur Förderung der wissenschaftlichen Forschung (SNF), der seinen PhD im Rahmen eines Projektes des Nationalen Forschungs-Programmes 74 „Smarter Health Care" (SNF NRP-74 Smarter Health Care, grant number 407440_167356) finanziert hat, sehr dankbar. PH ist Mitarbeiter im Projekt vALID, das vom Deutschen Bundesministerium für Bildung und Forschung (01GP1903A) gefördert wird. Ferner erhält er Förderung durch die *Emerging Talents Initiative* der Friedrich-Alexander-Universität Erlangen-Nürnberg.

Literatur

Albrecht JP (2016) How the GDPR will change the world. Eur Data Prot Law Rev 2:287

Article 29 Data Protection Working Party (2013) Opinion 03/2013 On Purpose Limitation. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

Baezner M, Robin P (2018) Cyber sovereignty and data sovereignty. Center for Security Studies, ETH Zürich, Zürich. https://doi.org/10.3929/ethz-b-000314613

Bergstraesser E, Nadal D, Özgü H, Kleist P (2020) Deficiencies in paediatric research applications delaying ethics committee approval. Swiss Med Weekly. https://doi.org/10.4414/smw.2020.20267

Bock K (2019) Schutzgut des Datenschutzrechts – Eine Replik auf Veil, Schutzgutmisere – Teil I. CR-online.de Blog. https://www.cr-online.de/blog/2019/03/22/schutzgut-des-datenschutzrechts-eine-replik-auf-veil-schutzgutmisere-teil-i/

Börzel TA, Risse T (2010) Governance without a state: can it work? Regul Gov 4(2):113–134

Brouwer E (2011) Legality and data protection law: the forgotten purpose of purpose limitation. In: Besselink LF, Pennings F, Prechal S (Hrsg) The eclipse of the legality principle in the European Union. Kluwer Law International, Alphen aan den Rijn, S 273–294

Budin-Ljøsne I, Teare HJA, Kaye J, Beck S, Bentzen HB, Caenazzo L et al (2017) Dynamic Consent: a potential solution to some of the challenges of modern biomedical research. BMC Med Ethics 18(1):4

Chen JH, Asch SM (2017) Machine learning and prediction in medicine — beyond the peak of inflated expectations. N Engl J Med 376(26):2507–2509. https://doi.org/10.1056/NEJMp1702071

Cohen IG (2018) Is there a duty to share healthcare data? In: Cohen IG, Lynch HF, Vayena E, Gasser U (Hrsg) Big data, health law, and bioethics. Cambridge University Press, Cambridge, S 209–222

Couture S, Toupin S (2019) What does the notion of "sovereignty" mean when referring to the digital? New Media Soc 21(10):2305–2322. https://doi.org/10.1177/1461444819865984

Dalla Corte L (2019) Scoping personal data: towards a nuanced interpretation of the material scope of EU data protecton law. Eur J Law Technol 10(1):1-26

Deutscher Ethikrat (2017) Big Data und Gesundheit. Datensouveränität als informationelle Freiheitsgestaltung. Deutscher Ethikrat, Berlin

Dove ES, Chen J (2020) Should consent for data processing be privileged in health research? A Comparative Legal Analysis. Int Data Priv Law 10(2):117–131

Dove ES, Thompson B, Knoppers BM (2016) A step forward for data protection and biomedical research. Lancet 387(10026):1374–1375

Dove ES, Townend D, Knoppers BM (2014) Data protection and consent to biomedical research: a step forward? Lancet 384(9946):855

Eyal N (2019) Informed consent. In Zalta EN (Hrsg) The Stanford Encyclopedia of Philosophy. Metaphysics Research Lab, Stanford University. https://plato.stanford.edu/archives/spr2019/entries/informed-consent/. Zugegriffen: 7. Mai 2020

Floridi L (2017) Group privacy: a defence and an interpretation. In Taylor L, Floridi L, van der Sloot B (Hrsg) Group privacy: new challenges of data technologies. Springer International Publishing, Cham, S 83–100. https://doi.org/10.1007/978-3-319-46608-8_5

Gasser U, Ienca M, Scheibner J, Sleigh J, Vayena E (2020) Digital tools against COVID-19: taxonomy, ethical challenges, and navigation aid. The Lancet Digital Health 2(8):E425-E434. https://doi.org/10.1016/S2589-7500(20)30137-0

Guerrini CJ, Majumder MA, Lewellyn MJ, McGuire AL (2018) Citizen science, public policy. Science 361(6398):134–136

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

Hummel P, Braun M, Dabrock P (2019) Data donations as exercises of sovereignty. In: Krutzinna J, Floridi L (Hrsg) The ethics of medical data donation. Springer, Cham, S 23–54

Hummel P, Braun M, Dabrock P (2020) Own data? Ethical reflections on data ownership. Philos Technol. https://doi.org/10.1007/s13347-020-00404-9

Hummel P, Braun M, Tretter M, Dabrock P (2021a) Data sovereignty. A review. Big Data & Society. http://dx.doi.org/10.1177/2053951720982012

Hummel P, Braun M, Augsberg S, von Ulmenstein U, Dabrock P (2021b) Datensouveränität. Governance-Ansätze für den Gesundheitsbereich. Springer VS, Wiesbaden

Kaye J, Whitley EA, Lund D, Morrison M, Teare H, Melham K (2015) Dynamic consent: a patient interface for twenty-first century research networks. Eur J Hum Genetics EJHG 23(2):141–146

Kish LJ, Topol EJ (2015) Unpatients—why patients should own their medical data. Nat Biotechnol 33(9):921–924. https://doi.org/10.1038/nbt.3340

Kiss A, Szőke GL (2015) Evolution or revolution? Steps forward to a new generation of data protection regulation. In: Gutwirth S, Leenes R, de Hert P (Hrsg) Reforming European Data Protection Law, vol 20. Springer, Netherlands, Dordrecht, S 311–331

Koops B-J (2014) The trouble with European data protection law. Int Data Priv Law 4(4):250–261. https://doi.org/10.1093/idpl/ipu023

Loi M (2019) The digital phenotype: a philosophical and ethical exploration. Philos Technol 32(1):155–171

Maughan T (2017) The promise and the hype of 'Personalised Medicine'. New Bioethics 23(1):13–20. https://doi.org/10.1080/20502877.2017.1314886

Mayer-Schönberger V (1997) Generational development of data protection in Europe. In: Technology and privacy: the new landscape. MIT Press, Cambridge, S 219–241.

Mayer-Schonberger V, Padova Y (2015) Regime change: enabling big data through Europe's new data protection regulation. Colum Sci Tech L Rev 17:315

Mayer-Schönberger V, Ramge T (2018) Reinventing capitalism in the age of big data, 1. Aufl. Basic Books, New York

McLennan S, Celi LA, Buyx A (2020) COVID-19: putting the general data protection regulation to the test. JMIR Public Health Surveill 6(2):e19279. https://doi.org/10.2196/19279
Miller FG (2010) Consent to clinical research. In Miller FG, Wertheimer A (Hrsg) The ethics of consent. Theory and practice. Oxford University Press, S 375–404
Mittelstadt B, Floridi L (2016) The ethics of big data: current and foreseeable issues in biomedical contexts. Sci Eng Ethics 22(2):303–341
Mondschein, CF, Monda C (2019) The EU's General Data Protection Regulation (GDPR) in a research context. In: Kubben P, Dumontier M, Dekker A (Hrsg) Fundamentals of clinical data science. Springer International Publishing, Cham, S 55–71. https://doi.org/10.1007/978-3-319-99713-1_5
Monteleone S (2015) Addressing the failure of informed consent in online data protection: learning the lessons from behaviour-aware regulation. Syracuse J Int Law Commer 43(1):69–119
Mostert M, Bredenoord AL, Biesaart MCIH, van Delden JJM (2016) Big Data in medical research and EU data protection law: challenges to the consent or anonymise approach. Eur J Hum Genet 24(7):956–960. https://doi.org/10.1038/ejhg.2015.239
Negrouk A, Lacombe D (2018) Does GDPR harm or benefit research participants? An EORTC point of view. Lancet Oncol 19(10):1278–1280. https://doi.org/10.1016/S1470-2045(18)30620-X
Ohm P (2009) Broken promises of privacy: responding to the surprising failure of anonymization. UCLA Law Rev 57:1701
Pinto RÁ (2018) Digital Sovereignty or Digital Colonialism? Sur Int J Hum Rights 15(27):15
Plaut VC, Bartlett RP (2012) Blind consent? A social psychological investigation of non-readership of click-through agreements. Law Hum Behav 36(4):293–311. https://doi.org/10.1037/h0093969
Ploug T, Holm S (2015) Meta consent: a flexible and autonomous way of obtaining informed consent for secondary research. BMJ 350. https://doi.org/10.1136/bmj.h2146
Ploug T, Holm S (2016) Meta consent – a flexible solution to the problem of secondary use of health data. Bioethics 30(9):721–732. https://doi.org/10.1111/bioe.12286
Porsdam Mann S, Savulescu J, Sahakian BJ (2016) Facilitating the ethical use of health data for the benefit of society: electronic health records, consent and the duty of easy rescue. Philos Trans R Soc A Math Phys Eng Sci 374(2083):20160130. https://doi.org/10.1098/rsta.2016.0130
Poullet Y (2005) Pour une troisième generation de règlementation de protection des données. Jusletter 3. Oktober 2005
Poullet Y (2010) About the e-privacy directive: towards a third generation of data protection legislation? In: Gutwirth S, Poullet Y, De Hert P (Hrsg) Data protection in a profiled world. Springer, Dordrecht, S 3–30. https://doi.org/10.1007/978-90-481-8865-9_1
Poullet Y (2018) Is the general data protection regulation the solution? Comput Law Secur Rev 34(4):773–778. https://doi.org/10.1016/j.clsr.2018.05.021
Purtova N (2012) Property rights in personal data: a European perspective. Kluwer Law International, Alphen aan den Rijn
Purtova N (2014) Who decides on the future of data protection? Role of law firms in shaping European data protection regime. Int Rev Law Comput Technol 28(2):204–221
Purtova N (2017) Do property rights in personal data make sense after the Big Data Turn? Individual control and transparency. Tilburg Law School Legal Studies Research Paper Series, 21. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3070228
Purtova N (2018) The law of everything Broad concept of personal data and future of EU data protection law. Law Innov Technol 10(1):40–81
Richter G, Buyx A (2016) Breite Einwilligung (broad consent) zur Biobank-Forschung – die ethische Debatte. Ethik in der Medizin 28(4):311–325. https://doi.org/10.1007/s00481-016-0398-4

Rodotà, S (2013) Il terribile diritto. Studi sulla proprietà privata e sui beni comuni (terza edizione.). Il Mulino, Bologna
Rossnagel A (2019) Datenschutz in der Forschung. Z Datenschutz 9(4):157–164
Ruyter KW, Lõuk K, Jorqui M, Kvalheim V, Cekanauskaite A, Townend D (2010) From Research exemption to research norm: recognising an alternative to consent for large scale Biobank research. Med Law Int 10(4):287–313
Sacco R (1991) Legal formants: a dynamic approach to comparative law (Installment I of II). Am J Comp Law 39(1):1–34
Sacco R (1995) Mute law. Am J Comp L 43:455
Sacco R (2015) Il diritto muto: neuroscienze, conoscenza tacita, valori condivisi. Il mulino
Schneble CO, Elger BS, Shaw DM (2020) Google's Project Nightingale highlights the necessity of data science ethics review. EMBO Mol Med 12(3):e12053
Shabani M, Borry P (2018) Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation. Eur J Hum Genet 26(2):149–156
Shirk JL, Ballard HL, Wilderman CC, Phillips T, Wiggins A, Jordan R et al (2012) Public participation in scientific research: a framework for deliberate design. Ecol Soc 17(2):29
Staunton C, Slokenberga S, Mascalzoni D (2019) The GDPR and the research exemption: considerations on the necessary safeguards for research biobanks. Eur J Hum Genet 27(8):1159–1167. https://doi.org/10.1038/s41431-019-0386-5
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
Sweeney L, Yoo JS, Perovich L, Boronow KE, Brown P, BrodyJG (2017) Re-identification risks in HIPAA safe harbor data: a study of data from one environmental health study. Technol Sci, (2017082801). https://techscience.org/a/2017082801
Thouvenin F (2017) Wem gehören meine Daten? Zu Sinn und Nutzen einer Erweiterung des Eigentumsbegriffs. Schweiz Juristen-Zeitung 113(2017):21–32
Thouvenin F, Weber RH, Früh A (2017) Data ownership: taking stock and mapping the issues. In: Dehmer M, Emmert-Streib F (Hrsg) Frontiers in data science. CRC Press, Boca Raton, S 111–145
Veil W (2019) Die Schutzgutmisere des Datenschutzrechts (Teil I). CR-online.de Blog. https://www.cr-online.de/blog/2019/02/06/die-schutzgutmisere-des-datenschutzrechts-teil-i/
Victor JM (2014) The EU general data protection regulation: toward a property regime for protecting data privacy. Yale Law J 123:513
Wachter S (2019) Data protection in the age of big data. Nat Electron 2(1):6–7. https://doi.org/10.1038/s41928-018-0193-y
Wachter S, Mittelstadt B (2019) A right to reasonable inferences: re-thinking data protection law in the age of big data and AI. Columbia Bus Law Rev 2019(2):494–620
Weichert Thilo (2020) Die Forschungsprivilegierung in der DS-GVO. Z Datenschutz 10(1):18–24
Yoo JS, Thaler A, Sweeney L, Zang J (2018) Risks to patient privacy: a re-identification of patients in maine and Vermont Statewide Hospital data. Technol Sci, (2018100901). https://techscience.org/a/2018100901
Zhu L, Zheng WJ (2018) Informatics, data science, and artificial intelligence. JAMA 320(11):1103–1104. https://doi.org/10.1001/jama.2018.8211