Steffen Augsberg,
Marcus Düwell,
Benjamin Müller
(Hg.)

Daten-zugangsregeln

Zwischen Freigabe und Kontrolle

campus

Datenzugangsregeln

Steffen Augsberg ist Professor für Öffentliches Recht an der Universität Gießen. *Marcus Düwell* lehrt Philosophie an der TU Darmstadt. *Benjamin Müller* ist wissenschaftlicher Mitarbeiter in der ZEVEDI-Projektgruppe »Datenzugangsregeln«.

Steffen Augsberg, Marcus Düwell,
Benjamin Müller (Hg.)

Datenzugangsregeln

Zwischen Freigabe und Kontrolle

Campus Verlag
Frankfurt/New York

ISBN 978-3-593-51966-1 Print
ISBN 978-3-593-45914-1 E-Book (PDF)
DOI 10.12907/978-3-593-45914-1

Umschlaggestaltung: Campus Verlag GmbH, Frankfurt am Main.
Satz: le-tex xerif
Gesetzt aus der Alegreya
Druck und Bindung: Beltz Grafische Betriebe GmbH, Bad Langensalza
Beltz Grafische Betriebe ist ein Unternehmen mit finanziellem Klimabeitrag (ID 15985–2104-1001).
Printed in Germany

www.campus.de

Inhalt

Zugangsverschränkungen: Neue Datenwelt und die alte Welt der Körper

Zugangs(begrenzungs)konsequenzen: Gesundheitsdaten – (nicht) nur für die Gesundheit?

Zugangsverantwortung: Die Zukunft und Notwendigkeit von informationeller Selbstbestimmung

Ausblick: Datenzugangsregulierung

Datenzugangsregeln – zur Einleitung

In der digitalisierten Welt spielen Daten, Informationen und das daraus gewonnene Wissen eine zunehmend entscheidende Rolle. Wirtschaft, Medizin, Forschung, Klimaschutz sind nur möglich auf der Basis einer verlässlichen Datenlage. Im Zuge der Digitalisierung der Lebenswelten werden Daten in ungekanntem Ausmaß produziert, miteinander verknüpft und für verschiedenste Zwecke genutzt. Mit der wachsenden Bedeutung der Daten ergeben sich zahlreiche normative Fragen. Diese reichen von der Frage, welche Daten von wem und zu welchen Zwecken denn überhaupt gesammelt, produziert und verwaltet werden sollen bzw. dürfen über Fragen nach der Zuverlässigkeit der Daten bis zu der Frage, wessen und welche Daten wem zugänglich sein sollen bzw. wer über die Kriterien zur Regelung dieses Zugangs entscheiden soll. Es geht dabei um Zugang zu Informationen, auf deren Basis man gesellschaftliche und persönliche Entscheidungen kompetent treffen kann. Zugang zu Daten zu verweigern, kann insofern zu wesentlichen Beeinträchtigungen und Benachteiligungen führen: Eine Person würde vielleicht eine fundamentale Lebensentscheidung anders treffen, wenn sie zu bestimmten medizinischen Informationen Zugang hätte, die nur aus spezifischen Daten gewonnen werden können. Zugleich kann der ungeregelte Zugang zu Daten zu gravierenden Bedrohungen und Beschädigungen führen, etwa wenn Dritte Zugang zu ihnen erhalten. Der Zugang zu bestimmten Forschungsdaten kann wichtige Forschungsprojekte ermöglichen, zugleich können algorithmisch erhobene Daten ganze Bevölkerungsgruppen signifikanten Risiken im Hinblick auf Diskriminierung und Manipulation aussetzen.

Die Gestaltung von Datenzugangsregeln ist insofern ein wesentlicher Faktor politischer und ökonomischer Macht und zugleich ein wichtiges Instrument zum Schutz wie zur Gefährdung von Individualrechten. Entspre-

chend groß sind die Interessen, die verhandelt werden, und entsprechend zahlreich ist der Kreis derer, die an der Regulierung interessiert sind. Da Datenströme (bzw. die sie tragenden Infrastrukturen) sich nur selten allein im Rahmen nationaler Grenzen bewegen, sind Datenzugangsregeln zudem potentiell Gegenstand konfligierender Regelungsregime und -kompetenzen. Dabei geht es nicht allein um die isolierte Frage, wie man den Zugang zu Daten regelt, denn Daten sind nicht einfach vorhanden – sie werden vielmehr gesammelt, verwaltet und hergestellt. Schon die Gestaltung der technischen Infrastruktur, mit deren Hilfe die Produktion von Daten allererst möglich ist, entscheidet darüber, wie Datenzugang überhaupt geregelt werden kann.

Schon diese wenigen Stichworte deuten die Reichweite des Themas an. Es ist daher auch nicht erstaunlich, dass ein deutlicher normativer Rahmen, ein umfassendes »framework«, innerhalb dessen sich Datenzugangsregulierung bewegt, weder national noch international vorliegt. Allerdings sind Entwicklungstendenzen zu verzeichnen: Traditionelle Datenschutzregelungen entstammen häufig einer Zeit, in der Produktion und Verwaltung von sowie Zugang zu Daten unter ganz anderen Voraussetzungen geschahen. Datenschutzregelungen werden nicht selten als Hemmnis für gewünschte Nutzung von Daten erfahren. In der Forschung wird etwa die Forderung nach mehr Offenheit im Austausch von Daten laut (→ *Gehring*), aber auch im Gesundheitsbereich werden bestehende Regelungen als zu restriktiv erlebt (→ *Niggemeier* und *Böning/Riechert*). Umgekehrt deuten sich Nutzungsmöglichkeiten im Bereich medizinischer Forschung und Technologie an, deren Regelung als dringend erforderlich scheint – man denke etwa an die von der Europäischen Kommission besonders geförderte Entwicklung eines sogenannten »digitalen Zwillings« von Individuen, der eine auf die Person zugeschnittene medizinische Diagnostik möglich machen würde und mit der Produktion enormer, potentiell hochsensibler Datenmengen verbunden wäre (→ *Gruber/Zihlmann* und *Kellmeyer*).

Es scheint daher erforderlich, eine umfassendere Perspektive auf dies Thema zu entwickeln. Das ist die Aufgabe des hier vorgelegten Buches. Dabei geht es auch um rechtliche Fragen der Regulierung im engeren Sinne (→ *Augsberg*), doch diese sind eingebettet in umfassendere Fragen nach der gesellschaftlichen Bedeutung von Daten (→ *Lambach*), den soziologischen Voraussetzungen von Datenzugangsregulierung (→ *Brieske/Schweizer*) und einer philosophischen Perspektive auf die Bedeutung von Datenzugangsregelungen auf Individualrechtsschutz (→ *Düwell*) und Demokratie (→ *Müller*). Eine

solche breite interdisziplinäre Perspektive scheint erforderlich, um die Aufgabe künftiger Datenzugangsregulierung überhaupt in den Blick nehmen zu können. In der weiteren Einleitung wollen wir kurz einige Diskussionslinien andeuten.

Die Bedeutung von Daten

Als in den 1970er und 1980er Jahren, unter anderem im Kontext einer geplanten Volkszählung, Datenschutzregeln entwickelt wurden, die teils noch heute in Kraft sind, war in keiner Weise absehbar, welche Rolle Daten vierzig Jahre später spielen würden. Es war nicht absehbar, in welchem Umfang Datenströme quer über den Globus ausgetauscht würden, es war nicht absehbar, dass auf der Basis sehr individuellen Verhaltens bei der Internetrecherche Nutzerprofile entwickelt werden, die ökonomisch sehr relevant sind. Es war auch nicht absehbar, dass die Zuverlässigkeit der Daten eine derart wesentliche Rolle spielen würde, weil Daten schlicht erfunden werden können, so dass die Frage zentral werden würde, welche Institutionen die Vertrauenswürdigkeit der Daten garantieren könne. Es war nicht absehbar, dass die Manipulation von Daten ein wichtiges Element in internationalen Konflikten und der Kriegsführung werden könnte. Es war nicht absehbar, dass die Medizin sich auf den Weg machen würde, die Gesundheitsdaten von Individuen in einer Weise zu kombinieren, dass detaillierte und integrierte Gesundheitsprofile von Menschen erstellt werden können, die es gestatten, die gesundheitlichen Aspekte des Lebens der Betroffenen umfassend digital zu begleiten und zu steuern.

Diese damals unvorstellbare, heute nahezu selbstverständliche Allgegenwart von Daten in der gesellschaftlichen, ökonomischen und politischen Welt und auch in der individuellen Lebensführung erlaubt es, von einer »Datafizierung der Welt« (→ *Lambach*) zu reden. Wenn diese Diagnose zutrifft, dann ist es für jeden Versuch der Datenzugangsregulierung erforderlich, zunächst diese Eingebundenheit von Daten, ihre Funktion, näher zu verstehen. Wenn man Datenzugang regelt, so stellt dies einen Eingriff in einen komplexen Prozess dar. Ein solcher Prozess hat nicht nur etwas mit der Verbindung von spezifischen Daten zu einer spezifischen physischen Person zu tun, über deren Verhalten oder Eigenschaften Daten erhoben werden. Es geht vielmehr um multipolare Prozesse, deren Implikationen

bisweilen kaum absehbar sind. Bisweilen werden Daten erhoben, von deren Existenz die Personen, auf die sich diese Daten beziehen, nichts wissen bzw. von denen sie im Regelfall nicht einschätzen können, welche Signifikanz diese Daten haben.

Wenn Daten ein derart ubiquitäres Phänomen sind, so stellt sich die Herausforderung nicht nur im Hinblick auf Daten, die aufgrund ihres Bezugs zu konkreten Individuen, regulierungsbedürftig erscheinen, sondern auch im Hinblick auf Daten, die in bedeutenden gesellschaftlichen Prozessen eine zentrale Rolle spielen, man denke insbesondere an Forschungsdaten (→ *Gehring*). Diese wurden bislang im Hinblick auf Rechte der Forschenden, Publikationsrechte oder ökonomische Verwertungsrechte reguliert. Doch jetzt wird weitgehende Offenheit im Umgang mit diesen Daten gefordert. Dabei geht es um effektiven Umgang mit Forschungsmitteln, Beschleunigung ihrer Weiternutzung im Forschungsprozess und Fragen internationaler Gerechtigkeit. Derartige Forderungen sind nun aber nicht allein im Hinblick auf potentielle Rechte von beforschten oder forschenden Personen relevant, sondern auf den Forschungsprozess selbst und das Verhältnis von Wissenschaft und Gesellschaft. Wenn etwa gefordert wird, nicht nur Forschungsergebnisse, sondern auch Daten, die zu diesen Ergebnissen geführt haben, weitgehend offen zugänglich zu machen, so hat dies Einfluss auf den Forschungsprozess selbst und das Selbstverständnis der Forschenden – denken wir etwa an die Frage, ob diese Daten für militärische oder ökonomische Zwecke Weiterverwendung finden können. Unabhängig davon, welche Regelung man befürwortet, zunächst muss man sich bewusst machen, dass diese Regulierung beurteilt werden sollte unter der Frage, wie die Regulierung den Forschungsprozess selbst beeinflusst. Ähnliches könnte man für den Bereich der Gesundheitsdaten sagen. Wenn im großem Stil Gesundheitsdaten erhoben und systematisch verwaltet werden zum Zwecke personalisierter Medizin, so ist dies nicht allein relevant im Hinblick auf unmittelbare Persönlichkeitsrechte von Personen, deren Privatheit und informierte Zustimmung. Vielmehr steht dabei zur Debatte, wie die Medizin der Zukunft aussehen wird, welche Aufgabe und welche Entwicklungsmöglichkeiten sie hat. Nicht zuletzt geht es auch um die komparative Perspektive, weil individualisierte und klassische Medizin zumal in einem Konkurrenzverhältnis stehen.

Wenn die Analyse der »Datafizierung der Welt« zutrifft, so geht es beim Umgang mit Daten nie allein um den Gebrauch der spezifischen Daten, sondern er ist eingebettet in umfangreichere Fragen menschlichen Zu-

sammenlebens und menschlichen Selbstverständnisses. Dann steht auch zur Debatte, wie, u.a., Wirtschaft, Forschung, Medizin und menschliches Zusammenleben im Sinne einer übergreifenden »Datenkultur« umgestaltet werden können. Es bedarf also einer umfassenderen Beschreibung von gesellschaftlichen und politischen Zusammenhängen und der Rolle von Daten, will man Datenzugang regulieren.

Die Regulierung von Datenzugang?

Wir hatten konstatiert, dass die derzeit relevanten Datenschutzregeln zum Teil aus Zeiten stammen, in denen die heutige gesellschaftliche Relevanz von Daten noch keineswegs absehbar war. Man kann also zunächst fragen, ob die Perspektiven, aus denen heraus Datenzugang reguliert wurde, noch der heutigen Situation entspricht. Ohne dies hier historisch im Einzelnen untersuchen zu wollen, kann man eine Reihe von Fragen stellen, die für die Regelungsperspektive erhellend sind. Ohne Anspruch auf Vollständigkeit seien die Folgenden genannt:

Schutzgut. Zunächst kann man fragen, in welcher Hinsicht Daten als regulierungs- und schutzbedürftig angesehen werden. Mit anderen Worten: was ist es an Daten, dass Menschen verletzlich und schutzbedürftig erscheinen lässt, weshalb eine Datenzugangsregulierung erforderlich erscheint? Hier kann man etwa darauf abheben, dass Daten mit der Privatsphäre von Menschen verbunden sind, weshalb sie ein legitimes Interesse haben könnten, dass Aspekte der Privatsphäre nicht publik werden. Damit würden etwa Nutzerdaten unbeachtet bleiben, bei denen Algorithmen Verhaltensdaten von Nutzern verwenden, ohne diese anderen gegenüber offenzulegen. Es kann sein, dass eine solche Nutzung unproblematisch(er) ist, relevant ist jedoch zunächst zu konstatieren, dass technische Möglichkeiten zu Veränderungen der Verletzlichkeiten führen können, wodurch neue Schutzbedürftigen entstehen.

Bedrohung. Damit verbunden stellt sich die Frage, *gegen wen* denn ein Schutz des Datenzugangs überhaupt erfolgen solle. Welche Instanzen stellen eine potentielle Bedrohung dar? In der bereits erwähnten Entscheidung zur Volkszählung war es vor allem der Staat, gegen den Bürger geschützt werden sollten. Die Schutzperspektive war also die klassisch liberale Idee, dass staatliches Handeln an den Rechten der Bürger seine Grenze findet.

Doch das ist ja nicht die einzige Möglichkeit. Man kann fragen, ob nicht ökonomisch motivierte Akteure heute eine stärkere Bedrohung darstellen. Auch muss man nicht annehmen, dass irgendjemand zielgerichtet versucht, Daten zu »missbrauchen«, sondern, wie die bereits angedeutete Diskussion um die Forschungsdaten zeigt, es könnte zunächst auch einfach von Bedeutung sein, welchen Effekt eine bestimmte Form der Datenzugangsregelung auf eine entsprechende Praxis hat (etwa Forschungspraktiken).

Schutzinstanz. Von wem wird erwartet, dass er einen Schutz gegen potentielle Bedrohungen einen Schutzguts gewährleistet? Traditionell wird hier zunächst an den Staat gedacht, und wenn es um Regulierung geht, bleibt dies natürlich auch in gewissem Sinne die zentrale Ausführungsinstanz. Doch gibt es hier zusätzliche Herausforderungen, insofern der Staat nicht in jeder Hinsicht die technische Infrastruktur kontrolliert. Dies gilt sowohl für die Rolle von Betreibern und deren technischem Know-how als auch im Hinblick auf internationale Vernetzungen. Dabei kann man natürlich versuchen, durch entsprechende Vereinbarungen allgemeine Standards international zu implementieren. Doch dafür ist ein internationales Klima vorauszusetzen, dass von Regulierung und Teilen von Daten ausgeht – eine Voraussetzung, die lange Zeit als selbstverständlich angenommen wurde, es aber derzeit keineswegs mehr ist (→ *Gehring/Lambach*).

Die Liste der relevanten Fragen und Antwortoptionen ist hiermit keineswegs ausgeschöpft. Wesentlich ist jedoch: Datenzugangsregeln müssen daraufhin befragt werden, was sie regulieren und schützen wollen, wogegen und durch wen (→ *Brieske/Schweitzer*). Je nachdem, welche Aspekte gestärkt werden, entstehen unterschiedliche Effekte und Transaktionskosten. Abhängig davon, wie man diese Fragen beantwortet, wird man zu sehr unterschiedlichen Datenzugangsregulierungen kommen können.

Normative Perspektiven

Schließlich kann man die Frage stellen, in welchem normativen Bezugsrahmen eine solche Datenzugangsregelung erfolgt. Das berührt nicht mehr nur die Frage nach direkter Gestaltung zugänglichen effektiven Regelungs- und Schutzformen, sondern berührt fundamentalere Fragen, die in Rechtswissenschaft, Rechtsphilosophie, Ethik und politischer Philosophie kontrovers diskutiert werden. So wird etwa beobachtet, dass einige Datenzugangs-

regeln davon ausgehen, dass es in manchen Hinsichten eine generelle Verpflichtung zur Datenspende gäbe bzw. es werde suggeriert, dass eine solche als wünschens- und förderungswürdig anzusehen sei (→ *Brieske/Schweitzer*). Von einer solchen Voraussetzung kann man aber nicht ohne Weiteres ausgehen. Hier sind nicht nur die konkrete Ausgestaltung und die rechtliche Zulässigkeit im gegebenen Datenschutzregime von Interesse, sondern es sind auch grundlegende Solidaritäts- und Freiheitsverständnisse betroffen. Es stellt sich zudem die Frage, ob und inwiefern eine an Individualrechten orientierte Schutzkonzeption nicht zu einer Reihe von Problemen führt – eine Frage die in vielen Beiträgen dieses Buches implizit oder explizit (→ *Düwell*) eine Rolle spielt. Dabei geht es vordergründig darum, ob nicht manche Regelungen, die auf den Schutz von Individualrechten abzielen, einerseits zu enormen Bürokratien, Kommissionen und Protokollen führen, die allen Beteiligten »auf die Nerven gehen« und deren Schutzwirkung häufig umstritten, wenn nicht rundheraus zweifelhaft ist. Zudem entsteht nicht selten der Eindruck, dass durch die primäre Fokussierung auf Individualrechte eine ganze Reihe von systemischen Faktoren aus dem Blick gerät. Vielleicht könnte man sich manche Maßnahmen sparen, die als »Gängelung« erlebt wird, wenn man auf infrastruktureller Ebene andere Wege beschreiten würde. Darüber hinaus gibt es aber eine weit fundamentalere Ebene, nämlich die Frage danach, ob nicht Regelungsformen jenseits des Individualrechtsschutz wünschenswert wären. Damit berühren wir sehr fundamentale Fragen, die für Rechtsordnungen, die sich auf Menschenwürde und Grundrechtsschutz verpflichtet haben, zu Identitätsfragen zu werden scheinen. Diese Fragen sind natürlich ideologisch hoch aufgeladen und werden es stets mehr, je mehr Rechtsstaatlichkeit und der Primat des Individuums international und national durch Kollektivismustendenzen unter Druck zu geraten scheinen. Die Funktion des wissenschaftlichen Diskurses wäre hier vielleicht weniger darin zu sehen, gegenüber entsprechenden Tendenzen schlicht die Fahne des traditionellen, individualzentrierten Rechtsstaatsdenkens hochzuhalten, sondern könnte zunächst darin bestehen, auszuloten, was denn der Respekt vor den Grundwerten und Individualrechten im digitalen Kontext genau bedeuten kann. Die klassisch liberale Antwort wurde in anderen Zeiten entwickelt und es ist keineswegs ausgemacht, welche Orientierung die klassischen Auffassungen vom Schutz von Rechten und Freiheiten im digitalen Zeitalter bedeuten können. Gerade wer dem (Rechts-)Subjekt in Rechtsstaat und Demokratie eine weiterhin zentrale Bedeutung zuweist, sollte nicht schlicht

auf Lösungen zurückgreifen, die in längst vergangenen Zeiten entwickelt wurden. Vor der kämpferischen Verteidigung von Grundwerten sollte ihre kritische Reflexion stehen, und dies könnte dazu führen, dass mancher Antagonismus an Schärfe verliert. Damit soll die ethische und rechtliche Brisanz des Themas keineswegs nivelliert und auch nicht gefordert werden, vom Individualrechtsschutz abzurücken. Stattdessen ist zunächst schlicht die Notwendigkeit zu betonen, die möglichen Zusammenhänge der Digitalisierung mit den Voraussetzungen einer freiheitlichen Rechtsordnung umfassender zu analysieren und besser zu verstehen. Auf dieser Basis lassen sich Rückwirkungen auf grundlegende Verständnisse von Individuum, Staat und Gesellschaft erkennen, und hieraus wiederum könn(t)en übergreifende theoretische Modelle entstehen, für die die Zeit jetzt indes noch nicht reif ist. Die Reflexion über Datenzugangsregeln versteht sich als ein Baustein eines solchen übergeordneten Projekts.

Die Beiträge dieses Buches

Wir haben die Beiträge unter recht breiten allgemeinen Stichworten versammelt, die eine erste Orientierung über die verhandelten Dimensionen der Datenzugangsregeln bieten sollen: Es geht um die Frage nach der Rolle von Subjekten bei der Regelung des Datenzugangs (*Zugangssubjekte*), den leitenden Interessen der Regulierung (*Zugangsinteressen*), der zunehmenden Verschränkung der digitalen und der analogen Welt (*Zugangsverschränkungen*), die Konsequenzen, die sich aus der Ermöglichung und Begrenzung des Datenzugangs ergeben (*Zugangs(begrenzungs)konsequenzen*) und der Verantwortung für die Regulierung des Datenzugangs bzw. die Möglichkeit zur Verantwortungsübernahme (*Zugangsverantwortung*). Die Reihe wird mit Beiträgen abgeschlossen, die in knapper Form mögliche Punkte für eine zukünftige Diskussion in den Blick zu nehmen versuchen (*Ausblick*).

Zugangssubjekte

Die traditionelle Rechtskonstruktion nimmt von natürlichen Personen als Rechtssubjekten ihren Ausgang, doch diese Rolle wird im digitalen Raum problematisch. Zugangssubjekte werden aus philosophischer und soziologischer Perspektive thematisiert.

Marcus Düwell diskutiert die Herausforderung der Digitalisierung für unser Verständnis von subjektiven Rechten, deren Schutz traditionell als Kern des Rechtstaats gesehen wird. Es ist nicht evident, dass aus einer an subjektiven Rechten orientierten normativen Perspektive folgt, dass Daten primär als Privateigentum aufgefasst werden und »informierte Zustimmung« das primäre Schutzinstrument darstellt. Vielmehr wäre vorrangig zu fragen, wie die digitale Infrastruktur derart gestaltet werden könne, dass ein Schutz subjektiver Rechte überhaupt möglich wird. Der Beitrag versucht eine Perspektive auf Datenzugangsregeln zu entwerfen, die die Brücke zwischen subjektiven Rechten und gemeinschaftlichen Interessen schlägt.

Jasmin Brieske und *Doris Schweitzer* untersuchen in ihrem Beitrag, auf welche Art und Weise in den drei Datenschutz- und -zugangsregulierungen DSGVO, Data Act und Data Governance Act der einzelne Mensch als Subjekt angerufen wird. Dabei lassen sich durchaus Verschiebungen zum herkömmlichen Subjektverständnis nachzeichnen. So wird der oder die Einzelne in der DSGVO noch primär als individuelles Subjekt adressiert, das sich in einem Spannungsverhältnis zwischen Selbstermächtigung und Kontrolle befindet. In DA und DGA tritt die Anrufung als ein »dividuelles« Subjekt hinzu, welchem als teilbarer »Datenschatz« eine Infrastruktur- und Gemeinwohlverantwortung zugeschrieben wird.

Zugangsinteressen

Wer Zugang zu Daten wünscht, verfolgt Interessen. Doch diese Interessen können sehr unterschiedlich geartet sein, und nicht jedes Interesse legitimiert die gleiche Art des Zugangs. Zugangsinteressen werden aus philosophischer und juristischer Perspektive untersucht.

In ihrem Beitrag beleuchtet *Petra Gehring* die sich durch Soft Law wie auch gesetzgebungspolitisch verändernden Regeln für die Forschungsdatennutzung. Es besteht ein Spannungsfeld zwischen der Normierung des Umgangs mit Daten aus der Wissenschaft und der Zugänglichkeit von Daten für die Wissenschaft. Hier gerät das Wissenschaftssystem in die Rolle eines Datenlieferanten, für den sich die Datenzugänge jedoch – namentlich, was nicht selbst produzierte Daten angeht – tendenziell erschweren.

Lars Pfeiffer betrachtet in seinem Beitrag die zunehmende Tendenz zur gesetzlichen Normierung von Datenzugangsansprüchen am Beispiel des europäischen Digital Markets Acts, der die größten digitalen Plattformen unserer Zeit in unterschiedlichen Konstellationen zur Öffnung

ihrer Datenbestände zugunsten ihrer Endnutzer, gewerblichen Nutzer und Wettbewerber verpflichtet. Vor dem Hintergrund der mit den jeweiligen Neuregelungen adressierten Problemlagen erfolgt eine Analyse der jeweils gewählten Lösungsansätze, vor allem unter Berücksichtigung der Begünstigten und Verpflichteten der einzelnen Vorschriften sowie den vorgesehenen technischen und organisatorischen Modalitäten der Datenbereitstellung.

Zugangsverschränkungen

Datenzugang ist nicht eine Einbahnstraße, in der natürliche, körpergebundene Personen Zugang zu Daten in einer körperlosen Welt suchen, sondern die digitale Welt hat Rückwirkungen auf die Welt der Körper und des Sozialen. Diese Zugangsverschränkungen werden aus politikwissenschaftlicher und rechtlicher Perspektive untersucht.

Daniel Lambach setzt sich aus politikwissenschaftlicher Perspektive mit der *Datafizierung* der Welt auseinander. Mit diesem Begriff wird darauf hingewiesen, dass die Digitalisierung auf alle Bereiche des Lebens Einfluss hat. Dabei ist für die Regulierung des Datenzugangs ein zentrales Problem, dass die Digitalisierung einerseits keinen eindeutigen Ort in der physischen Welt hat, keine Geographie hat, was für ihre Regulierung ein zentrales Problem darstellt. Andererseits hat die Digitalisierung aber Effekte auf alle Dimensionen von Ökologie, Gesellschaft und Politik. Dieser Ambivalenz der Datafizierung muss jede erfolgreiche Regulierung Rechnung tragen.

Malte Gruber und *Zaira Zihlmann* thematisieren in ihrem Beitrag neuere Entwicklungen der datengetriebenen personalisierten Medizin, die in den jüngsten Projekten der Modellierung von menschlichen digitalen Zwillingen als medizinischen Datenkörpern gipfeln. Die Formierung solcher Datenkörper weckt auch das Interesse des Rechts, denn obschon es keinen spezifischen Rechtskorpus gibt, der sich mit dem digitalen Zwilling befasst, so agiert dieser nicht in einem rechtsfreien Raum, sondern bietet Grundlagen zur Entwicklung eines Rechts der Biodaten und wirft insbesondere die Frage nach einem transsubjektiven Datenschutzrecht auf.

Zugangs(begrenzungs)konsequenzen

Ob nun Datenzugang gewährt oder begrenzt wird, beides hat Konsequenzen oder kann Konsequenzen haben. Die Frage der Zugangs(begrenzungs)kon-

sequenzen wird besonders im Gesundheitsbereich als dringlich erfahren. Daher wird diese Frage aus medizinischer, medizinethischer und -rechtlicher Perspektive thematisiert.

Der Beitrag von *Fabiola Böning* und *Anne Richert* behandelt den angekündigten Paradigmenwechsel im Gesundheitswesen weg von einer Sekundärnutzung von Gesundheitsdaten, die insbesondere von der datenschutzrechtlichen Einwilligung abhängt, hin zu einer Widerspruchslösung unter einer erweiterten Zweckbestimmung und einem vergrößerten Kreis der zugangsberechtigten Akteure. Bei gleichzeitiger Verringerung individueller Einflussnahmemöglichkeiten führt dies zu Überlegungen, wie die Rechte der Patienten und Patientinnen auf kollektiver Ebene gestärkt werden können. Im Fokus stehen dabei die relevanten Digitalgesetze auf europäischer und nationaler Ebene.

Frank Niggemeier erörtert in seinem Beitrag die Frage, ob Selbstbestimmung – einschließlich der Zustimmung zur Erhebung, Verarbeitung und Speicherung zweckrelevanter Daten – nicht primär in lebensweltlichen Entscheidungen wie dem Aufsuchen eines Arztes stattfindet. Insofern wäre statt einer weiteren bürokratischen Aufspaltung separater »Einwilligungen« der Ausbau wirksamer Maßnahmen gegen unbefugte Datenzugriffe, gegen Datenmissbrauch und daraus resultierende Stigmatisierung, Diskriminierung oder Benachteiligung geboten, um die Persönlichkeitsrechte effektiv zu schützen und eine kontrollierte Datennutzung zu individuellen oder gesetzlich bestimmten Zwecken zu erleichtern.

Der Beitrag von *Philipp Kellmeyer* untersucht die ethischen Herausforderungen der Nutzung digitaler Zwillinge im Gesundheitswesen, mit besonderem Fokus auf Datenessenzialismus, Vulnerabilität und strukturelle Ungerechtigkeit. Er argumentiert, dass die Reduktion komplexer menschlicher Identitäten auf quantifizierbare Daten die Gefahr von Fehldiagnosen und Datenschutzverletzungen birgt, und hebt die Notwendigkeit hervor, vulnerable Gruppen zu schützen. Durch partizipative Forschung und partizipative Governance-Modelle sollen ethische Spannungen gemindert und eine gerechte und inklusive Nutzung dieser Technologien sichergestellt werden

Zugangsverantwortung

Unter dem Stichwort *Zugangsverantwortung* wird philosophisch und juristisch in den Blick genommen, mit welchen Veränderungen der Verantwortungsperspektive im digitalen Raum zu rechnen ist.

Benjamin Müller fragt, was die digitale Situation für die menschliche Freiheit im demokratischen Kontext bedeutet. Kann man sich im Datendickicht noch selbstbestimmt behaupten und sinnvoll zur Verantwortung gezogen werden? Neben den digitalen Herausforderungen ist Selbstbestimmung zugleich mit systematischen Problemen einer Freiheitsdialektik konfrontiert, die sich an Datenzugängen aufzeigen lässt und an Datenschutz und Aufklärung näher beleuchtet wird.

Der Beitrag von *Steffen Augsberg* untersucht aus primär rechtswissenschaftlicher Perspektive, welche Regulierungsmodi in der bisherigen Regelung von Datenzugangsmodellen dominieren, welche praktischen und ideologischen Gründe hinter diesen Entscheidungen stehen und inwieweit sich aktuell Veränderungen sowie zukunftsrelevante Entwicklungstrends erkennen lassen. Er kontrastiert die herkömmlichen, stark auf die Individualkontrolle abstellenden Ansätze sodann mit unterschiedlichen Alternativkonzepten und legt dar, inwieweit diese jeweils mit konkreten Verantwortungszuweisungen verbunden sind. Ziel ist es, zunächst ein Bewusstsein für komplexere, netzwerkadäquate Regelungsoptionen und deren Konsequenzen zu schaffen – gerade weil *one size fits all*-Lösungen illusorisch und folglich stärkere Ausdifferenzierungen geboten sein dürften.

Ausblick

Der Beitrag von *Petra Gehring* und *Daniel Lambach* thematisiert neue Imperative, welche die sogenannte »Zeitwende« für eine datafizierte Wissenschaft mit sich bringt. Zum Programm »Open Science« stehen neuartige Maßgaben, Dual Use-Konstellationen durchgehend zu prüfen sowie internationale Kooperationsbeziehungen als Teil der Verantwortung von Wissenschaftlern restriktiv zu handhaben, in einem noch gänzlich ungeklärten Verhältnis.

Der abschließende Text »*Datenzugangsregeln als Aufgabe*« von *Steffen Augsberg* und *Marcus Düwell* formuliert auf der Basis der Texte dieses Bandes einige grundlegende Gesichtspunkte für die zukünftige Diskussion um Datenzugangsregeln. Damit wollen wir das Gespräch zu dem Thema nicht ab-

schließen, sondern vielmehr einen Beitrag leisten, um diesem Gespräch eine fruchtbare Richtung zu geben.

Dank

Dieses Buch repräsentiert das Ergebnis der Projektgruppe »Datenzugangsregeln« des »Zentrums Verantwortungsbewusste Digitalisierung« (ZEVEDI). Die seit Ende 2022 tätige Projektgruppe hat drei Veranstaltungen in Kassel, Gießen und Darmstadt ausgerichtet, von denen die Texte dieses Bandes sehr profitiert haben. Wir danken allen Teilnehmenden dieser Workshops für ihre konstruktiven Beiträge. Wir danken ferner allen Mitgliedern und Mitarbeitenden der Projektgruppe für die konstruktive, verbindliche und menschlich angenehme Arbeitsatmosphäre. Wir danken der Geschäftsstelle des ZEVEDI für die gute Unterstützung, insbesondere Klaus Angerer für seine Hilfe bei der Vorbereitung der Workshops.

Wir hoffen, dass dieses Buch seinen Weg in die wissenschaftliche wie politische Debatte um Datenzugangsregeln finden und weitere Diskussionen anregen wird.

Gießen und Darmstadt im Juni 2024

Steffen Augsberg, Marcus Düwell und Benjamin Müller

Zugangssubjekte: Zuordnungsprobleme und Ambivalenz der Regelungskompetenz

Datenzugangsregeln und subjektive Rechte: Zum Spannungsfeld von Individualschutz und gesellschaftlichen Gütern

Marcus Düwell

1. Einleitung

Der Schutz von Individualrechten bildet die normative Grundlage des modernen Rechtsstaats. Recht schützt die Rechte des Individuums. Rechte sind immer Rechte von Individuen, die der Staat in kollektiver Perspektive schützt, der Staat schützt die Rechte aller Individuen. Auch wenn es objektive Verpflichtungen des Staates oder die fiktive Rechtssubjektivität von nicht-natürlichen Personen gibt, so sind diese doch begründet oder begrenzt durch Rechte von natürlichen Personen. Im Hinblick auf Datensubjektivität scheint dies prima facie zu implizieren, dass das Subjekt ein Recht auf seine Daten hat, dass es sie als sein Eigentum oder analog zu Eigentumsverhältnissen auffassen kann und dass ihm eine Autorität über die Verwendung seiner Daten zukommt – eine Autorität, die den Staat bindet und wodurch das Handeln des Staates und das Handeln Dritter zu begrenzen ist. Im Lichte einer solchen Auffassung von Daten wäre für jede Form des Umgangs mit Daten die Zustimmung der Eigentümer erforderlich. Diese Konstruktion ist jedoch in mehrfacher Hinsicht zumindest dysfunktional oder sogar zweifelhaft: Ein solches Konsenserfordernis scheint nicht praktikabel, bisweilen sind die Nutzungsmöglichkeiten von Daten nicht im Vorhinein absehbar, die Schutzwirkung einer Zustimmung ist zweifelhaft und in internationaler Perspektive wird die nationale Gesetzgebungskompetenz, die für die Durchsetzung eines solchen Erfordernis notwendig wäre, durch technologische Entwicklungen und Verflechtungen von global-agierenden Firmen ausgehebelt. Dieses Verständnis von Daten in eigentumsrechtlicher Perspektive ist jedoch möglicherweise nicht allein dysfunktional, sondern es verstellt vielleicht auch den Blick darauf, dass es alternative Verständnisse von Individualrechten gibt, durch welche Schutz-

mechanismen in den Blick genommen werden könnten, die subjektive Rechte effektiver schützen könnten.[1]

Falls die Vermutung der Dysfunktionalität dieses Regelungsregimes zutreffen sollte, kann man daraus unterschiedliche Konsequenzen ziehen. Man kann etwa die Position vertreten, dass wir Regelungen treffen sollten, die sich von der Bindung an Individualrechten verabschieden. Ein solcher Vorschlag wäre allerdings kaum mit der grundlegenden normativen Festlegung des Rechtsstaats auf den Schutz von Individualrechten vereinbar. Falls man diesen Weg einschlagen würde, müsste man die gesamte Rechtsordnung so interpretieren, dass der Schutz von Individualrechten nicht mehr den höchsten normativen Gesichtspunkt der Rechtsordnung darstellt. Eine solche Position könnte man etwa versuchen damit zu begründen, dass es unmöglich sei, den normativen Vorrang von Individualrechten konsequent aufrechtzuerhalten, weil die komplexe Lebenswirklichkeit im digitalen Zeitalter dies de facto unmöglich mache, etwa weil ein konsequenter Datenschutz mit derart problematischen Konsequenzen für den Schutz von Individualrechten in anderen Bereichen verbunden wäre, dass eine Individualrechtsposition an ihren inneren Widersprüchen scheitern würde. Eine solche Schlussfolgerung wäre meines Erachtens allerdings nur dann intellektuell plausibel, wenn man zuvor gezeigt hätte, dass eine Individualrechtsposition auch wirklich scheitern muss, d.h. dass nicht allein die derzeitige Ausgestaltung einer derartigen Individualrechtsordnung sondern auch mögliche alternative Gestaltungsformen zum Scheitern verurteilt seien. Davon kann bislang aber keine Rede sein.

---

1 Niklas Kirchner (ETH Zürich) hat diesen Beitrag während eines Workshops im April 2024 mit einem ganz hervorragenden Kommentar versehen, für den ich ihm nachdrücklich zu Dank verpflichtet bin. Ich bin leider in diesem Kontext nicht in der Lage, alle weiterführenden Gesichtspunkte so zu würdigen, wie sie es verdienen. Eine wesentliche Unterscheidung sei allerdings in meinen Worten kurz paraphrasiert: Die hier angedeutete Dysfunktionalität könnte in zweierlei Hinsicht interpretiert werden. Einerseits könnte man behaupten, dass bestimmte Datenzugangsregelungen dysfunktional seien, weil sie gegebene normative Ziele nicht erreichen (also etwa den Schutz von Individualrechten). In einem anspruchsvolleren Sinne könne man aber auch von Dysfunktionalität reden, wenn die Datenzugangsregeln selbst normative Sachverhalte schaffen, die zu schaffen zweifelhaft wäre. So könnte man etwa fragen, ob nicht mit der Idee, dass ich ein eigentumsanaloges Recht auf meine Daten habe, diese erst eine Form erhalten, in denen sie zum Gegenstand ökonomischen Handelns zu werden. Eine solche Kommodifizierbarkeit der Daten durch die Zuschreibung eines spezifischen Rechtsstatus könnte man allerdings im Rahmen einer Ethik subjektiver Rechte als solche bereits moralisch kritisch betrachten.

Hier soll ein alternativer Weg erkundet werden, indem zunächst gefragt wird, ob eine normative Bindung von Datenzugangs- und Datenumgangsregeln an Individualrechte notwendigerweise dazu führt, dass diese Rechte in Form von Eigentumsbegriffen oder eigentumsanalogen Begriffen gedacht werden müssen oder ob es andere Möglichkeiten der Interpretation von Individualrechten gibt und welche normativen Konsequenzen daraus zu ziehen seien. Kurz gesagt geht es darum zu erkunden, welche alternativen Wege zu Datenzugangsregeln auf der Basis einer Theorie subjektiver Rechte verfolgt werden können. Der Text wird sein Argument in drei Schritten entfalten: Zunächst wird ein grundlegendes Verständnis subjektiver Rechte vorgeschlagen (2.), danach werden Implikationen für das Verhältnis von Rechten und Daten erarbeitet (3.) und zum Schluss einige Konsequenzen für Datenzugangsregeln vorgeschlagen (4.).

Da ich hier als Philosoph (und juristisch interessierter Laie) argumentiere, scheint mir eine Vorbemerkung am Platze, wie ich das Verhältnis von Philosophie und Recht sehe. Mir scheint, dass die Grundlage des Rechts nicht einfach mit dem positiven Recht gesetzt wird, sondern dass eine Rechtsordnung den Anspruch haben sollte, die basalen Annahmen, auf denen sie beruht, konsistent und systematisch erläutern zu können. Dies folgt bereits aus der Idee der Rechtsordnung als einer systematischen Ordnung von rechtlichen Regelungen und gilt sicherlich in besonderer Weise für eine Rechtsordnung, die auf Menschenwürde und Grundrechte festgelegt ist. Die Reflexion auf die systematische Konsistenz der normativen Ausgangspunkte der Rechtsordnung ist aber nach meinem Verständnis eine der Aufgaben der praktischen Philosophie. Wenn es in diesem Zusammenhang also um »Rechte« geht, so behaupte ich, dass dies Thema angemessen nicht allein im Rahmen der Rechtsphilosophie zu thematisieren ist, sondern auf der Schnittstelle von Ethik, politischer Philosophie und Rechtsphilosophie. Das setzt kein besonderes Geheimwissen des Philosophenkönigs voraus, sondern nur konsequente Ausarbeitung dessen, wie wir »Recht« und »Rechte« konsistent denken können. Der Anspruch auf konsistentes Denken verbindet aber Philosophie, Rechtswissenschaften und den um ein Verständnis des Rechts bemühten Bürger, kurz gesagt: uns alle.

2. Ein Verständnis subjektiver Rechte[2]

Es ist keineswegs eine ausgemachte Sache, wie wir subjektive Rechte interpretieren können und sollten und es ist ebenso wenig ausgemacht, wie die Geschichte des Entstehens der Idee subjektiver Rechte rekonstruiert werden kann. Diese Geschichte zu verstehen ist jedoch wichtig, weil eine spezifisch historisch-kulturelle Sichtweise zutreffen könnte, wonach die Idee subjektiver Rechte lediglich die Antwort auf spezifische Herausforderungen der Vergangenheit darstellt und sich nicht dafür eignet, normative Antworten auf die Herausforderungen des 21. Jahrhunderts (wie die Regulierung der Digitalisierungen oder ökologische Probleme) zu finden. Während die Akzeptanz subjektiver Rechte bisweilen mit der Entstehung moderner Eigentumsverhältnisse verbunden und/oder als Resultat frühmoderner Religionskriege verstanden wurde, ist jedoch besonders die mittelalterliche und frühneuzeitliche Vorgeschichte dieser Idee und damit verbunden ihre ideengeschichtliche Einordnung Gegenstand interessanter Debatten (z.B. Tuck 1979, Tierney 2014, Brett 1997). Abhängig von den unterschiedlichen Perspektiven auf diese Geschichte wird man die Rolle der Rechte seit dem 18. Jahrhundert (etwa Moyn 2010) und ihre mögliche Rolle im 21. Jahrhundert unterschiedlich interpretieren. Dabei geht es sowohl um die Rolle von Grundrechten, ihre globale Erweiterung zu Menschenrechten und deren konzeptionelle Grundlegung im Begriff der Menschenwürde (Düwell u.a. 2014). Strittig dabei ist aber nicht nur im engeren Sinne das Konzept von Rechten in Ethik und Recht, sondern auch das Verständnis von Subjektivität, welches den subjektiven Rechten zugrunde liegt, oder auch die Frage, wie verschiedene Auffassungen von der Rolle des Staates und der Rolle der Politik mit dem Verständnis von Rechten verbunden sind, bzw. verbunden sein können, bzw. wie ein veränderndes Verständnis dieser Begriffe auf deren internen Zusammenhang zurückwirkt.

Es wird etwa der Verdacht geäußert, dass die Festlegung staatlichen Handelns auf vorpolitische moralische Ansprüche in Form von Rechten verhindert, dass der politische Raum sich als effektiver Ort politischer Auseinandersetzungen entwickeln kann, da er gleichsam moralisch stillgestellt wird und daher zwangsläufig zur Entpolitisierung neigt (Menke 2015). Eine

2 Diese kurze Skizze steht im Zusammenhang eines umfangreicheren Projekts zum Thema Menschenwürde und Menschenrechte, das ich in zahlreichen Texten entwickelt habe. Siehe etwa Düwell 2014, 2020, 2022.

ähnliche Kritik wurde international in den letzten 15 Jahren um das Verständnis der Menschenrechte geführt, wobei besonders C. Beitz (2009) (und seine Anhänger) sich dagegen gewandt haben, Menschenrechte im Sinne moralischer Ansprüche zu verstehen. Dahinter steht die Annahme, dass ein moralisches Verständnis der Menschenrechte zu einer Auffassung führt, wonach diese quasi direkt aus dem Naturrecht in die Grundlage internationalen Rechts einwandern. Dies fördere aber nicht nur ein inadäquates Verständnis der politischen Funktion von (Menschen-)Rechten (nämlich als Gegenstand politischer Auseinandersetzung), sondern verenge (oder bedrohe) auch den Raum politischer Handlungs- und Verhandlungsmöglichkeiten in problematischer Weise. J. Waldron (1999) (und andere) haben dagegen bereits seit Langem die Auffassung vertreten, dass der politische Raum als Ort verstanden werden muss, in dem Uneinigkeit auf sehr fundamentalem Niveau möglich ist und möglich sein muss. Diese Uneinigkeit schließt Streit über das Verständnis von Grund- und Menschenrechten explizit ein, womit eine vorgängige Bindung des Staates an derartige Rechte im Streit zu sein scheint. Wird dieser Streit innerhalb des politischen Raums nicht mehr führbar, so verlieren wir wesentliche Funktionen des Politischen mit weitreichenden und potentiell desaströsen Folgen. Dagegen soll hier eine Perspektive auf Rechte vorgestellt werden, wonach diese zwar mit einem fundamentalen moralischen Anspruch verbunden sind, welcher aber den politischen Raum nicht zu destruieren, sondern allererst zu ermöglichen beansprucht.

Auf dem Weg zu subjektiven Rechten spielt der franziskanische Armutsstreit des 14. Jahrhunderts laut verschiedener Autoren eine wesentliche Rolle (etwa Brett 1997). Während im römischen Recht Rechtstitel gebunden sind an die Zugehörigkeit zu einem »dominium«, entspinnt sich im Gefolge des Ideals radikaler Armut und Besitzlosigkeit der franziskanischen Minoriten die Frage nach dem naturrechtlichen Status des Eigentums. Während die offizielle Lehre behauptet, dass es auf Eigentum einen naturrechtlichen Anspruch gibt und dass nur das Haben von Eigentum den Genuss weltlicher Dinge (zumindest Nahrung, Kleidung, Obdach) gestattet, wird zunächst eine Minderheitenposition vertreten, die den Anspruch auf Eigentum optional macht und die Möglichkeit zur Nutzung weltlicher (zumindest lebensnotwendiger) Dinge nicht vom Eigentum abhängig macht. Einerseits wird das Konzept des Benutzens und Genießens von weltlichen Dingen (usufructus) entwickelt, wodurch ein komplexeres Verständnis von »etwas haben«, »etwas besitzen« und »etwas gebrauchen und genießen« können entsteht. Damit wird auch

das Verhältnis des Subjekts und Objekts des »Besitzens«/»Habens« komplexer gedacht. Brian Tierney rekonstruiert anhand der Position im Armutsstreit von Marsilius von Padua (Tierney 2017), dass in das Verständnis des Rechts die Idee einer Erlaubnis eingeführt wird. Wenn A einen Anspruch auf X hat (etwa einen Besitztitel), so muss es für A zunächst erlaubt (permission) sein X zu haben, bevor von einem Anspruch geredet werden kann. Mit der Erlaubnis wird jedoch der Wille des Subjekts des Habens zu einer wesentlichen Instanz, wodurch eine Konzeption des Rechts denkbar wird, für die der Wille des Rechtssubjekts eine autoritative Instanz wird. Indem das Naturrecht Eigentum optional macht (das Subjekt also auch entscheiden kann, besitzlos zu leben und von den Dingen zu leben, die die Natur zur Verfügung stellt oder die erbettelt werden), wird die Möglichkeit des subjektiven Rechts möglich. Laut Tierney ist es diese sukzessive Ausbreitung des »permissive natural laws« zwischen dem 12. und 18. Jahrhundert, dass den Weg zu einem gewandelten Verständnis von Rechten ermöglicht und damit die Idee einer liberalen politischen Ordnung allererst denkbar macht. Mit diesem Konzept eines subjektiven Rechts wird es dann auch denkbar, dass allerlei immaterielle, subjekt-gebundene Rechtsgüter den Status eines Rechts erhalten, wie etwa das Recht, die eigene Meinung frei zu äußern, oder das Recht, einen spezifischen Lebenswandel zu pflegen, der seinerseits in bestimmten Glaubensüberzeugungen begründet ist.

Es geht jetzt nicht darum, dieser Geschichte im Einzelnen nachzugehen. Auch sei betont, dass ich hier lediglich aus der Forschungsliteratur berichte und nicht den Anspruch erhebe, eigene ideengeschichtliche Forschungsergebnisse vorzustellen. Doch dieser kurze Ausflug ins Mittelalter verdeutlich bereits, dass es zu kurz gegriffen wäre, würde man die Idee subjektiver Rechte lediglich als Abwehrrecht gegenüber dem Staat oder als Lösung der frühneuzeitlichen Glaubenskriege verstehen. In all diesen Hinsichten mögen subjektive Rechte eine Rolle gespielt haben und spielen, aber ihre Bedeutung erschöpft sich nicht darin.

Wenn diese Rekonstruktion plausibel ist, so deutet dies auch darauf hin, dass ein adäquates Verständnis von Rechten mit dem menschlichen Willen verbunden ist, dass Rechte also nicht verstanden als Schutzformen von grundlegenden Interessen (Beitz 2009) werden sollten. Rechte haben vielmehr mit der Ermöglichung der Realisierung des Willens zu tun, wobei der Wille des Anderen die grundlegende Grenze für ihre Realisierungsmöglichkeit darstellt. Dies muss nicht so verstanden werden, dass die Faktizität des Willens selbst eine normative Bindung hervorbringt. Der Übergang

von einem Willen zu einem Recht wäre begründungstheoretisch genauso mysteriös wie derjenige von einem faktischen Interesse zu einem Recht. Moralphilosophisch relevant wäre insofern zu verstehen, wie der Übergang von einem Wollen zu einem Sollen verstanden werden kann. Zu begründen wäre also, dass im Wollen ein Anspruch auf Realisierung dieses Wollens grundgelegt ist, der andere Handelnde verpflichtet.

Dies kann meines Erachtens nur erfolgreich sein, wenn man zeigen kann, dass das Verhältnis zum eigenen Wollen nicht nur kontingenterweise ein normativ gehaltvolles ist, sondern dass Handelnde im Allgemeinen die eigene Handlungsfähigkeit als ein Gut ansehen müssen (Gewirth 1978). Dabei wäre dies »müssen« so zu verstehen, dass eine rationale Rekonstruktion derjenigen Annahmen, die handlungsfähige Wesen vornehmen müssen, um sich als praktische Wesen konsistent verstehen zu können, stets implizieren, dass sie die eigene Fähigkeit, handeln zu können als Gut ansehen. Dabei geht es um eine rationale Rekonstruktion des »praktischen Selbstverständnisses« und nicht um eine spieltheoretische Erläuterung, dass dies im strategischen Vorteil von Handelnden läge. Eine solche Argumentation wird dann aber ein Ansatz sein müssen, der über die Fähigkeit zum Handeln argumentiert, die zu erhalten und entwickeln zu können, Gegenstand des Rechtsschutzes ist.[3]

Für diese Argumentation muss man annehmen, dass der Grund für den Respekt vor subjektiven Rechten in der Wertschätzung vor der eigenen Handlungsfähigkeit in Handlungssubjekten liegt und dass diese Wertschätzung allen Handlungssubjekten zugeschrieben werden kann. Wenn dies zutrifft, so sind zugleich die Bedingungen der Handlungsfähigkeit Gegenstand des Schutzes subjektiver Rechte. Subjektive Rechte zu respektieren bedeutet dann, die Bedingungen zu schützen, die diese Subjekte zum Handeln befähigen. Diese Bedingungen sind subjektiv variabel, aber zugleich gibt es eine kollektive Dimension. Ich habe etwa – wie andere auch – ein Recht auf körperliche Unversehrtheit, um Handeln zu können, aber zugleich gibt es kollektive Rahmenbedingungen (relative Sicherheit, ökologische Rahmenbedingungen etc.), ohne die eine Wahrnehmung von Rechten überhaupt nicht möglich ist. Subjektive Rechte begründen insofern eine staatliche Verpflichtung, auf die Sicherstellung von Rahmenbedingungen, unter denen erfolgreiches Handeln allererst möglich ist. Da über die Frage,

3 Zur Unterscheidung des hier angenommen Ansatzes vom sogenannten »Capabilities approach« vgl. Claassen/Düwell 2013.

welche Rechte dies im Einzelnen sind und wie sie zu hierarchisieren sind, Streit und Auseinandersetzung möglich ist, ergibt sich die Notwendigkeit des Schutzes eines politischen Raums, in dem dieser Streit geführt werden kann.

In dieser Konstruktion werden bestimmte Annahmen gemacht über Handlungssubjekte. Diese ergeben sich aus den Sinnbedingungen des Handelns, wie es für jede Form praktischer Konflikte, praktischer Auseinandersetzung und praktischer Deliberation vorausgesetzt werden muss. Das heißt, mit der Rede von Handeln, Rechten und Politik sind bestimmte Voraussetzungen notwendigerweise verbunden: Wir müssen Subjekte voraussetzen, die in der Lage sind, praktische (instrumentelle, moralische, politische etc.) Forderungen und Gründe zu verstehen und sich zu ihnen (affirmierend oder abweisend) zu verhalten. Wir müssen Subjekte voraussetzen, die zumindest im Prinzip in der Lage sind, Präferenzen, Wünsche und Interessen zu entwickeln, diejenigen anderer zu verstehen und sich zu den Präferenzen, Wünschen und Interessen anderer zu verhalten. Wir müssen darüber hinaus annehmen, dass diese Subjekte weiterhin in der Lage sind, zwischen den verschiedenen normativen Erwägungen Hierarchisierungen und Abwägungen vorzunehmen. Letzteres wird ab einem bestimmten Komplexitätsgrad nur arbeitsteilig und in organisatorischer Abstimmung erfolgen können.

Für den hier vorliegenden Kontext ist der wesentlichste Gesichtspunkt, dass subjektive Rechte als Legitimationsinstanz für staatlich und politisches Handeln gedacht werden können, dass aber die korrespondierenden Verpflichtungen nicht notwendigerweise Verpflichtungen gegenüber individuellen Handlungssubjekten sind, sondern gegebenenfalls Verpflichtungen zur Gestaltung eines geteilten Handlungsraums. Subjektive Rechte zur respektieren, impliziert notwendigerweise, diejenigen Voraussetzungen zu schützen und zu fördern, die erforderlich sind, um subjektive Rechte realisieren zu können. Und diese Voraussetzungen sind primär geteilte Güter generische Bedingungen der Handlungsfähigkeit, wie man sie im Anschluss an A. Gewirth (1978) nennen kann (vgl. hierzu: Steigleder 1999). Wer subjektive Rechte respektiert, schützt Güter, die für uns gemeinsam Bedingungen sind, unter denen gehandelt werden kann. Dabei sind nicht alle »generic goods« gleich wichtig für die Realisierungsmöglichkeiten von Handlungsfähigkeit. Es gibt daher von der Perspektive der Dringlichkeit bestimmter Güter als Bedingungen der Handlungsfähigkeit die Notwendigkeit von Hierarchisierungen. Zugleich kann natürlich von einem Respekt

vor subjektiven Rechten gesprochen werden, wenn die Art dieses Schutzes sich in den Grenzen abspielt, in denen das Subjekt nicht zu kollektiven Zwecken geopfert wird. Wo diese Grenze genau verläuft, ist ein Thema, dass im Einzelnen nicht einfach zu bestimmen ist.

3. Daten und subjektive Rechte

Vor dem Hintergrund dieser Skizze zur Rolle subjektiver Rechte ergeben sich verschiedene Wege, wie »Daten« in den Blick kommen können. Es geht mir im Folgenden darum zu verstehen, in welcher Hinsicht Daten im Hinblick auf subjektive Rechte eine Rolle spielen können. Dabei werde ich die Diskussion nicht von vorneherein auf die moralische, politische oder rechtliche Dimension beschränken, sondern ich werde versuchen, eine generische normative Dimension in den Blick zu nehmen. Entsprechend wird von »Rechten« und »Verantwortung« auch nicht allein auf einer dieser drei Dimensionen gesprochen. Das bedeutet keineswegs, dass diese Unterscheidungen irrelevant seien, ganz im Gegenteil. Aber zunächst einmal geht es mir darum zu verstehen, welche Charakteristika von Daten denn überhaupt im Hinblick auf subjektive Rechte relevant sein können. Dabei stellt ein solcher Relevanzaufweis noch keinen Grund für strikte Verbote dar. Auch wenn manche Rechte Gründe für kategorische und eventuell sogar ausnahmslose Verbote sein mögen (das Folterverbot könnte ein Beispiel dafür sein), so sind Rechte im Allgemeinen doch Gegenstand von Abwägungen. Über die Frage, nach Kriterien der Gewichtung in solchen Abwägungsprozessen wird man noch eigens nachdenken müssen, wobei das Gewicht, dass die verschiedenen Aspekte für die Bedingungen der Handlungsfähigkeit haben, bei der Abwägung leitend sein müsste. Zunächst geht es aber nur darum sehr schematisch grundsätzliche Aspekte einer normativen Relevanz von Daten unterscheiden. Es geht dabei lediglich um eine rein begriffliche Unterscheidung von Verantwortungsdimensionen, ohne mit den Unterscheidungen bereits Gewichtungen und substantielle Stellungnahmen zu verbinden.

Erstens: Daten sind nicht einfach da, sondern Daten werden erhoben, gesammelt oder produziert, kurz: hergestellt. Damit können Fragen nach der Verantwortung dieser Herstellung gestellt werden. Man kann also fragen, wann Daten erhoben werden dürfen, unter welchen Bedingungen, über wen, von wem. Man kann dies *Datenverantwortung* nennen.

Zweitens: die Herstellung erfolgt nicht fallweise, sondern systematisch. Man erhebt Forschungsdaten, Gesundheitsdaten, die Daten von Bevölkerungsgruppen, Patientengruppen, Teilnehmende an einem Forschungsprojekt etc. Es werden Datenbanken gebaut, Infrastrukturen und Netzwerke bereitgestellt und möglicherweise erfolgt deren Erstellung sogar auf der Basis einer gesetzlichen Anordnung. Die Systematik der Erstellung dieser Infrastruktur kann unter Verantwortungsgesichtspunkten befragt werden, ist also rechtfertigungsbedürftig. Man könnte von *Infrastrukturverantwortung* sprechen.

Drittens: die Erhebung von Daten ist in vielen Fällen eine Voraussetzung zur Aufrechterhaltung der Funktionalität bestimmter gesellschaftlicher (Sub-)Systeme. Medizinischer Fortschritt etwa ist ohne systematische Erhebung von Gesundheitsdaten nicht denkbar. Insofern es ein Recht auf Zugang zu medizinischer Versorgung gibt und insofern Patienten sogar (laut Menschenrechtsregelungen) einen Anspruch auf Zugang zur qualitativ besten Medizin haben, gibt es aus der Perspektive von Individualrechten eine gesellschaftliche Verpflichtung, Forschungen durchzuführen, womit in der Regel auch die Notwendigkeit begründet ist, Gesundheitsdaten zu erheben. Entsprechendes gilt für Forschungsdaten sowie für Datenerhebungen, die zur Erfüllung basaler gesellschaftlicher und politischer Aufgaben erforderlich sind. Man könnte hier von einem *Gesellschaftsbezug der Daten* sprechen.

Viertens: Daten können einen direkten Individualbezug haben. Daten sagen dann etwas über Individuen, lassen Rückschlüsse auf die Gesundheit von Individuen zu, offenbaren private Aspekte von Handlungssubjekten, von denen nicht eo ipso angenommen werden kann, dass eine entsprechende Publizität gewünscht ist. Es kann also einen Anspruch von Individuen geben, die Publizität der Daten zu autorisieren, da die Bekanntheit der Daten deren Interessen berührt. In diesem Fall gibt es ein *subjektives Interesse an den eigenen Daten*.

Fünftens: noch unabhängig von den Interessen, die man an den Daten haben kann, könnte man behaupten, dass es Ansprüche gibt, die allein mit der Herkunft der Daten zu tun hat. Die Daten stammen von mir und man könnte argumentieren, dass ich ein Recht habe zu autorisieren, was mit diesen Daten geschieht. Dieser Aspekt könnte etwa relevant sein, weil ohne die Teilnahme von Individuen bestimmte Datenerhebungen gar nicht möglich sind. Der Aspekt ist unterschieden von dem unter Viertens genannten Gesichtspunkt, weil es hier Ansprüche geben könnte, die auch dann relevant

sind, wenn die Daten vollständig anonymisiert sind und ein Rückbezug auf den Datenspender gar nicht möglich ist. In dem Fall wäre zu argumentieren, dass es auch ohne einen Rückbezug auf subjektive Interessen Rechte an Daten gibt. Man könnte hier von *Datenspenderechten* sprechen.

Es ist wahrscheinlich, dass die Liste relevanter Unterscheidungen im Hinblick auf den Bezug von Daten und subjektiven Rechten unvollständig ist. Insbesondere kommen sicherlich mit dem Gesellschaftsbezug von Daten eine Reihe weiterer Gesichtspunkte in den Blick, die wiederum indirekt subjektive Rechte tangieren könnten. Der Zusammenhang mit subjektiven Rechten ist in vielen Fällen nicht so direkt, wie es das Beispiel von Gesundheitsdaten suggeriert, bei dem es einerseits darum gehen kann, dass betroffene Subjekte zumindest prima facie einen Anspruch darauf haben, dass Forschung im Bereich der Medizin gemacht wird, und andererseits die für diese Forschung erforderliche Datenerhebung häufig sehr direkt deren individuelle Interessen berührt. In einem beträchtlichen Teil der Forschung dagegen sind derartige normative Zusammenhänge mit subjektiven Rechten indirekt und spekulativ. So wird in der Regel ein Forschungszusammenhang etabliert, der zwar in seiner generellen Zielsetzung einen Verband mit gesellschaftlichen Zielen aufweist, der seine letzte Legitimität in Rechten hat.

Dies gilt etwa für Forschung im Bereich von Gesundheit und Nachhaltigkeit, die sich aus Rechten von Bürgern an Gesundheit und entsprechenden Umweltbedingungen ergibt. Da bestimmte Umweltbedingungen für das Leben der Menschen unverzichtbar sind, ungeachtet der Handlungsziele, die sie verfolgen mögen, haben sie auch ein Recht auf die Etablierung einer Forschung, die für einen Schutz entsprechender Umweltbedingungen erforderlich sind. Würde eine solche Forschung gar nicht gefördert, könnte man nicht seriös behaupten, die entsprechenden Rechte von Menschen zu respektieren. Da aber der geeignete Weg, die Umweltbedingungen zu schützen, gerade Gegenstand der politischen Auseinandersetzung und der Forschung ist, lässt sich hier in der Regel nur ein Zusammenhang rekonstruieren zwischen den Rechten von Menschen und der Legitimität oder Notwendigkeit der Etablierung eines entsprechenden Forschungsgebiets, nicht auf spezifische Forschungsprojekte (sicherlich nicht im Sinne eines rechtlich einklagbaren Anspruchs). Das heißt, man kann aus der Verbindlichkeit von Rechten nur schließen, dass ein Forschungsprozess in diesem Bereich prinzipiell geboten ist. Das bedeutet aber auch, dass die Erhebung der entsprechenden Daten geboten ist. Aber die Unbestimmtheit des geeig-

neten Weges zur Erreichung des normativen Ziels hat auch Konsequenzen für die Art der Verbindlichkeit zur Erhebung der entsprechenden Daten. Es kann also nicht einfach aus der Zielsetzung der Forschung zur Nachhaltigkeit geschlossen werden, dass Individualrechte zurücktreten müssen. Gleichwohl kann es auch nicht der Fall sein, dass derartige Forschung mit Verweis auf Individualrechte prinzipiell verunmöglicht wird, denn die Verbindlichkeit der Individualrechte erfordert es, eine solche Forschung durchzuführen.

Wenn man auf dieser Linie weiterdenkt, so gibt es noch eine weitere Verantwortungsdimension. Wenn einerseits aus der Verbindlichkeit von Individualrechten folgt, dass es eine Verantwortung dafür gibt, Forschung zu ermöglichen, die für die Sicherung dieser Rechte langfristig erforderlich ist, und man sich zugleich bewusst macht, dass durch die für diese Forschung erforderliche Datensammlung ihrerseits eine mögliche Gefährdung von Individualrechten darstellt, so ergibt sich eine höherstufige Verantwortungsdimension: Die Infrastrukturverantwortung müsste so gestaltet werden, dass eine Datenverantwortung überhaupt wahrgenommen werden kann, d.h. dass es politische und gegebenenfalls auch rechtliche Möglichkeiten gibt, die entsprechenden Abwägungen über den Umgang mit Daten Individualrechtskonform gestalten zu können.

Nun könnte man argumentieren, dass einer solchen Infrastrukturverantwortung eine besondere Dinglichkeit zukommt, insofern sie die Bedingung dafür darstellt, Verantwortung überhaupt wahrnehmen zu können. Dieses Primat ergibt sich aus der kollektiven Natur von Datensammlungen, die nur in einem großen Stil gesammelt werden können und sich daher Einzelfallabwägungen und Individualregelungen häufig oder sogar in der Regel entziehen. Daraus ergibt sich jetzt das folgende Problem: Je stärker versucht wird, Datenverantwortung im Einzelnen zu regeln, desto komplexer und schwieriger wird es häufig, Abwägungsfragen zwischen den legitimen Interessen an den eigenen Daten und der Realisierung des relevanten Gesellschaftsbezuges zu entscheiden. Es kann also die Situation auftreten, dass gerade der Versuch, Individualrechte auf dem Niveau konkreter Datenerhebungen zu schützen, das Risiko mit sich führt, dass Rechte auf medizinischen Leistungen nicht oder unzureichend geschützt werden. Das soll nicht bedeuten, dass die Erwartung eines möglichen medizinischen Fortschritts es legitimiert, sich über allerlei Fragen des Datenschutzes großzügig hinweg zu setzen, aber es geht zunächst einmal darum, derartige mögliche Zielkonflikte überhaupt in den Blick zu nehmen und einen

Kontext zu schaffen, in denen damit verantwortbar umgegangen werden kann. Es ist insofern naheliegend zu fragen, wie die Infrastruktur gestaltet werden muss, damit es möglich wird, Abwägungen bezüglich des adäquaten Schutzes von Rechten überhaupt vornehmen zu können. Auf dieser Ebene der Infrastrukturverantwortung stellt sich dann die Frage, welches Risiko auf Rechteverletzungen mit der Gestaltung kritischer Infrastrukturen verbunden ist.

Für eine Diskussion der Infrastrukturverantwortung auf der Basis einer Rechte-basierten Konzeption ist ein Bezug auf Risiken im Allgemeinen unvermeidlich, da mit der Einrichtung einer Infrastruktur vielfältige, in der Regel unübersichtliche und ambivalente Konsequenzen verbunden sind. Das macht es erforderlich, Abwägungen unter Bedingungen von Risiko und Unsicherheit vorzunehmen. In den entsprechenden ethischen Debatten waren in den letzten Jahrzehnten konsequentialistische Theorien dominanter als Rechte-orientierte Theorien, von denen häufig unterstellt wurde, dass sie bei Abwägungen unter derartigen Bedingungen scheitern würden. In den letzten Jahren wurden im Kontext der Klimaethik explizit Rechte basierte Risiko-Ethiken entwickelt, deren Begrifflichkeit man auch in anderen Kontexten anwenden könnte (siehe Steigleder 2016 und Meyer u.a. 2018). Dabei wurde herausgearbeitet, dass es beim Schutz von Rechten nicht immer um ein einfaches binäres Konzept gehen muss, dass Handlungen unter der Perspektive beurteilt, ob eine Handlung Rechte schützt oder verletzt. Vielmehr ist es aus einer Rechte-basierten Konzeption naheliegender Handlungsoptionen graduell daraufhin zu beurteilen, mit welchem Risiko ihre Realisierung verbunden ist, Rechte zu verletzen. Im Rahmen der Klimaethik scheint mir deutlich zu sein, dass das Konzept eines »rights-violating potential« geradezu eine Bedingung dafür ist, dass Rechte geschützt werden können, insofern es beim Klimawandel stets um Bedingungen von Risiko und Unsicherheit geht.

Dies scheint mir auch der Fall zu sein, wenn es um die Verantwortung für die Dateninfrastruktur geht. Es wird in diesem Kontext also darum gehen, welche Rechte an eigenen Daten und Datenspenderechte bei der Gestaltung der Dateninfrastruktur spielen können und sollen. Doch gegenüber der Frage der konkreten Regulierungen ist die Frage nach der Regulierbarkeit vorgängig (vgl. Düwell 2017). Wenn man davon ausgehen muss, dass die Etablierung von Datensystemen für den Schutz von Rechten relevant ist, aber zugleich das Rechte-verletzende Potential nicht oder nur begrenzt abschätzen kann, so ist es im Lichte einer Rechte-basierten Ethik primär geboten,

eine Infrastruktur so zu gestalten, dass die Möglichkeit einer Regulierung und der Revision einer Regulierung überhaupt gegeben ist.

4. Wege zu Datenzugangsregeln

Die bisherigen Überlegungen zielten zunächst darauf ab, die Verschränkung von Individualrechten mit kollektiven Interessen und Schutzdimensionen aufzuzeigen. Aus einer normativen Theorie, die vom Schutz von Individualrechten ihren Ausgangspunkt nimmt, ist der Schutz jener Voraussetzungen normativ verpflichtend, die für einen (langfristigen) Schutz und eine Wahrnehmung von Rechten vorausgesetzt werden müssen. Die kollektive, gesellschaftliche Dimension ist den Rechten gewissermaßen nicht äußerlich, es geht vielmehr um eine Abwägung zwischen Aspekten, die einem System von Rechten eigen sind. Ferner sollte deutlich geworden sein, dass sich eine Rechte-basierte Konzeption nicht darin erschöpfen kann, Daten als Eigentum zu betrachten. Das sind bislang jedoch allein negative Bestimmungen. Im Folgenden will ich versuchen, einige positive Konsequenzen aus dem bisher Gesagten zu skizzieren.

Wie angedeutet wäre es auf Basis einer Rechte-basierten Konzeption vordringlich, infrastrukturelle Bedingungen zu etablieren, die eine Kontrolle des Umgangs mit Daten in der Form ermöglichen, dass der Effekt auf Rechte überhaupt nachvollziehbar und beeinflussbar ist. Dies ist notwendig für die Möglichkeit, dass Bürger effektiv ihre Rechte auf politische Entscheidungen zum Umgang mit den Daten wahrnehmen können. Das ist ferner notwendig, um gegebenenfalls Rechtsschutz realisieren zu können, wenn die Existenz und Publizität dieser Daten vitale Interessen von Bürgern betreffen. Diese Infrastrukturverantwortung impliziert, dass die technische Erfassung der Daten und die Eigentumsverhältnisse eine derartige Kontrolle überhaupt zulassen. Dies hat etwa Konsequenzen für die Frage, wer denn überhaupt Besitzer der entsprechenden Infrastruktur ist. Da Bürger in der Regel nicht selbst in der Lage sind, individuellen Rechtsschutz zu realisieren, sind Institutionen erforderlich, die zur Wahrnehmung eines Schutzes der Rechte befähigt sind. Insofern digitale Infrastrukturen international organisiert sind, bzw. auf technischen Voraussetzungen mit internationalen Besitzverhältnissen beruhen, wäre es normativ wichtig, Kontrollmöglichkeiten in internationaler Zusammenarbeit zu realisieren.

Ich hatte bereits angedeutet, dass bei der Bestimmung von legitimen Zielen von Datensammlungen der Schutz jener Bedingungen von normativ wesentlicher Bedeutung ist, die für die Handlungs- und Lebensmöglichkeiten von Menschen wesentlich sind, Beispiele waren hier Gesundheits- und Nachhaltigkeitsbezogene Forschungen. Die Logik war hier: man kann nicht von der normativen Verbindlichkeit von Individualrechten ausgehen, ohne die Bedingungen zu sichern und zu fördern, die erforderlich sind, dass Menschen diese Rechte langfristig wahrnehmen können. Diese Bemerkung verdient verschiedene Qualifizierungen. Zunächst ist es in einer freiheitlichen Gesellschaft auch ohne diese Zielsetzung legitim Forschungen zu betreiben, bei denen Daten erhoben und versammelt werden. Das soll hier auch nicht in Frage gestellt werden. Doch stellt sich im Falle einer Abwägung der Rechte-relevanten Gesichtspunkte der normative Konflikt anders dar als im Falle von Forschungen, deren Legitimation mit der langfristigen Sicherung von Rechten zu tun hat. Im letzteren Fall kann der Schutz individueller Daten jedenfalls nicht so weit ins Feld geführt werden, dass die Forschung unmöglich gemacht wird, denn es stehen gewissermaßen Rechte auf beiden Seiten der Abwägung. Natürlich steht man hier vor dem Problem, dass ein beträchtlicher Teil heutiger Forschung sich rhetorisch auf Nachhaltigkeit und Gesundheit als langfristiges Ziel beruft und es kann nicht darum gehen, nur anwendungsnahe Forschung durch langfristigen Schutz von Rechten legitimiert zu sehen. Vielmehr muss Forschung sich von der inneren Logik her entwickeln können. Das kann im Rahmen einer Rechte-basierten Konzeption kein legitimer Grund sein, Datenschutz völlig auszuhebeln. Aber die Schwierigkeit einzelne Forschung zum langfristigen Effekt auf einen Schutz der Rechte in ein rekonstruierbares Verhältnis zu setzen kann ebenso wie die Möglichkeit einer rein rhetorischen Behauptung eines solchen Verhältnisses, kein Argument sein, derartige Abwägungen von vorneherein auszuschließen. Aber prinzipiell scheint mir die Möglichkeit derartiger Konflikte ein zentrales Argument für eine Möglichkeit reflektierten regulatorischen Umgangs mit den Sammlungen von Daten zu sein. Das wäre im Bereich der Forschung etwa auch ein Argument gegen unbegrenzte Open Science Policies, bei der nicht nur Auswertungen von Daten, sondern auch Datensammlungen selbst standardmäßig öffentlich zugänglich gemacht werden.

Neben diesen generischen Überlegungen gibt es natürlich für einen Rechte-basierten Ansatz ganz wesentlich die Ebene der Begrenzung des Umgangs mit den Daten des Individuums, also die Ebene, bei der ein

Individuum durch die Publizität von und den Umgang mit Daten seine Interessen berührt sieht. Das ist jene Ebene, an die man zunächst denkt, wenn von Individualrechten im Kontext des Umgangs mit Daten die Rede ist. Und letztlich geht es natürlich auch um den Schutz dieser Individualrechte. Es gibt Daten, die zu sammeln und gegebenenfalls publik zu machen, Aspekte fundamentaler Rechte von Individuen berühren, die nicht ohne Autorisierung der Betroffenen gesammelt und publiziert werden dürfen. Dies gilt umso mehr, je mehr die Daten einen Kernbereich von Interessen berühren, je mehr Privatsphäre berührt ist etc. Und in der Tat muss es hier einen Kern »des Privaten« geben, der geschützt ist und dessen Schutz auch nicht Gegenstand von Abwägungen sein kann.

Fraglich ist jedoch, in welcher Weise man diesen Schutz gestalten kann. Konzipiert man diese Daten als Eigentum, so konzentriert sich die Regulierungsfrage auf den Umgang mit dem Eigentum, also den Schutz der Rechte des Eigentümers. Nun kann man prinzipiell fragen, ob es aus dem Konzept des Eigentums heraus überhaupt plausibel ist, Daten als Eigentum zu verstehen. Zumindest wird dabei ignoriert, dass Daten hergestellt werden und sowohl die Bedingungen der Herstellung als auch die Verantwortung des Herstellenden geraten durch den Fokus auf Eigentum aus dem Blick.

Gerade wenn der Kernbereich des Privaten und der Interessen des Individuums von so großer Bedeutung ist und ein so wesentliches Schutzgut darstellt, wird die Frage nach dem effektiven Schutz von zentraler Bedeutung. Die erste Konsequenz müsste dann doch sein, die Frage zu stellen, wie die Produktion von Daten so gestaltet werden kann, dass die Wahrscheinlichkeit, dass dieser Kernbereich berührt ist, minimiert ist. Das würde etwa bedeuten, dass die Produktion personenbezogener Daten nur dann erfolgt, wenn es für die Datenerhebung unvermeidlich ist, und die Möglichkeit der Rückverfolgung auf Personen eher erschwert wird. Es ist deutlich, dass mit diesen kursorischen Bemerkungen die Thematik erschöpft ist, aber die Überlegungen zielen primär darauf ab zu betonen, dass aus den Eigenschaften von Daten und der Möglichkeiten des Schutzes von durch Daten betroffene Rechte es naheliegend ist, eher generische Regelungen zu suchen, die primär bei der Datenproduktion ansetzten statt von Individuen eine aktive Schutzaktivität zu erwarten, die effektiv nur vor dem Hintergrund umfangreicherer Kenntnisse wahrgenommen werden kann.

Von anderer Art ist dann die Dimension, die ich weiter oben »Datenspenderechte« genannt habe, also Rechte, die nicht darum ein Recht darstellen, weil ein zentrales Interesse des Datenspenders betroffen sind, sondern nur

weil die Daten von dieser Person stammen. Nun ist nicht von vorneherein deutlich, wann die Grenze, an der es um Interessen einer Person geht, genau erreicht ist. Es könnte hier auch unterschiedliche Interessen geben, weshalb nicht davon ausgegangen werden kann, dass diese Grenzziehung unstrittig ist. Aber die Diskussion sollte sich dann auf die Frage dieser Grenzziehung richten, während die bloße Tatsache, dass Daten in irgendeinem Sinne zu mir zurückverfolgt werden können, noch nicht eo ipso Rechtsansprüche begründet. Solche Rechte müssten in einem qualifizierten Sinne eine Verbindung zu Handlungsmöglichkeiten von Individuen aufweisen. Zu betonen wäre aber auch, dass, sollte man zum Ergebnis kommen, dass die Bereitstellung von Daten an sich noch keine Rechte des Datenspenders berührt, damit keine Annahmen begründet werden, dass es Pflichten zur Datenspende gäbe.

Ich habe keine konkreten Regelungen, sondern lediglich die grundlegenden Überlegungen skizziert, die für eine nähere Bestimmung von Datenzugangsregeln wichtig sind. Dabei bin ich noch nicht auf die Ebene konkreter Regelungen gekommen. Auch habe ich nicht konkrete Akteure bestimmt und zwischen einer moralischen, rechtlichen und politischen Betrachtung von Rechten nur im Ansatz, aber noch nicht im Hinblick auf konkrete Regelungen und Zuständigkeiten unterschieden. Das hat mit der Komplexität des Themas zu tun, nicht weil ich diese Unterscheidungen nicht für wichtig halte, ganz im Gegenteil. Es scheint mir aber philosophisch problematisch zu sein, die Logik der Rechte zu verfolgen, ohne den Zusammenhang der verschiedenen normativen Dimensionen in den Blick zu nehmen. Wenn das Rechtssystem auf Individualrechte begründet wird, so ist es vordringlich zu verstehen, welcher Umgang mit diesen Rechten rational begründet und rekonstruiert werden kann. Damit habe ich versucht eine Reihe von Zusammenhängen zu rekonstruieren, die von Regulierungen nicht ignoriert werden können. Von der Kritik an einer Rechte-basierten Regulierung würde ich dann auch erwarten, dass sie den systematischen Zusammenhang dieser Überlegungen angreift. Jedenfalls müsste eine Kritik des Rechte-basierten Ansatzes mehr zeigen, als dass eine Eigentumsauffassung von Datenrechten zu kurz greift, denn das kann man aus der Perspektive der Individualrechte selbst einsehen und intern korrigieren.

Literatur

Beitz, Charles (2009): *The Idea of Human Rights*, Oxford.

Beyleveld, Deryck (1991): *The Dialectical Necessity of Morality: An Analysis and Defense of Alan Gewirth's Argument to the Principle of Generic Consistency*, Chicago.

Brett, Annabel (1997): *Liberty, Right and Nature. Individual Rights in Later Scholastic Thought*, Cambridge.

Claassen, Rutger/Düwell, Marcus (2013): The Foundation of Capability Theory: Comparing Nussbaum and Gewirth, in: *Ethical Theory and Moral Practice* 16, Heft 3, S. 493–510.

Düwell, Marcus (2014): Human Dignity: Concept, Discussions, Philosophical Perspectives, in: Düwell, Marcus/Braarvig, Jens/Brownsword, Roger/Mieth, Dietmar (Hg.): *Cambridge Handbook on Human Dignity*, Cambridge, S. 23–49.

Düwell, Marcus (2017): Human Dignity and the Ethics and Regulation of Technology, in: Brownsword, Roger/Scotford, Eloise/Yeung, Karen (Hg.): *The Oxford Handbook of Law, Regulation, and Technology*, Oxford, S. 177–196.

Düwell, Marcus (2020): Menschenwürde und menschliches Selbstverständnis, in: Neumann, Ulfried/ Tiedemann,Paul/ Liu, Shing-I (Hg): *Menschenwürde ohne Metaphysik*, Archiv für Rechts- und Sozialphilosophie, Beiheft Band 165, Stuttgart, S. 9–22.

Düwell, Marcus (2022): Kantian Human Dignity and a »Community of Rights«, in: van der Rijt, Jan-Willem/Cureton, Adam (Hg.): *Human Dignity and the Kingdom of Ends: Kantian Perspectives and Practical Applications*, London/New York, S. 90–205.

Düwell, Marcus/Bos, Gerhard (2018): Why ›rights‹ of Future People?, in: Düwell, Marcus/Bos, Gerhard/Van Steenbergen, Naomi (Hg.): *Towards the Ethics of a Green Future. The Theory and Practice of Human Rights for Future People*, Abingdon, Oxon/New York, S. 9–27.

Gewirth, Alan (1978): *Reason and Morality*, Chicago.

Gewirth, Alan (1996): *The Community of Rights*, Chicago.

Meyer, Lukas H./Schuppert, Fabian/Stelzer, Harald/Placani, Adriana (2018): Risk and Rights. How to Deal with Risks from a Rights-based Perspective, in: Düwell, Marcus/Bos, Gerhard/van Steenbergen, Naomi (Hg.): *Towards the Ethics of a Green Future. The Theory and Practice of Human Rights for Future People*, Abingdon, Oxon/New York, S. 28–46.

Moyn, Samuel (2010): *The Last Utopia: Human Rights in History*, Cambridge/Massachusetts.

Jellinek, Georg (1919): *Die Erklärung der Menschen- und Bürgerrechte*, München/Leipzig.

Menke, Christoph (2015): *Kritik der Rechte*, Frankfurt am Main.

Steigleder, Klaus (1999): *Grundlegung der normativen Ethik: Der Ansatz von Alan Gewirth*, Freiburg im Breisgau.

Steigleder, Klaus (2016): Climate risks, climate economics, and the foundations of a rights-based risk ethics, in: *Journal of Human Rights* 15, Heft 2, S. 251–271.

Tierney, Brian (2014): *Liberty & Law. The idea of permissive natural law 1100–1800*, Washington.

Tuck, Richard (1979): *Natural Rights Theories: Their Origin and Development*, Cambridge.

Waldron, Jeremey (1999): *Law and Disagreement*, Oxford.

Die Datensubjekte in den Datenzugangsregulierungen

Jasmin Brieske und Doris Schweitzer

Einleitung

Welche Effekte die »Datafizierung des Sozialen«[1] auf das Subjekt zeitigt, ist umstritten. Wiederkehrendes Thema sind Spannungsverhältnisse zwischen Autonomie und Kontrolle bzw. Empowerment und Unterwerfung.[2] Das wird in der Soziologie insbesondere mit Blick auf die Techniken und Praktiken des Self-Trackings respektive des »Lifeloggings«[3] diskutiert: Die einen erkennen darin verbesserte Möglichkeiten eines Wissens über das Selbst, was eine gesteigerte Selbstbestimmung bewirke[4] – ein Wissen »by numbers«, wie es in der Quantified Self-Bewegung im positiven Sinne propagiert wird.[5] Andere wiederum warnen vor solchen technikoptimistischen und fortschrittsgläubigen Stimmen, handele es sich beim Lifelogging doch vielmehr um eine Form der »digitalen Selbstüberwachung«[6], mittels derer sich das Selbst dem Imperativ der ständigen Selbstoptimierung qua Selbstkontrolle aussetze.[7]

---

1 Wenn nicht gar schon von der »Datengesellschaft« gesprochen wird, Houben/Prietl 2018.

2 Vgl. Paulitz 2005 sowie die Beiträge in Houben/Prietl 2018.

3 Selke 2014. Repräsentativen Studien für Deutschland zufolge betreiben ca. 35 % der erwachsenen Bevölkerung zwischen 20 und 50 Jahren Self-Tracking, Findeis u.a. 2023.

4 Vgl. bspw. Zillien/Fröhlich 2018.

5 Vgl. Lupton 2016.

6 Schaupp 2016.

7 Vgl. Duttweiler/Passoth 2016. Aus solchen Befunden werden gesellschaftstheoretische und -diagnostische Rückschlüsse gezogen: So repräsentiert das Self-Tracking bei Andreas Reckwitz in der Beschreibung der gegenwärtigen *Gesellschaft der Singularitäten* (2020) paradigmatisch die Gleichzeitigkeit aus Vergesellschaftung und Singularisierung. Steffen Mau erkennt in seinem Buch *Das metrische Wir* (2017) aufgrund der über Profile zunehmend identifizierten Subjekte einerseits eine Hyperindividualisierung. Diese gehe jedoch Hand in Hand mit einem Wandel hin zu einer Bewertungsgesellschaft, in der das Subjekt qua datengestützter Identifikation immer nur vor dem

In welcher Form hier das Subjekt angesprochen wird – wie es zum Subjekt gemacht wird – steht zentral zur Debatte.[8] So wird in der Foucault'schen Tradition in den Techniken und Praktiken des Lifeloggings eine Zuspitzung der in unserer Gesellschaft hegemonialen Subjektivierungsform des »unternehmerischen Selbst« gesehen:[9] Das Subjekt wird primär als Unternehmen im ökonomischen Sinne angerufen. Dem entspricht auf der Ebene der Selbsttechnologien ein Konzept des auf Selbstoptimierung gerichteten Managements der eigenen Person: »Sich selbst zu managen, verlangt nicht nur die gleichen Tugenden wie die Führung eines Unternehmens, sondern besteht vor allem in der Fähigkeit, sich selbst als Unternehmen zu begreifen und entsprechend zu führen.«[10] Man wird in allen Lebensbereichen – auch und vor allem jenseits der Ökonomie im klassischen Sinne – zum »Unternehmer seiner Selbst«. Diese spezifische Form der Selbstregierung wird dabei im Einklang mit gesellschaftlichen Steuerungsmodellen gesehen, insbesondere solchen des Neoliberalismus.[11]

Demgegenüber erscheint in Ansätzen, die den Fokus auf die Eigenheiten der Datafizierung legen,[12] das Subjekt nicht primär einer zunehmenden Selbstkontrolle und -überwachung ausgesetzt, sondern vielmehr einer forcierten Fremdkontrolle und -überwachung. In der der Datafizierung eigentümlichen Logik wird der Einzelne – so den Annahmen Deleuze folgend[13] – nicht als Individuum, als unteilbare Einheit, sondern als »Dividuum« adressiert: Im Datenraum habe das Subjekt keinen einheitlichen Körper mehr, sondern ein Profil, das aus einer beständigen Rekombination von immer öfter im präsentischen Modus geteilten Daten und Teilungen von Datensätzen hervorgeht, d.h. aus »riesige[n] Akkumulationen von Daten, die auf unendliche Arten geteilt, wieder zusammen- und inwertgesetzt werden können«[14]. Dies folge der Logik eines konstanten Flusses, in dem Zustände einem ständigen Wandel unterworfen sind. Dabei gelte es, diesen Fluss zu kontrollieren, und die Kontrolle setze dabei an »Fragmente[n] des Individuums [an],

---

Hintergrund eines metrisch verfassten »Wir« erscheine – letztlich also eine neue Form der Soziometrie respektive des *social engeneerings*.

8 Vgl. Bettinger 2022.

9 Bröckling 2007; Gertenbach/Mönkeberg 2016; Duttweiler u.a. 2016.

10 Bröckling 2000, S. 154.

11 Vgl. Catlaw/Sandberg 2018; Bröckling 2000, 2007; Rose 1996.

12 Vgl. Seyfert/Roberge 2017.

13 Vgl. Deleuze 1993, S. 258.

14 Raunig 2015, S. 159; vgl. auch Ott 2015; Hörtnagl 2019.

die sich im ständigen Fluss der Modulation kontinuierlich bilden und verändern. Sie bilden einzelne Eigenschaften ab, die im jeweiligen Kontext stellvertretend für die Person stehen und auf die sich bestimmte Operationen anwenden lassen.«[15] Mit Jennifer Whitson gesprochen gilt: »Instead of individuals – irreducible and with an autonomous sense of agency – the new subject of governance is instead the dividual, an artifact of data mining searches and computer profiles.«[16] Die dividuelle Anrufung des Einzelnen erscheint hier als eine Machttechnik, die quasi von außen als Fremdanrufung auf das Subjekt einwirkt. Wer dabei die Kontrolle über die dividuellen Praktiken hat, wer den Fluss der Daten kontrolliert, kann somit die Subjekte kontrollieren. Das Problem wird also weniger in der forcierten Selbstkontrolle verortet, sondern in den dividuellen Techniken und Praktiken einer forcierten Fremdkontrolle.

Gemein ist all diesen soziologischen und sozialwissenschaftlichen Beiträgen, dass das Recht in seiner konkreten Gestalt und Entwicklung für die Beantwortung der Frage nach den Subjekten in der »Datengesellschaft« eine sehr geringe bis gar keine Rolle spielt – und dies, obwohl hier angesichts der angesprochenen Problemlagen um eine staatliche Regulierung gerungen wird. Hier setzt der Beitrag an, indem drei auf Fragen des Datenzugangs und der Datenverfügbarkeit gerichtete Unionsrechtsakte, namentlich der Data Governance Act (DGA)[17], der Data Act (DA)[18] und die Datenschutzgrundverordnung (DSGVO)[19], auf die ihnen zugrundeliegenden Subjektivierungsweisen hin untersucht werden. Jenseits rechtsdogmatischer Überlegungen und Bestimmungen soll in der Analyse der Rechtsakte der Frage nachgegangen werden, wer auf welche Art und Weise, d.h. wie, als Subjekt adressiert wird und wie dieses Subjekt sich selbst in den entsprechenden Handlungsoptionen konstituiert. Die Adressierung eines Subjekts als Individuum oder als Dividuum stellen dann unterschiedliche Subjektivierungsweisen dar, welche in verschiedenen Handlungsoptionen ihren Ausdruck finden.

Dabei kann man zunächst feststellen: In den Datenregulierungen wimmelt es nur so von Akteur:innen: Es gibt selbstverständlich »natürliche« und »juristische« Personen, aber auch »betroffene« Personen, Dateninhaber,

15 Hörtnagl 2019, S. 142.
16 Whitson 2015, S. 343.
17 Europäische Kommission (2022).
18 Europäische Kommission (2023)
19 Europäische Kommission (2016).

Nutzer, Datenvermittlungs- und Verarbeitungsdienste, Datenaltruismus-Dienste etc. pp. Angesichts dieser Tatsache stellt sich die Frage, ob man immer von demselben Datensubjekt ausgehen kann. Das soll mit Blick auf die Frage, wie der einzelne Mensch jeweils adressiert wird, untersucht werden. Dabei zeigt die Analyse – so die hier darzustellende These – dass in den genannten Rechtsakten der Mensch nicht nur als individuelles Subjekt adressiert wird, das sich in einem Spannungsverhältnis zwischen Selbstermächtigung und Kontrolle befindet, sondern ebenso als ein »dividuelles« Subjekt, welchem als teilbarer »Datenschatz« eine Infrastruktur- und Gemeinwohlverantwortung zugeschrieben wird.

Um diese These darzulegen, wird in drei Schritten vorgegangen: Zunächst wird die analytische Heuristik der Untersuchung der Subjektivierungsweise dargelegt (I.). In einem zweiten Schritt werden aus dieser Perspektive die einzelnen Rechtsakte auf die in ihnen erkennbaren Subjektivierungsweisen hin analysiert (II.). Daraus werden abschließend Schlussfolgerungen für die Frage gezogen, ob in diesen Regulierungen gegenüber den soziologischen Annahmen einer forcierten Fremdkontrolle über die Anrufung als dividuelles Subjekt Verschiebungen zu erkennen sind (III.).

I. Analytische Heuristik

1. Subjektivierungsweise

Die offene Frage nach den Datensubjekten in den Datenzugangsregulierungen setzt voraus, dass man nicht vorab weiß, von welchem Subjekt wir eigentlich jeweils sprechen.[20] Dies entspricht den Prämissen der soziologischen Analyseperspektive der Subjektivierungstheorie, wie sie sich unter Berufung auf Autorinnen und Autoren wie Judith Butler, Louis Althusser, Jacques Rancière, aber vor allem mit Bezug auf das Spätwerk von Michel Foucault in der Soziologie herausgebildet hat. Ausgangspunkt ist eine konsequent deontologische Perspektive: In Absetzung von einem

20 Vgl. zum Folgenden auch Schweitzer 2017, Schweitzer 2018. Anders als bei Thomas Vesting 2021 zielt unsere Analyse nicht darauf ab, einen Idealtypus der Datenzugangsregulierung herauszuarbeiten, sondern Verschiebungen in der Art und Weise der Anrufung des Subjekts in den verschiedenen Rechtsakten aufzuzeigen.

philosophischen Verständnis des autonomen Subjekts als einer ahistorischen Figur oder anthropologischen Konstante werden die historischen Konstitutionsbedingungen von Subjektivität betrachtet.[21] Das Subjekt der Subjektivierung existiert nicht a priori, sondern erscheint als radikal historisiertes Produkt. Daher kann es weder zum erkenntnistheoretischen noch im Bereich des Rechts zum normativen Ausgangspunkt gemacht werden, sondern wird zum Gegenstand der Untersuchung. Die Beschreibung dessen, was ein Subjekt ist, ab wann man von einem Subjekt sprechen kann, ja wie der einzelne Mensch zu einem Subjekt gemacht wird, ist dann erst das Ergebnis der Analyse.

In der Untersuchung der jeweiligen Subjektivierungsweisen und den dadurch konstituierten Subjektpositionen werden die Anrufungen (Althusser) und Adressierungen der einzelnen Menschen als Subjekte in den Blick genommen, aber auch die spezifischen Praktiken und Techniken, mittels derer auf das Subjekt Bezug genommen wird. Dies umfasst nicht nur den Fremdbezug, d.h. den Zugriff auf das oder die Unterwerfung des Subjekts, sondern zugleich den Selbstbezug des Subjekts, in dem es sich als agierende, selbstbestimmte Instanz in seiner Freiheit der Selbstgestaltung konstituiert: »Das Wort ›Subjekt‹ hat zwei Bedeutungen: Es bezeichnet das Subjekt, das der Herrschaft eines anderen unterworfen ist und in seiner Abhängigkeit steht; und es bezeichnet das Subjekt, das durch Bewusstsein und Selbsterkenntnis an seine eigene Identität gebunden ist.«[22] Autonomie und Heteronomie bedingen einander,[23] gesellschaftliche Zurichtung und Selbstmodellierung gehen in eins, was letztlich bedeutet, dass Subjektivierung und Machtpraktiken aneinandergekoppelt sind.[24]

In dieser Verschränkung von Wirkung und Voraussetzung der Machtinterventionen ist das Subjekt der Subjektivierung nur performativ denkbar: »Eine Entität, die sich performativ erzeugt, deren Performanzen jedoch eingebunden sind in Ordnungen des Wissens, in Kräftespiele und Herrschaftsverhältnisse.«[25] Dieses performative Subjekt existiert daher, wie

21 Vgl. Saar 2013, S. 17.

22 Foucault 2005a, S. 275.

23 Vgl. Butler 2005; mit Blick die Verwobenheit von Autonomie und Heteronomie hinsichtlich des Subjekts des Rechts argumentiert Ino Augsberg ähnlich, wobei er jedoch den Übergang zum dividuellen Verständnis des Subjekts primär auf der sprachphilosophisch-erkenntnistheoretischen Ebene ansetzt, Augsberg/Keller/Lindner 2023.

24 Vgl. Lemke 1997, S. 291 ff.

25 Bröckling 2007, S. 21.

Ulrich Bröckling schreibt, »nur im Gerundivum: als zu erkundendes, zu produzierendes, zu optimierendes, zu normalisierendes usw. Es ist der Fluchtpunkt der Definitions- und Steuerungsanstrengungen, die auf es einwirken und mit denen es auf sich selbst einwirkt. Kein Produkt, sondern Produktionsverhältnis.«[26] Im Zentrum steht die gesellschaftliche Konfiguration von Subjekten im Zusammenwirken von Fremd- und Selbstformierung, die sich insbesondere in der Verschränkung und Wechselwirkung von Fremd- und Selbstanrufung soziologisch analysieren lässt.

Man bezieht sich also nicht auf eine Theorie des Subjekts, sondern analysiert die verschiedenen Arten und Weisen des Fremd- und Selbstbezugs, durch die der einzelne Mensch dazu gelangt, sich selbst als Subjekt zu konstituieren.[27] Um dabei Differenzen ausmachen zu können, wird der Assemblage-Gedanke herangezogen, der eng mit dem Gedanken der Performativität zusammenhängt: Das Subjekt wird nicht als homogene Einheit, sondern als ein je historisch-spezifischer Kreuzungspunkt, eine Verknüpfung bzw. ein Gefüge heterogener Elemente begriffen.[28] An dieser Stelle kommt auch die Unterscheidung von Individuum und Dividuum zum Tragen: Gerade weil das Subjekt nicht a priori als Einheit begriffen wird, erscheint es möglich, es sowohl als Individuum, d.h. als unteilbare Einheit, als auch als Dividuum anzurufen – und zwar sowohl im Fremd- als auch im Selbstbezug.

Fragt man diesen methodologischen Prämissen folgend nach der Subjektivierungsweise in den verschiedenen rechtlichen Regulierungen, so sind angesichts des Materials insbesondere zwei mögliche Formen der »Anrufung des Subjekts« zu unterscheiden: einerseits mit Blick auf »subjektive Rechte« (2.), andererseits im Bezug auf das jeweils problematisierte Subjektverhältnis angesichts des regulierten Sachverhaltes (3.).

2. Subjektanrufung in Form des »subjektiven Rechts«

Im ersten Fall, wenn man also die verhandelten »subjektiven Rechte« fokussiert, wird man auf die klassisch liberale Subjektivierungsform verwiesen.[29]

---

26 Bröckling 2002, S. 6.

27 Vgl. Foucault 2009, S. 18.

28 Vgl. Serres 1998, S. 418; Deleuze/Guattari 1992, S. 18, 59 ff.

29 Siehe hierzu den Beitrag von Düwell in diesem Band. Dass man Rechte jedoch nicht zwangsläufig an ein Subjekt binden muss, zeigen gerade angesichts der Problemlagen des Datenzugangs die Überlegungen von Steffen Augsberg zum inpersonalen Recht in diesem Band.

Besonders deutlich wird dies in der DGSVO, in der dem »Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten« der Status eines »Grundrechts« zugesprochen wird (Erw.Gr. 1 DSGVO). Das Subjekt der subjektiven Rechte wird hier also als eine »natürliche Person« angerufen, der aufgrund dieser Tatsache spezifische Rechte zukommen.

Unabhängig von der Frage, ob man diese »natürliche Person« als Naturalisierung oder Konstruktion bzw. als »Realfiktion« oder »Adresse« versteht,[30] wird hier auf einen individuellen Einzelmenschen, ausgestattet mit einem Körper und einem Willen, verwiesen. Dieses Subjekt muss als solches identifizierbar sein und mit einer eigenen Identität angerufen werden können. Das zeigt sich etwa in Art. 4 Nr. 1 DSGVO, der den Ausdruck »personenbezogene Daten« definiert als

> »alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden »betroffene Person«) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.«

Das identifizierbare körperliche Subjekt fungiert als ein Zurechnungspunkt, dem Rechte, Pflichten und über die Willensbetätigung Handlungen zugeschrieben werden können.[31] Um diese Zuschreibungsleistung erbringen zu können, muss dieses Subjekt des subjektiven Rechts zudem dem Recht vorgängig erscheinen (worin auch seine rechtshistorische Bedeutung liegt[32]).

Diese Eigenschaften verweisen auf die klassisch liberale Subjektivierungsform. Die Person des Rechts wird als das liberale Subjekt der subjektiven Rechte gedacht, mit qua Geburt (d.h. dem Recht vorgängigen und nicht per Gesetz) zugeteilten Freiheitsrechten, die im Willen ihren Ausdruck

---

30 Siehe zur »Naturalisierung« Menke 2015; zur »Konstruktion« Kelsen 1960, S. 178; zur »Realfiktion« Hutter/Teubner 1994; zur »Adresse« Fuchs 1997. Letztlich ist es für die Frage, ob das Subjekt als Individuum oder als Dividuum adressiert wird, unerheblich, ob es sich dabei um eine solche (Real-)Fiktion oder Konstruktion handelt, die immer nur Teilaspekte umfasst. Es wird eben nicht in den Blick genommen, ob die Einheit als solche adäquat erfasst wird, sondern wie sie statuiert wird. Denn auch nur durch Teilinformationen oder Fiktionen etc. gewonnene Adressen können als einheitlicher Zurechnungspunkt dienen, in dem das Subjekt als Einheit, d.h. als Individuum, adressiert wird.

31 Vgl. Menke 2015.

32 Vgl. Menke 2008, 2015; Luhmann 1981.

finden und über Ansprüche – wie im Falle der DSGVO etwa über Löschungs- oder Berichtigungsansprüche etc. – geltend gemacht werden. Diese Freiheitsrechte sind ihrer Konzeption nach auch unteilbar, sie kommen einem Menschen qua Menschsein zu. Insofern wird dieser hier als Individuum angerufen: Als individuelles Subjekt, das mit einem Körper und einer Identität ausgestattet ist, und dem dann Rechte zugesprochen werden können, die es geltend machen kann.

3. Anrufung über das problematisierte Subjektverhältnis

Die Fokussierung auf das subjektive Recht verstellt jedoch den Blick auf die zweite Form der Anrufung des Subjekts, wie sie in den Regulierungen erkennbar sind: die Anrufungen über spezifische Subjektverhältnisse. Denn zum einen werden die subjektiven Rechte in ganz spezifische Problemkonstellationen eingeschrieben, d.h. es werden ganz spezifische Subjektverhältnisse in den Gesetzen reguliert. Mithin kann man sagen: DSGVO, DGA und DA stellen jeweils unterschiedliche »Problematisierungsweisen«[33] solcher Subjektverhältnisse dar. Damit geht es um die Formierung eines Problems als solches. Denn etwas als Problem- oder Notlage zu formulieren, das – wie in den vorliegenden Fällen – einer gesetzlichen Regulierung bedarf, ist selbst eine spezifische Art des Umgangs mit einer konkreten Situation bzw. eine strategische Intervention in ein dynamisches Feld gesellschaftlicher Auseinandersetzungen. DSGVO, DA und DGA werden mithin als spezifische Ausformungen des Problems des Zugangs zu und des Umgangs mit Daten angesehen – man könnte dies ja jeweils auch ganz anders problematisieren und damit angehen. Dabei wird das Subjekt angerufen, indem bestimmte Subjektverhältnisse als regelungsbedürftig adressiert werden und über den Bezug auf das Subjekt hierfür eine Lösung gefunden werden soll. Um ein kurzes Beispiel hierfür vorwegzunehmen: So antwortet die DSGVO auf eine spezifische Problemlage im Subjektverhältnis. Es ist dies die Differenz von »natürlicher Person« und digital erzeugtem Bild dieser Person, sozusagen eine Konfrontation des Selbstbildes des Individuums mit einem digital erzeugten Fremdbild, das in der Identitätskonstruktion einer dividuellen

33 Vgl. Foucault 2005b, S. 733; Foucault 2005c. Zur Debatte steht damit, »[w]ie und warum bestimmte Dinge (Verhalten, Erscheinungen, Prozesse) zum *Problem* wurden«, Foucault 1996, S. 178, H.i.O.

Logik folgt.[34] Man könnte das Ganze aber auch als Problem framen, dass auf der Ebene der Ersteller:innen von solchen Profilen angesiedelt ist oder auf der Ebene der technischen Infrastruktur. Dann würde man an diesen Punkt zur Regulierung ansetzen – so etwa dadurch, dass Daten mit einem Verfallsdatum versehen werden.[35]

Die Frage, welche Subjektverhältnisse hier wie zur Lösung eines Problems adressiert werden, hängt also eng mit dem eigentlichen Gegenstandsbereich und der Zielsetzung der jeweiligen Verordnungen zusammen. Innerhalb dieser Problemkontexte wird der einzelne Mensch nicht nur in der abstrakten Form des Subjekts der »subjektiven Rechte« angerufen. Vielmehr werden spezifische Subjektpositionen zugeschrieben. Der einzelne Mensch wird in den jeweiligen Regulierungen ganz spezifisch adressiert: als »Nutzer«, als »betroffene Person«, als altruistisches Subjekt usw. Die entsprechenden Handlungsoptionen sind im Lichte der jeweiligen Problemkontexte zu interpretieren.

Legt man diese Folie nun in der Analyse der Regulierungen an, so fragt man danach, welche Subjektverhältnisse mit Blick auf den einzelnen Menschen hier regelungsbedürftig erscheinen und wie in dieser Problemlage der einzelne Mensch als Subjekt adressiert wird – und zwar als Verschränkung von Fremdbezug (etwa Anrufung als Subjekt der subjektiven Rechte, Zuteilung von Positionen in der Regulierung) und Selbstbezug (Handlungsoptionen als Selbstanrufung).

II. Die Datensubjekte der DSGVO, DGA und DA

1. DSGVO

Die DSGVO ist einer der wichtigsten Instrumente der vergangenen Jahre für den Schutz von Daten »natürlicher Personen«. Die bereits seit dem 25. Mai 2018 anzuwendende Verordnung ist als Teil der Datenschutzstrategie der Europäischen Union auf den Schutz personenbezogener Daten

34 Vgl. hierzu auch die Rechtsprechung des EuGH zum subjektiven »Recht auf Vergessenwerden«, EuGH Urteil vom 13.5.2014 – C-131/12 – *Google Spain/AEPD*; erläuternd Schweitzer 2017.

35 Vgl. Mayer-Schönberger 2009.

gerichtet.[36] Mit der Anknüpfung an die Personenbezogenheit von Daten verbindet die DSGVO die abstrakten Informationen, die in technisch lesbarer und verwertbarer Weise einen maßgeblichen Bestandteil der Digitalsphäre bilden, mit natürlichen Personen, zu denen sie einen Bezug aufweisen.[37] Der DSGVO liegt dabei der Gedanke zugrunde, dass die natürliche Person im digitalen Raum Spuren hinterlässt und dadurch zur Existenz von Daten beiträgt, die einen Informationsgehalt über die natürliche Person besitzen.

Schon die Bezugnahme auf die »natürliche Person« zeigt in seiner konkreten Ausformung, dass hier die Person als Individuum adressiert wird. Denn das Recht auf Schutz personenbezogener Daten ist, wie die DSGVO mit Verweis auf Art. 8 Abs. 1 GRCh und Art. 16 Abs. 1 AEUV deutlich macht, ein Grundrecht (vgl. Art. 1 Abs. 2, Erw.Gr. 1 S. 2 DSGVO) – es folgt also eine Kopplung des Schutzgedankens an die Idee des subjektiven Rechts. Ausgegangen wird davon, dass die natürliche Person ein Interesse daran hat, welche Daten wie existieren und verarbeitet werden, und welche Informationen sich aus diesen über sie ableiten lassen.

Darüber hinaus zeigt sich die Adressierung des Subjekts als Individuum auch in der Ausgestaltung des Personenbezugs. Denn nur personenbezogene Daten besitzen nach dem Grundgedanken der DSGVO in Abgrenzung zu nicht-personenbezogenen Daten eine besondere Schutzwürdigkeit. Nur sie fallen in den Anwendungsbereich, da nur an diesen ein besonderes Schutzinteresse der natürlichen Person besteht. Allerdings ist die Grenze, wann etwas nicht mehr auf eine Person verweist (oder verweisen kann) schwierig zu ziehen.[38] Nach der DSGVO sind Daten nur personenbezogen, wenn sie zumindest die Identifizierbarkeit der dahinterstehenden natürlichen Person

36 Vgl. Europäische Kommission (2010). Dass auch die Diskussion um Daten, die keinen Personenbezug aufweisen, Teil der Debatte um Datenregulierung sein sollte, argumentiert Lambach in diesem Band.

37 Zum Begriff der Daten siehe beispielsweise Zech 2012, S. 24–33. In dieser Verbindung von Daten und der natürlichen Person klingt die Idee des »digitalen Zwillings« an, siehe hierzu den Beitrag von Gruber/Zihlmann in diesem Band.

38 Bomhard/Merkle 2022, S. 172 Rn. 27 ff.; Rücker/Dienst 2021, § 6 Rn. 127 ff. Im Ergebnis ist die Abgrenzung angesichts Big Data auch nicht unbedingt weiterführend. So merkt Steffen Augsberg zu Recht an: »Unter Big-Data-Bedingungen ist es erstens notwendig, sich von überholten Vorstellungen einer spezifischen, vorgegebenen Sensibilität bestimmter Daten und hierauf rekurrierender besonderer Schutzmechanismen zu lösen. Datenschutz kann nicht mehr statisch an bestimmten Daten und Datennutzungskategorien ansetzen, sondern muss sich auf ständige Rekombinationen und Rekontextualisierungen einstellen«, Augsberg 2022, S. 126.

ermöglichen (Art. 4 Nr. 1 DSGVO). Diese Rückbindung des Informationsgehaltes von Daten an die dadurch ermöglichte Identifizierbarkeit machen das Subjekt als Individuum zum zentralen Bezugsobjekt der DSGVO: Es geht um Personen, die *eine* Identität haben, auf die Rückschlüsse gezogen werden können. So ist – wie oben bereits erwähnt – gemäß Art. 4 Nr. 1 DSGVO eine natürliche Person identifizierbar, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann. Teilinformationen erlauben also Rückschlüsse auf diese eine Identität – und ohne diese Annahme der einen individuellen Identität wäre die Identifizierbarkeit auch gar nicht möglich. Denn die Identifizierung wird über die »Zuordnung« eines Datensatzes auf eine »natürliche Person« als Einheit hergestellt.[39] Insofern wird der Regelungsgegenstand als Problem der Herrschaft über die Bestimmung des Selbst, der eigenen Identität, ausgeformt.

Datensatz und natürliche Person werden also durch den Identifikationsakt verbunden.[40] Dabei folgt die Seite des Operierens mit Daten im Rahmen der Identifizierung, die Erstellung eines Profils, einer anderen Logik als die Annahme einer einheitlichen Identität: Die einzelnen Daten sprechen weder für sich, noch können sie über die Person informieren. Das ist erst in ihrem Verbund möglich. Es handelt sich also um eine spezifische Verknüpfungsleistung, die ein Personenbild, eine »digitale Person«[41], als ihr Produkt formt und hervorbringt und die sich mit jeder Änderung der Verknüpfung, jeder Neuerstellung der Liste wandelt. Es ist dies jene eingangs beschriebene dividuelle Logik der Erstellung von Profilen über beständige Rekombinationen von geteilten Daten und Teilungen von Datensätzen. Das Profil ist insofern Produkt einer Verknüpfungs- und Strukturierungsleistung von Daten.

---

39 Bei der Feststellung, ob Personenbezug gegeben ist, sollen nach Erw.Gr. 26 DSGVO alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren. Für die Beurteilung, ob sich Daten auf eine natürliche Person beziehen lassen, kommt es auf die Möglichkeiten und Kenntnisse des Verantwortlichen für die Datenverarbeitung oder eines Dritten an. Die jeweiligen Merkmale machen die Rückbindung der Daten an das damit verbundene Individuum deutlich, vgl. Karg 2019, DSGVO Art. 4 Nr. 1, Rn. 32.

40 Vgl. Karg 2019, DSGVO Art. 4 Nr. 1, Rn. 1.

41 Schweitzer 2017. Vgl. hierzu auch den Beitrag von Gruber/Zihlmann in diesem Band.

Vor dieser Verknüpfung hat die »digitale Person« keine digitale Existenz und damit keinerlei Existenz. Daher ist sie im strengen Sinne performativ.

Zudem ist diese »digitale Person« dem direkten Zugriff durch die natürliche Person entzogen.[42] Denn grundsätzlich werden Daten innerhalb eines Plattformzusammenhangs generiert, gesammelt und wirtschaftlich verwertet.[43] Der Einzelne hat allenfalls eingeschränkt, wenn überhaupt, Zugriff und Einsicht in die Sammlung und Speicherung von Daten. Vor allem hat die einzelne Person auch keine Einsicht darin, welche Daten wo und wie zusammengeführt werden, d.h. aus welchen Daten welche Rückschlüsse qua Kombination auf die Identität gezogen werden (können). Datensatz und natürliche Person sind somit voneinander verschieden, sie folgen unterschiedlichen Logiken. Dem Grunde nach sind sie getrennt. Gleichsam wird der oder die Einzelne aber beständig mit diesen Datenakkumulationen und Kombinationen über den Identifikationsakt konfrontiert – beide Seiten werden durch den Identifikationsakt in Verbindung gesetzt.

Es geht also – um in der obigen Terminologie zu bleiben – um die Konfrontation des individuellen Subjekts mit dem Personenprofil, das aus den Daten hergestellt wird, um die einzelne Person darüber zu identifizieren. Diese Konfrontation des einzelnen Menschen mit einem derart digital erzeugtem Fremdbild, die Konfrontation des Individuums mit seinem dividuellen Profil, stellt das problematisierte Subjektverhältnis dar. Von diesem Problem ist der oder die Einzelne »betroffen«, er oder sie wird eben – um im Sinne der DSGVO zu sprechen – zur »betroffenen Person«.[44]

Die Lösung dieses Problems erfolgt in der DSGVO nun über die Rückbindung des dividuellen Personenprofils an das individuelle Subjekt. Es wird am Grundrechtsschutz, am Schutz des Subjekts der subjektiven Rechte, angesetzt. Dabei wird die einzelne Person nicht als passives Schutzobjekt adressiert, sondern wird mit Handlungsoptionen ausgestattet. Sie wird in die Rolle der Entscheiderin und der autonomen Vertragspartnerin gesetzt.[45] Am deutlichsten zeigt sich dies im Einwilligungserfordernis für eine rechtmäßige Datenverarbeitung. Abseits einzelner Ausnahmen vom

42 Schweitzer 2017, S. 248.

43 Vgl. Möslein/Beise 2022, S. 106.

44 Das passiert vor dem Hintergrund, dass im Online-Kontext die Verfügungsmacht über Daten und die Betroffenheit durch bzw. das Interesse an Daten häufig auseinanderfallen.

45 Vgl. hierzu auch Möslein/Beise 2022, S. 109; Bunnenberg 2020, S. 29. Hanloser spricht hier auch vom »rationalistisch-normative[m] Leitbild« der DSGVO, Hanloser 2023, S. 65.

Einwilligungserfordernis ist die Verarbeitung von personenbezogenen Daten nur dann rechtmäßig, wenn die betroffene Person ihre Einwilligung zu der Verarbeitung der sie betreffenden Daten für einen oder mehrere bestimmte Zwecke gegeben hat (Art. 6 Abs. 1 lit. a) DSGVO). Voraussetzung für die Einwilligung ist, dass sie freiwillig, in informierter Weise und unmissverständlich abgegeben wird (Art. 4 Nr. 11, Erw.Gr. 32 DSGVO). Durch die Gestaltung einer Einwilligungspflicht in die Datenverarbeitung sowie der Regulierung bestimmter, auf die personenbezogenen Daten bezogenen Handlungsoptionen[46] versucht die DSGVO den Einzelnen Instrumente an die Hand zu geben, um in eigener Verantwortung Kontrolle über die digitale Person auszuüben.

Die Handlungsoptionen, welche die DSGVO den »betroffenen Personen« bietet, müssen diese jedoch auch aktiv in Anspruch nehmen, um ihre subjektiven Rechte durchzusetzen.[47] Aus der Fremdanrufung durch die DSGVO wird mithin eine Selbstanrufung. Damit wird aber zugleich die Verantwortung für die Kontrolle über dieses digitale Fremdbild dem Subjekt überantwortet. Datenschutz heißt insofern: Der einzelnen Person Möglichkeiten zu geben, die individuellen Rechte geltend zu machen – und nicht etwa nur ein Ansetzen an der Dateninfrastruktur. Dann gilt aber: Das individuelle Subjekt trägt Verantwortung für das eigene Bild im digitalen Raum, indem es entscheidet, wer Zugang bzw. nicht mehr Zugang zu den »eigenen« Daten erhält. Der Umgang mit dem »Dividuellen«, einem Gegenstand, der ja ständig im Fluss ist und daher auch ständig kontrolliert werden müsste,[48] wird mithin dem Individuum überantwortet.[49]

Diese Überantwortung der Kontrolle über das eigene, durch Daten generierte Bild wird vielfach kritisiert. Eine Verantwortungsübertragung

46 Zu diesen Handlungsoptionen gehören beispielsweise das Auskunftsrecht nach Art. 15 DSGVO, das Recht auf Berichtigung aus Art. 16 DSGVO, das Recht auf Löschung aus Art. 17 DSGVO, das Recht auf Datenübertragbarkeit aus Art. 20 DSGVO, und das Recht aus Art. 21 DSGVO, gegen die Verarbeitung personenbezogener Daten Widerspruch einzulegen. Die Rechte der betroffenen Personen könne man im Hinblick auf die auf die bezogenen Daten mit dem dinglichen Herausgabeanspruch vergleichen, so unter anderen Möslein/Beise 2022, S. 109.

47 Anders nur bei Pflichten, die vom Datenverantwortlichen bei jeder Verarbeitung von Daten einzuhalten sind, wie beispielsweise die Zweckbindung der Daten (Art. 5 Abs. 1 lit. b) DSGVO), die Datenminimierung (Art. 5 Abs. 1 lit. c) DSGVO) und die Wahrung der Richtigkeit der Daten (Art. 5 Abs. 1 lit. d) DSGVO).

48 Vgl. Schweitzer 2017, S. 253.

49 Dies kann als Form der Datensouveränität verstanden werden, die auf dem zivilrechtlichen Prinzip der Privatautonomie fußt, Möslein/Beise 2022, S. 107.

auf die einzelnen Person berge etwa die Gefahr, dass das Individuum eher überfordert, als in seinen Rechten gestärkt werde – aus der Perspektive des individuellen Subjekts steht seine Handlungssouveränität zur Debatte.[50] So könnten auch Rechtsfolgen, die mit der Einwilligungserteilung einhergehen, vom Individuum nur bedingt überblickt werden.[51] Es lässt sich sogar bezweifeln, ob Nutzer:innen überhaupt Interesse an einem hohen Schutz personenbezogener Daten haben, oder nicht viel eher die Vorteile eines eingeschränkteren Schutzes (beispielsweise in Form von kostenlosen Angeboten) in Anspruch nehmen wollen.[52] Daneben steht das Problem fehlender Parität in der Vertragsbeziehung zwischen Datenverarbeitenden und dem einzelnen Subjekt. Dieses ist aufgrund von Informationsdefiziten und Netzwerkeffekten/Lock-In Effekten mit einer schwächeren Verhandlungsposition konfrontiert, wodurch die Gefahr besteht, dass die Einwilligung in die Datenverarbeitung nicht auf Freiwilligkeit beruht.[53] Das Subjekt wird diesen Kritiken zufolge gerade als selbstbestimmte, souveräne, eigenverantwortliche individuelle Person überfordert – es wird aber gleichsam auch hier als Individuum adressiert. Auch in der Kritik wird das Subjekt also in seiner Individualität, d.h. als individuelles Subjekt adressiert.

Demgegenüber adressieren neuere Rechtsakte wie der Data Act und der Data Governance Act Daten nicht nur mit Blick auf die Individuen, sondern gehen von einer über die einzelne Person hinausgehenden Bedeutung und Wert der Daten für die gesamtgesellschaftliche Entwicklung aus (»Big Data«). Hier werden dann allgemeine, wenn nicht gar Allgemeinwohlinteressen an Datensätzen,[54] vor allem der potentielle Nutzen, der in der Dividualität der Datensätze liegt, adressiert.[55] In dieser Blickverlagerung wird – wie gleich zu zeigen sein wird – auch das einzelne Subjekt in anderer Art und Weise adressiert als noch in der DSGVO.

50 Denga 2022, S. 1114.
51 Vgl. hierzu Hanloser 2023, S. 64 f.
52 Denga 2022, S. 1116; Hanloser 2023, S. 64 f.
53 Dem beugt die DSGVO jedoch zumindest in gewissem Umfang vor, beispielsweise durch Informations- und Auskunftsansprüche in den Art. 13 ff. DSGVO, vgl. Möslein/Beise 2022, S. 109 f. Vgl. zum Thema auch Bunnenberg 2020, S. 104 ff. sowie den Beitrag von Pfeiffer in diesem Band.
54 Vgl. auch Denga 2022, S. 1117; Richter/Slowinski 2019, S. 7; Heinzke 2022, S. 1.
55 Zum Nutzen von Open Data beispielsweise für die wissenschaftliche Forschung siehe den Beitrag von Gehring in diesem Band.

2. DGA

Bei der zweiten zu untersuchenden Datenzugangsregulierung handelt es sich um den Data Governance Act, der zusammen mit dem Data Act eine der jüngsten Bestrebungen des Unionsgesetzgebers zur Regulierung des Datenflusses im Internet und des Zugangs zu diesen Daten ist.[56] Statt auf den Schutz von Daten ist der DGA auf eine erleichterte Nutzung von Daten, auch branchenübergreifend, gerichtet. Dies zeigt sich in der Zielsetzung der Verordnung, die darauf gerichtet ist, Hemmnisse im Zugang zu und in der Weiterverwendung von Daten zu beseitigen. Konkret zielt der DGA auf den Ausbau einer Dateninfrastruktur, die Zugang und Übertragbarkeit der Daten sicherstellt (Erw.Gr. 3 DGA). Wie die DSGVO ist der DGA somit auf die privatautonome Disposition über Daten gerichtet, diesmal jedoch nicht in einer auf die einzelne Person bezogenen Art und Weise, sondern in Zielrichtung einer besseren Datennutzbarkeit über den Einzelnen hinaus unter gleichzeitiger Wahrung bestehender Vertrauensstrukturen in eine ordnungsgemäße Datenverarbeitung.

Heruntergebrochen auf die Kernbestandteile richtet sich der DGA auf drei unterschiedliche Formen der Datennutzung, nämlich 1) die Weitergabe von Daten, die sich im Besitz öffentlicher Stellen befinden, 2) die Schaffung eines Ordnungsrahmens für Datenvermittlungsdienste und 3) die Zugänglichmachung von Daten aus Gründen eines Datenaltruismus. Anders als die DSGVO ist der DGA in seinem Anwendungsbereich nicht auf personenbezogene Daten beschränkt, sondern umfasst auch nicht personenbezogene Daten.

Statt des einzelnen Subjekts liegt der Fokus des DGA auf den Wirtschaftsteilnehmenden insgesamt, die in ihrer Funktion hinsichtlich der Zugangsgewährung und Weitergabe von Daten betrachtet werden, sowie auf der Nutzung der Daten zu kommerziellen oder auch nichtkommerziellen Zwecken. Beim DGA geht es somit um eine aktive Teilnahme an der Datenwirtschaft i.S.d. handelnden Akteur:innen. Demnach gibt es nicht einen eindeutig umrissenen Adressaten, sondern viele: Der DGA spricht neben »öffentlichen Stellen« (Art. 1 Abs. 1 lit. a), Art. 2 Nr. 17 DGA), »Datenvermittlungsdiensten« (Art. 1 Abs. 1 lit. b), Art. 2 Nr. 11 DGA) und Diensten des

56 In Kraft getreten am 23. Juni 2022, von den angesprochenen Akteur:innen anzuwenden ab dem 24. September 2023 (Art. 38 DGA).

»Datenaltruismus« (Art. 1 Abs. 1 lit. c), Art. 2 Nr. 16 DGA), auch von »Dateninhabern« (Art. 2 Nr. 8 DGA), »Datennutzern« (Art. 2 Nr. 9 DGA) sowie von »betroffenen Personen« (Art. 2 Nr. 7 DGA).

Indem der DGA – anders als die DSGVO – nicht primär auf den Datenschutz gerichtet ist, sondern die Förderung der Datenteilung und des Datenaustauschs intendiert, erfolgt eine Einordnung des einzelnen Menschen in einen datenbezogenen Wirtschaftskontext. Der Mensch wird in einen Funktionskontext gesetzt, der über eigene individuelle Interessen an Daten hinausgeht. Stattdessen will der DGA gesellschaftliche Chancen einer Datenzugänglichkeit nutzen und Hürden und Ungleichheiten beim Zugang abbauen (vgl. Erw.Gr. 2, 27 DGA).

Trotz dieser Fokusverlagerung kann man den DGA auch auf dessen nach wie vor bestehenden Bezugspunkte auf die einzelne Person hin untersuchen, auch hier werden mithin Subjektverhältnisse problematisiert. Diese Bezugspunkte bestehen schon deshalb, weil der DGA an einigen Stellen auf die »betroffene Person« im Sinne des Art. 4 Nr. 1 DSGVO rekurriert, und damit auf die datenschutzrechtliche Regulierung ausdrücklich Bezug nimmt.[57] Auch im Rahmen des DGA wird das Subjekt mithin als Individuum adressiert. Allerdings geht es nun weniger um die Handlungsermächtigung aufgrund der Betroffenheit – also Handlungsmacht zur Abwehr der Betroffenheit –, sondern um ein »zu schützendes« und »zu unterstützendes« Subjekt. So bleibt der DGA im Schutzgehalt nicht nur bei der Anerkennung der Personenbeziehbarkeit von Daten stehen, sondern beinhaltet auch Regelungen, die das Individuum in seinen hierin begründeten Rechten schützen sollen.

Dies ist insbesondere bei den Regelungen zur Ausgestaltung der Weitergabe von Daten, die sich im Besitz öffentlicher Stellen befinden, zu bemerken, sowie bei den Regelungen zu den Datenvermittlungsdiensten, die eine Art treuhänderische Funktion zugunsten des Individuums einnehmen: Die Bedingungen und der Ablauf bei der Weiterverwendung von Daten, darunter auch personenbezogene Daten (siehe Art. 3 Abs. 1 lit. d) DGA), die sich im

57 Art. 2 Nr. 7 DSGVO. In Art. 1 Abs. 3 DGA heißt es ausdrücklich, dass die DSGVO auch im Anwendungsbereich des DGA gilt, im Falle der Kollision sogar Vorrang eingeräumt bekommt. Einzelheiten sind dennoch umstritten, vgl. Denga 2022, S. 1118. Der DGA könne zumindest nicht die Rechtmäßigkeit der Verarbeitung personenbezogener Daten jenseits der Vorgaben der DSGVO begründen, Savary 2023, § 19 Rn. 17.

Besitz öffentlicher Stellen befinden, sind in Kapitel II des DGA normiert. Obwohl die Regelungen primär auf die Öffnung und Zugänglichkeit von Daten gerichtet sind, schafft der DGA in den Art. 5 ff. einen Ordnungsrahmen, der unter anderem den integren Umgang mit Daten bei der Weitergabe gewährleisten soll. So haben öffentliche Stellen dafür Sorge zu tragen, dass die Daten, die der Weitergabe unterfallen, geschützt bleiben (Art. 5 Abs. 3 S. 1 DGA). Beispielsweise ist vor der Zugangsgewährung zur Weitergabe der Daten sicherzustellen, dass personenbezogene Daten anonymisiert wurden (Art. 5 Abs. 3 S. 2 lit. a), i) DGA), und der Zugang in einer kontrollierten Verarbeitungsumgebung unter Einhaltung hoher Sicherheitsstandards erfolgt (Art. 5 Abs. 3 S. 2 lit. b), c) DGA). Gleichzeitig haben die öffentlichen Stellen Bedingungen aufzustellen, mit denen die Integrität des Betriebs der technischen Systeme der verwendeten sicheren Verarbeitungsumgebung gewahrt wird (Art. 5 Abs. 4 S. 1 DGA). Als weitere Sicherungsmaßnahme sind öffentliche Stellen berechtigt, die Einhaltung von Datenschutzstandards beim Weiterverwender zu prüfen (Art. 5 Abs. 4 S. 2 DGA). Auch wenn die einzelne Person hier nicht selbst adressiert ist, kommen die Regeln dieser zugute. Auch hier steht wieder das Problem der Konfrontation der Person mit den Daten, die auf sie beziehbar sind, zur Debatte – also eine analoge Problematisierung eines bestimmten Subjektverhältnisses wie in der DSGVO. Anders als dort erfolgt die Lösung des Problems nicht darüber, dass der betroffenen Person Handlungsoptionen geboten werden, sondern es wird sozusagen an der Weitergabe und an der Infrastruktur angesetzt. Dadurch soll sie nun Schutz erhalten.[58]

Adressiert wird das Subjekt als betroffene Person darüber hinaus in den Regelungen des DGA zu den Datenvermittlungsdiensten (Art. 10 ff. DGA). Datenvermittlungsdienste sind gemäß Art. 2 Nr. 11 DGA Dienste, mit denen durch technische, rechtliche oder sonstige Mittel Geschäftsbeziehungen zwischen einer unbestimmten Anzahl von betroffenen Personen oder Dateninhabern einerseits und Datennutzern andererseits hergestellt werden sollen, um die gemeinsame Datennutzung, auch für die Zwecke der Ausübung der Rechte betroffener Personen in Bezug auf personenbezo-

58 Lediglich der natürlichen (oder juristischen) Person, die von einer Entscheidung über einen Antrag auf Weiterverwendung von Daten direkt betroffen ist, soll nach Art. 9 Abs. 2 DGA ein Rechtsbehelf zur Verfügung gestellt werden. Die Ergänzung des Wortes »direkt« soll den Anwendungsbereich der Vorschrift zusätzlich einschränken, Specht-Riemenschneider/Hennemann 2023, Art. 9 Rn. 2.

gene Daten zu ermöglichen. Mit der Festlegung von Rahmenbedingungen für Datenvermittlungsdienste soll der Austausch von Daten und damit ein »nichtdiskriminierende[r] Zugang zur Datenwirtschaft« gewährleistet werden (Erw.Gr. 27 S. 4 DGA). Datenvermittlungsdienste sind somit nicht per se auf den Schutz von hinter den Daten stehenden Individuen gerichtet. Dennoch wird die Ausübung von Betroffenenrechten in Bezug auf personenbezogene Daten ausdrücklich als Anwendungsfeld der Datenvermittlungsdienste genannt. Auch hier wird also zur Lösung des Problems auf die Weitergabe und damit die Infrastruktur als Regelungsgegenstand des DGA abgestellt, um das Subjekt zu schützen.

Dabei unterstützen nach Erw.Gr. 30 DGA eine besondere Kategorie an Datenvermittlungsdiensten betroffene Personen bei der Durchsetzung ihrer Rechte aus der DSGVO, beispielsweise im Hinblick auf die Erteilung und den Widerruf der Einwilligung oder der sonstigen Betroffenenrechte wie Auskunfts- oder Löschungsrechte oder auch das Recht auf Datenübertragbarkeit aus Art. 20 DSGVO. Die Anbieter sollen hierbei im besten Interesse der betroffenen Person handeln, und informieren beispielsweise in prägnanter, transparenter, verständlicher und leicht zugänglicher Weise über die beabsichtigte Nutzung der Daten durch Datennutzer und die üblichen Geschäftsbedingungen für solche Nutzungen (Art. 12 lit. m) DGA). Ausgeglichen werden kann durch diese Übernahme einer treuhänderischen Funktion[59] gegenüber der betroffenen Person die oben bereits angesprochene Überforderungssituation bei der Rechtsdurchsetzung durch Einzelpersonen, die im Rahmen der DSGVO naheliegt.[60] Hier erscheint das Subjekt als unterstützungsbedürftig, und es werden Unterstützungsmaßnahmen geregelt.[61]

Dieser Gedanke der gebündelten Interessenvertretung, der den Datenvermittlungsdiensten zugrunde liegt, wird noch verstärkt, wenn im

59 Vgl. Erw.Gr. 33 Abs. 2, S. 3 DGA: »Anbieter von Datenvermittlungsdiensten, die die Datenweitergabe zwischen Einzelpersonen als betroffenen Personen und juristischen Personen als Datennutzer vermitteln, sollten darüber hinaus treuhänderische Pflichten gegenüber den Einzelpersonen haben, damit sichergestellt ist, dass sie im besten Interesse der betroffenen Personen handeln.«

60 Möslein/Beise 2022, S. 110 f. Abgesichert wird die Einhaltung der Pflichten durch Anbieter von Datenvermittlungsdiensten durch die Eingliederung in eine behördliche Aufsichtsstruktur. Beispielsweise bedarf das Angebot eines solchen Dienstes der Anmeldung bei einer Behörde (Art. 11 Abs. 1 DGA), und die zuständige Behörde überwacht zusammen mit den Datenschutzbehörden die Einhaltung der Pflichten des DGA (Art. 14 DGA).

61 Kritisch in Bezug auf den Entwurf zum DGA, Roßnagel 2021, S. 175.

DGA auch von sogenannten Datengenossenschaften die Rede ist.[62] Sie sind ebenfalls darauf gerichtet, die betroffenen Personen bei der Ausübung ihrer Rechte in Bezug auf bestimmte Daten zu unterstützen (vgl. Art. 2 Nr. 15 DGA). Dazu gehört laut Erw.Gr. 31 S. 1 DGA beispielsweise die Stärkung der Position von Einzelpersonen bei der sachkundigen Entscheidung vor der Einwilligung zur Datennutzung und die Beeinflussung von Geschäftsbedingungen von Datennutzerorganisationen zugunsten besserer Wahlmöglichkeiten.

Neben der Ansprache des Subjekts als ein zu unterstützendes und zu schützendes, wird es darüber hinaus auch als eine Art »zu überzeugendes« adressiert. In seinen Formulierungen ist der DGA darauf gerichtet, Vertrauen als konstituierendes Element eines freien Datenverkehrs herauszustellen. Vertrauen soll vor allem durch eine ökonomische Infrastruktur geschaffen werden, die das Individuum in die Lage versetzt, eigene Rechte zu kennen und effektiv wahrzunehmen (Erw.Gr. 5 DGA). Das Vertrauen als zentraler Topos im DGA[63] zeigt sich an unterschiedlichen Stellen. In Erw.Gr. 5 S. 1 DGA heißt es beispielsweise, dass die Verordnung darauf gerichtet ist,

»Vertrauen in die gemeinsame Datennutzung zu stärken, indem geeignete Mechanismen geschaffen werden, die es den betroffenen Personen und Dateninhabern ermöglichen, Kontrolle über die sie betreffenden Daten auszuüben, und sonstige Hemmnisse für eine gut funktionierende und wettbewerbsfähige datengesteuerte Wirtschaft abzubauen.«

Bei der Weiterverwendung von geschützten Daten i.S.d. DGA sollen Unternehmen und betroffene Personen darauf vertrauen können, dass die Weiterverwendung in einer Art und Weise erfolgt, die ihre Rechte und Interessen wahrt. Und auch hinsichtlich der Datenvermittlungsdienste wird betont, dass es gerade das Ziel der Schaffung eines Rechtsrahmens für diese Dienste sei, das Vertrauen in sie zu stärken (Erw.Gr. 32 S. 1 DGA).[64]

Trotz der (mittelbaren) Stärkung der Rechte des Individuums, ist das zentrale Ziel des DGA, die öffentlich verfügbaren Daten der Gesellschaft zugutekommen zu lassen, also die Verteilung und Zugänglichkeit von Daten zu för-

62 Es handelt sich um eine spezielle Form an Datenvermittlungsdiensten, deren Mitglieder betroffene Personen, Ein-Personen-Unternehmen oder Kleinstunternehmen sowie kleine und mittlere Unternehmen (KMU) sein können (Art. 2 Nr. 15 DGA).

63 Der Begriff des »Vertrauens« wird im DGA 12-mal verwendet.

64 Vgl. hierzu auch Savary 2023, § 19 Rn. 4. Kritisch Hornung/Schomberg 2022, S. 513 Rn. 29 f.

dern (Erw.Gr. 2 DGA).[65] In dieser Perspektive steht letztlich die einzelne Person (oder auch das Unternehmen), bei welcher die Daten liegen, im Hinblick auf die datenschutzrechtliche Sicherung der Daten als Störfaktor den Zielen des DGA entgegen.[66] Datenschutz – so die implizite Annahme – entfaltet hemmende Wirkung auf den freien Datenfluss.[67] Nicht der Staat hemmt die freie Entfaltung des Marktes, sondern das Individuum, indem es Daten an sich bindet (insbesondere durch datenschutzrechtliche Regelungen) anstelle sie zu verbreiten bzw. verfügbar zu machen – so das problematisierte Subjektverhältnis. Das Subjekt ist Tor und gleichzeitig Zugangsschranke einer freien Datennutzbarkeit. Um genau diesen Hemmnissen entgegenzuwirken, wird das Subjekt nun unter dem Stichwort »Datenaltruismus« als eine Art Dividuum adressiert: Es wird angerufen als eine Person, deren Daten prinzipiell teilbar sind, und es wird dazu aufgefordert, bestimmte abgetrennte bzw. abtrennbare Daten, die gemeinwohlfördern sind, zu teilen.[68] Namentlich geht es um Daten für die Gesundheitsversorgung, die Bekämpfung des Klimawandels, die Verbesserung der Mobilität, die einfachere Entwicklung, Erstellung und Verbreitung amtlicher Statistiken, die Verbesserung der Erbringung öffentlicher Dienstleistungen, die staatliche Entscheidungsfindung oder die wissenschaftliche Forschung im allgemeinen Interesse (vgl. Erw.Gr. 45 S. 2, 3 DGA).

Während der DGA die betroffene Person bei der Weiterverwendung von Daten, die sich im Besitz öffentlicher Stellen befinden, und bei den Datenvermittlungsdiensten als passiv zu förderndes und zu unterstützendes, aber nicht zu befähigendes Subjekt adressieren, kommt dem Subjekt im Rahmen des sogenannten Datenaltruismus, der auch als Form der Datenspende gesehen werden kann, Handlungsoptionen in Form der Einwilligungserteilung

65 Die Herrschaft über Daten auf eigenem Hoheitsgebiet wird unter dem Stichwort »Digitale Souveränität« diskutiert, Augsberg/Gehring 2022, S. 7; Denga 2022, S. 1119, Hornung/Schomberg 2022, S. 509 Rn. 3 ff.

66 Vgl. Specht-Riemenschneider u.a. 2021, S. 25 f.; Engeler 2022.

67 Vgl. etwa Erw.Gr. 6 DGA: »Aufgrund der Sensibilität solcher Daten müssen bestimmte verfahrenstechnische und rechtliche Anforderungen erfüllt werden, bevor sie zur Verfügung gestellt werden […]. Die Erfüllung dieser Anforderungen erfordert in der Regel viel Zeit und Sachverstand. Dies hat auch dazu geführt, dass diese Daten unzureichend genutzt werden.« Instruktiv auch Hornung/Schomberg 2022.

68 Kritisch, ob der DGA tatsächlich in der Lage ist, die aus dem Datenschutz rührenden Hemmnisse aufzulösen, Schildbach 2022, S. 152; Specht-Riemenschneider u.a. 2021, S. 26; Savary 2023, § 19, Rn. 17; Hornung/Schomberg 2022, S. 514 f. Rn. 33, 38.

zu (Erw.Gr. 45 S. 1, Art. 21 Abs. 2, 3, 25 DGA).[69] Das Subjekt soll sich zum Wohle der Allgemeinheit selbstlos verhalten, indem es in spezifischen Bereichen Daten über sich teilt. Es soll sich also nicht als zu schützendes oder wehrhaftes individuelles Subjekt verstehen, welches Daten an sich bindet und damit die Bestimmung über seine Identität, seine Individualität sichert. Es soll sich vielmehr als Marktteilnehmer verstehen, der problemlos und vertrauensvoll bestimmte Teile seines »Datenschatzes« nicht nur teilen soll, sondern aus altruistischen Gründen auch teilen müsste. Das Vertrauen, welches hierfür als Grundlage dient, wird beispielsweise durch das Eintragungserfordernis von datenaltruistischen Organisationen geschaffen (Art. 17 ff. DGA).[70]

Der Gedanke der Teilbarkeit, also der Fokuswechsel vom Individuum auf das Dividuum, wird hier, anders als bei der DSGVO, nicht als Problem verstanden, sondern als Lösung für das Problem des gehemmten Datenflusses. Das Subjekt wird gerade nicht in der Gefährdung seiner Rechte als Individuum angesprochen, sondern es wird als Hemmnis eines gemeinwohlfördernden Datenflusses adressiert. Daher wird es dazu aufgefordert, sich selbst als Dividuum zu verstehen – das Selbst als einen teilbaren Datenschatz, den es zugunsten des Gemeinwohls auch partiell teilen kann und soll. Damit wird das Subjekt aber zugleich für die Verwirklichung der Gemeinwohlbelange verantwortlich gemacht – wer egoistischerweise nicht teilt, unterwandert die Gemeinwohlziele. Diese Annahme ist vor dem Hintergrund möglich, dass man das Subjekt eben als – letztlich problemlos – teilbare Datenansammlung versteht.

3. DA

Der DA ist die jüngste Datenzugangsregulierung der Europäischen Union und am 11. Januar 2024 in Kraft getreten. In seiner verkündeten Fassung vom 13. Dezember 2023 stellt der DA eine Ergänzung zum DGA dar: Auch der DA zielt auf eine bessere Datennutzbarkeit und eine erleichterte Zugänglichkeit von Daten. Während der DGA jedoch primär auf die Datenweitergabe

69 Datenaltruismus beschreibt, so die Legaldefinition in Art. 2 Nr. 16 DGA, die freiwillige gemeinsame Nutzung von Daten auf der Grundlage der Einwilligung betroffener Personen zur Verarbeitung der sie betreffenden personenbezogenen Daten oder einer Erlaubnis anderer Dateninhaber zur Nutzung ihrer nicht personenbezogenen Daten.

70 Vgl. hierzu auch Erw.Gr. 46 DGA; Savary 2023, § 19 Rn. 54.

zwischen öffentlichen Stellen, Datentreuhändern und Dritten gerichtet ist, soll im Rahmen des DA gerade der oder die Nutzer:in eines Produktes oder Dienstes (nicht identisch mit: die betroffene Person i.S.d. DSGVO) Zugangsmöglichkeiten zu und Verfügungsmöglichkeiten über bestimmte Daten eingeräumt bekommen. Gerichtet ist der DA spezifisch auf Daten, die durch die Nutzung von vernetzten Produkten und damit verbundenen Diensten erzeugt werden, d.h. Geräten, bei denen der physische Gegenstand mit einer virtuellen Funktionalität und einer Netzwerkstruktur ausgestattet ist (sog. Produktdaten und verbundene Dienstdaten, vgl. Erw.Gr. 15 DA).[71]

Der DA besitzt das Ziel, die generierten Daten von einzelnen, marktmächtigen Unternehmen, die grundsätzlich die Verfügungsmacht über die Daten haben, zu lösen und damit eine insgesamt gerechtere Zugänglichkeit und Nutzbarkeit der Daten zu gewährleisten (vgl. Erw.Gr. 5, 6 DA).[72] Damit ist der DA auf den wirtschaftlichen Wert von Daten und das hieran angebundene akteursübergreifende Interesse gerichtet. Neben der Förderung des Zugangs zu und der Nutzung von Daten soll ebenso eine Gewährleistung eines hohen Interoperabilitätsstandards gefördert werden (Erw.Gr. 5 S. 6, Art. 1 Abs. 1 lit. f) DA), was wiederum wettbewerbliche Vorteile mit sich bringt.[73] Auch hier steht wie beim DGA nicht der Schutz des individuellen Interesses im Vordergrund, sondern das Funktionieren des Marktes.[74]

Der DA ist dabei nicht auf personenbezogene Daten beschränkt,[75] und intendiert keine Modifikation geltenden Datenschutzrechts. Sind personenbezogene Daten betroffen, ist das Grundrecht auf den Schutz dieser Daten nach Maßgabe der DSGVO zu wahren, der DA lässt diesen Schutz unberührt (Erw.Gr. 7 S. 1, 4 DA). Im Falle eines Widerspruchs der Rechtsakte habe das Datenschutzrecht gegenüber den Regelungen des DA Vorrang (Art. 1 Abs. 5 S. 3 DA).[76] Fehle es an einer Rechtsgrundlage zur Erhebung und Verarbeitung personenbezogener Daten nach der DSGVO, so könne eine solche Rechts-

71 Insbesondere IoT-Daten (»Internet of Things«), Hennemann/Steinrötter 2022, S. 1482; Podszun/Pfeifer 2022, S. 953, 955.

72 Zum Hintergrund auch Mendelsohn/Richter 2023, § 20 Rn. 5 ff.

73 Vgl. hierzu insbesondere die Art. 33 ff. DA.

74 Kritisch hinsichtlich der Vereinbarkeit der dem oder der Nutzer:in zugewiesenen Zugangsmöglichkeiten zu Daten mit dem Ziel des DA, einen über den oder die Einzelnen hinausgehenden Zugang zu Daten zu fördern, vgl. Funk 2023.

75 Vgl. nur Art. 1 Abs. 2 DA.

76 Noch zum Verhältnis von DSGVO zur Vorschlagsfassung des DA der EU-Kommission Steinrötter 2023, S. 216.

grundlage auch nicht aus den Regelungen des DA zur Weitergabe von Daten abgeleitet werden (Erw.Gr. 7 S. 7 DA).

Auch wenn es beim DA primär um die Regulierung der Marktstrukturen geht, wird ebenso die einzelne Person, nun als Teil dieses Marktgeschehens, adressiert. Im Vordergrund steht dabei die Anrufung als Person – allerdings nicht als die natürliche Person, auf die Daten bezogen sind, sondern die natürliche oder juristische Person, die ein vernetztes Produkt oder einen verbundenen Dienst nutzt und dadurch zur Datengenerierung beiträgt. Begrifflich ist hierbei die Rede vom Nutzer, als einer natürlichen oder juristischen Person, die ein vernetztes Produkt besitzt oder der vertraglich zeitweilige Rechte für die Nutzung des vernetzten Produktes übertragen wurden oder die verbundenen Dienste in Anspruch nimmt (Art. 2 Nr. 12 DA).[77] Adressiert wird somit die einzelne Person als Subjekt, das konsumiert und dabei produziert. Das Subjekt des DA wird insofern als bestimmte Form des »Prosumenten«[78] wahrgenommen. Es ist nicht beschränkt auf seine Eigenschaft als Konsument:in eines Produktes oder Dienstes, sondern wird auch als Produzent:in von Daten verstanden (vgl. Erw.Gr. 6 S. 1 DA). Es geht also um die Nutzung von Produkten oder Diensten, bei der unvermeidlich Daten anfallen, quasi als Nebenwirkung – nicht intendiert und nicht unbedingt personenbezogen.[79] Hier ist das Subjekt durchaus aktiv – aber nicht mit Blick auf seine Rechte an Daten, indem es Ansprüche geltend macht, sondern als praktisch handelndes und dadurch produzierendes Subjekt. Es erscheint dabei als Produzent:in einer Ansammlung von teils zufällig, unbeabsichtigt generierten Daten, die weder Bezug zueinander noch Bezug zum Nutzer oder der Nutzerin aufweisen müssen, außer dass sie auf den Nutzungsakt eines Produktes oder Dienstes zurückzuführen sind. Daten verweisen hier nicht auf eine Identität, sondern auf einen Nutzungsakt.[80]

77 Der »Nutzer« i.S.d. Art. 2 Nr. 12 DA kann zwar auch betroffene Person i.S.d. Art. 4 Nr. 1 DSGVO sein (sofern es sich um auf die natürliche Person bezogene Daten handelt), gleichermaßen kann es sich beim »Nutzer« aber auch um den Verantwortlichen i.S.d. Art. 4 Nr. 7 DSGVO handeln, nämlich dann, wenn die Daten personenbezogen sind, der Nutzer aber nicht selbst datenschutzrechtlich von diesen betroffen ist, Steinrötter 2023, S. 220; Hartmann/McGuire/Schulte-Nölke 2023, S. 56 Rn. 42 f.

78 Die Wortgenese, die auf Toffler 1980 zurückgeht, ist hier in der Weise nur modifiziert heranzuziehen, als dass keine intendierte Produktion seitens des Konsumenten stattfindet.

79 Vgl. Bomhard/Merkle 2022, S. 170 Rn. 10 ff.

80 Die Nutzung allein reicht jedoch nicht, es bedarf auch der Einbindung in ein (vor-)vertragliches Verhältnis, vgl. Art. 3 Abs. 2, 3 DA; Hartmann/McGuire/Schulte-Nölke 2023, S. 55 Rn. 38.

Dem gegenüber steht der »Dateninhaber« als natürliche oder juristische Person, die berechtigt oder verpflichtet ist, Daten – soweit vertraglich vereinbart, auch Produktdaten oder verbundene Dienstdaten – zu nutzen und bereitzustellen, die sie während der Erbringung eines verbundenen Dienstes abgerufen oder generiert hat (Art. 2 Nr. 13 DA). Auch der Dateninhaber trägt somit zur Datengenerierung bei, ist aber gegenüber dem Nutzer im Ausgangspunkt alleiniger Profiteur der Daten. Der DA problematisiert nun die Zugänglichkeit genau dieser Daten als Infrastrukturproblem des Datenmarktes. Der Nutzer als Prosument der Daten trägt zwar zur Entstehung der Daten bei, gesammelt, gespeichert und verarbeitet werden die Daten jedoch primär bei Anbietern vernetzter Produkte oder verbundener Dienstleistungen, die somit auch die Verfügungsmacht über die Daten besitzen und in Konsequenz dann auch von diesen Daten profitieren.[81] Der DA zielt angesichts dessen auf eine forcierte Teilbarkeit bei der Verteilung der Daten. Diese sollen nicht etwa an einem Ort gebündelt sein, sondern dezentral in unterschiedlichen Wirtschaftszusammenhängen zu einer verbesserten Datenlage beitragen.[82]

In dieser Konstellation wird das Subjekt nun als aktiver Garant des Marktgeschehens adressiert: Es soll die Hindernisse der Datenteilung überwinden helfen. Insofern kann man das problematisierte Subjektverhältnisse hier als Frage nach der Rolle des Subjekts für das Funktionieren des Marktes umschreiben.[83] Um Probleme der Datenzugänglichkeit zu beheben, stattet der DA den Nutzer mit verschiedenen Handlungsoptionen aus. So wird ihm die Möglichkeit gegeben, vom Dateninhaber den Zugang zu den generierten Daten zu verlangen, soweit er nicht selbst direkt vom vernetzten Produkt oder dem verbundenen Dienst auf die Daten zugreifen kann (Art. 4 Abs. 1 DA), sowie Dritten den Zugang zu Daten zu ermöglichen (Art. 5 Abs. 1 DA). Anknüpfungspunkt für die Gewährung von Handlungsoptionen ist nicht der Personenbezug wie bei der DSGVO, sondern der Nutzungsakt eines Produktes oder eines Dienstes, durch den Daten generiert werden. Anders als bei der DSGVO knüpft die Verantwortlichkeit des Subjekts somit nicht an das in der digitalen Person verkörperte Fremdbild an, sondern an die personenbezogenen und nicht-personenbezogenen Daten insgesamt sowie der integren

81 Vgl. Podszun/Pfeifer, S. 953.
82 Vgl. Mendelsohn/Richter 2023, § 20 Rn. 10.
83 Kritisch zur Nutzerzentrierung des DA, Podszun/Pfeifer 2023, S. 960 f.

Nutzung der Daten durch den Nutzer selbst sowie durch Dritte, die Daten zur Verfügung gestellt bekommen.[84] Grenzen findet die Dispositionsbefugnis in den Interessen des Dateninhabers (vgl. Art. 4 Abs. 6–8, 10 DA).

Letztlich geht der DA von der Annahme aus, dass der Nutzer ein Interesse daran hat, auf eigens produzierte Daten zugreifen zu können bzw. diese Dritten zur Verfügung zu stellen. Das Subjekt hat also – dieser Sichtweise folgend – ein Interesse, dass die Daten, die es produziert, geteilt werden. Auch hier wird es demgemäß als Dividuum adressiert: Ein Datenschatz als Ansammlung vieler Datenspuren, die von ihm erzeugt werden, und welche möglichst vielen zugänglich gemacht werden sollen, damit der Datenmarkt funktioniert.

Das Subjekt wird damit allerdings (zumindest implizit) zugleich auch in seiner Verantwortlichkeit für eine möglichst frei zugängliche Dateninfrastruktur adressiert: Letztlich ist der DA auf die Förderung der Distribution von Daten durch das Subjekt als Datenproduzent gerichtet. Indem das Subjekt selbst über die Zugänglichkeit und Verbreitung der Daten bestimmen können soll, wird es zum Mittler bzw. Distributor der Daten. Auch hier gilt wie bei dem DGA: Der Gedanke der problemlosen Teilbarkeit der Daten über das Selbst, also der Fokuswechsel vom Individuum auf das Dividuum, wird als Lösung für das Problem des gehemmten Datenflusses adressiert, wobei es vor allem um die Infrastruktur der Datenwirtschaft geht. Der DA intendiert und fördert die Teilbarkeit der Daten über das Subjekt. Daten werden gelöst von ihrer Bindung an das Datensubjekt, die über die Identifizierbarkeit hergestellt wird, und das Subjekt soll sich selbst letztlich als teilbare, zur Distribution fähige Datenvielfalt verstehen.[85] Damit einher geht jedoch wiederum eine Verantwortungszuweisung an das Subjekt, auch zu einer Distribution der Daten faktisch beizutragen.[86]

84 Defizite in der verfassungsrechtlichen Begründung der Zuweisung dieser »Rechte« an den die Daten produzierenden Nutzer sieht Funk 2023, S. 424.

85 Das Subjekt muss sich jedoch auch in dieser Rolle verstehen und aktiv einen Beitrag zur Datenteilbarkeit leisten wollen, ansonsten läuft der DA Gefahr, die Datenzugänglichkeit durch die Zuweisung eines beinah ausschließlichen Rechts an Daten insgesamt eher einzuschränken als zu fördern, Funk 2023, S. 424 ff.

86 Vgl. Mendelsohn/Richter 2023, § 20 Rn. 13: »Datenzugangsrechte [stellen] eine Pflicht zum Datenteilen dar«. Zu der hiermit einhergehenden potentiellen Überforderungssituation für den Nutzer, ebd., § 20 Rn. 41.

III. Fazit

Auch wenn alle drei hier untersuchten Regulierungen auf den Schutz der personenbezogenen Daten Bezug nehmen, werden ganz unterschiedliche Subjektverhältnisse problematisiert und durch die Regulierungen einer Lösung zugeführt: In der DSGVO geht es primär um die Konfrontation des Individuums mit einem dividuellen Zugriff etwa über das Personenprofil, das im Akt der Identifizierung auf das individuelle Subjekt zurückgebunden wird. Diese Problemlage wird über den Rückgriff auf das individuelle Subjekt der subjektiven Rechte gelöst: Ihm werden dadurch Handlungsoptionen zur Kontrolle des Profils zugeschrieben. Die dividuelle Natur von Datensätzen wird von der DSGVO als *Problem für das Individuum* verstanden, als Problem des Grundrechtsschutzes, und der Umgang mit diesem Problem wird dem Individuum überantwortet – es muss seine Rechte geltend machen, indem es das jeweilige Profil »kontrolliert«. Damit wird dies gleichzeitig zum individuellen Problem.

Demgegenüber zielen DGA und DA auf die über die einzelne Person hinausgehende Bedeutung und den Wert der Daten für die gesamtgesellschaftliche Entwicklung mit Blick auf Gemeinwohlinteressen und einen funktionierenden Datenmarkt ab (»Big Data«). Hier werden vor allem der potentielle Nutzen, der in der Dividualität der Datensätze liegt, adressiert. Dabei zielt der DGA darauf, über den Ausbau einer entsprechenden Infrastruktur Hemmnisse im Zugang zu und bei der Weiterverwendung von Daten zu beseitigen. Das einzelne Subjekt erscheint hier einerseits als ein zu unterstützendes und zu schützendes Subjekt – durchaus auch primär im individuellen Sinne, wenn es um die Unterstützung der Rechte aus der DSGVO geht. Das gilt auch für die Adressierung als »zu überzeugendes« Subjekt, wenn der DGA auf die Herstellung von Vertrauen in den Umgang mit Daten zielt. Wenn es andererseits darum geht, die Verteilung und Zugänglichkeit von Daten zu fördern, dann erscheint der Schutz der Daten einzelner Personen aber primär als Hemmnis. Die hemmende Wirkung des Individuums auf die freie Entfaltung des Datenmarktes erscheint als das problematisierte Subjektverhältnis. Zur Lösung dieses Problems des gehemmten Datenflusses wird nun das Subjekt als Dividuum adressiert: als altruistisches Subjekt, dass seine Daten a) problemlos teilen kann – das Selbst als teilbarer Datenschatz – und diese b) aus Gemeinwohlgründen auch teilen soll. Darüber wird das Subjekt für die Verwirklichung der Gemeinwohlbelange (mit-)verantwortlich gemacht.

In Ergänzung zum DGA zielt auch der DA auf eine bessere Datennutzbarkeit und eine erleichterte Zugänglichkeit von Daten, hat aber primär die Daten, die bei Nutzung von vernetzten Produkten und verbundenen Diensten anfallen, im Blick. Dabei geht es um das Funktionieren des Marktes, d.h. die gerechtere Zugänglichkeit und Nutzbarkeit der Daten. Das problematisierte Subjektverhältnisse dreht sich nun um die Frage nach der Rolle des einzelnen Subjekts für das Funktionieren des Marktes. Dabei erscheint es als »Prosument«, das über den Konsum ständig Daten produziert, darüber aber (zunächst) keine Verfügungsmacht hat. Diese Verfügungsmacht wird ihm erst durch den DA zugeteilt: Es kann gegenüber den Dateninhabern Ansprüche geltend machen, um die Daten dann weiter zu verteilen. Auch hier wird es als Dividuum adressiert: Als ein Subjekt, dessen produzierte Daten ohne Probleme teilbar sind und welches daher ein Interesse daran hat, seinen Datenschatz zu teilen – als eine Art Garant eines gerechten Marktgeschehens.

Bezieht man diesen Befund nun auf die eingangs dargestellte Diskussion in der Soziologie und in den Sozialwissenschaften auf die Auswirkungen der Datafizierung auf die Hervorbringung des Subjekts, so muss man feststellen: Anhand der Regulierungen lassen sich Verschiebungen erkennen. Denn entgegen der Annahme der forcierten Fremdkontrolle über die Anrufung als dividuelles Subjekt zeigen die Analysen des DA und des DGA: Auch das Recht kennt angesichts der Datafizierung des Sozialen das Dividuum, es wird explizit mit den hieraus entstammenden Problemen gerungen. Und dabei zeigt sich: Allenfalls in der DSGVO geht es um die Konfrontation des Individuums mit der dividuellen Datenlogik, tritt das Dividuum sozusagen dem Individuum gegenüber, das es unter Kontrolle halten muss. Für den DGA und den DA jedoch gilt: In je unterschiedlichen Konstellationen enthalten sie Möglichkeiten und Aufforderungen der Selbstanrufung als ein »dividuelles« Subjekt, als teilbarerer Datenschatz, das seine Daten teilen soll und angesichts der bestehenden Problemlagen auch müsste. Damit wird dem Subjekt zugleich eine Infrastruktur- und Gemeinwohlverantwortung zugeschrieben, dem es gerade über die Teilungslogik entsprechen kann. Welche Auswirkungen das auf das Subjektverständnis im Recht, aber auch in der Gegenwart hat – das ist noch offen.

Literatur

Augsberg, Ino/Keller, Helen/Lindner, Franz Josef (2023): Selbstbestimmung und Fremdbestimmung in der liberalen Demokratie, in: Schorkopf, Franz (Hg.): *Verfasste Freiheit*, Berlin, S. 29–196.

Augsberg, Steffen (2022): Datenschutz, Datensouveränität, Data Governance: Überlappungen, Spannungen und mögliche Lerneffekte, in: Augsberg, Steffen/Gehring, Petra (Hg.): *Datensouveränität. Positionen zur Debatte*, Frankfurt am Main, S. 121–134.

Augsberg, Steffen/Gehring, Petra (2022): Datensouveränität als Diskursgegenstand: Ambiguität als Chance?, in: Augsberg, Steffen/Gehring, Petra (Hg.): *Datensouveränität. Positionen zur Debatte*, Frankfurt am Main: Campus Verlag, S. 7–18.

Bettinger, Patrick (Hg.) (2022): *Educational Perspectives on Mediality and Subjectivation*, Cham.

Bomhard, David/Merkle, Marieke (2022): Der Entwurf eines EU Data Acts. Neue Spielregeln für die Data Economy, in: *Recht Digital (RDi)*, Heft 4, S. 168–176.

Bräutigam, Peter/Kraul, Torsten (Hg.) (2021): *Internet of Things. Rechtshandbuch*, München.

Bröckling, Ulrich (2007): *Das unternehmerische Selbst. Soziologie einer Subjektivierungsform*, Frankfurt am Main.

Bröckling, Ulrich (2002): Jeder könnte, aber nicht alle können. Konturen des unternehmerischen Selbst, in: *Mittelweg 36* 11, Heft 4, S. 6–26.

Bröckling, Ulrich (2000): Totale Mobilmachung. Menschenführung im Qualitäts- und Selbstmanagement, in: Bröckling, Ulrich/Krasmann, Susanne/Lemke, Thomas (Hg.): *Gouvernementalität der Gegenwart: Studien zur Ökonomisierung des Sozialen*, Frankfurt am Main, S. 131–167.

Bunnenberg, Jan Niklas (2020): *Privates Datenschutzrecht. Über Privatautonomie im Datenschutzrecht – unter besonderer Berücksichtigung der Einwilligung und ihrer vertraglichen Kopplung nach Art. 7 Abs. 4 DS-GVO*, Baden-Baden.

Butler, Judith (2005): *Psyche der Macht: Das Subjekt der Unterwerfung*, Frankfurt am Main.

Catlaw, Thomas J./Sandberg, Billie (2018): The Quantified Self and the Evolution of Neoliberal Self-Government: An Exploratory Qualitative Study, in: *Administrative Theory & Praxis* 40, Heft 1, S. 3–22.

Deleuze, Gilles (1993): Postskriptum über die Kontrollgesellschaften, in: Deleuze, Gilles (Hg.): *Unterhandlungen*, Frankfurt am Main, S. 254–262.

Deleuze, Gilles/Guattari, Félix (1992): *Tausend Plateaus. Kapitalismus und Schizophrenie 2*, Berlin.

Denga, Michael (2022): Digitale Souveränität durch Datenprivatrecht?, in: *Gewerblicher Rechtsschutz und Urheberrecht (GRUR)*, Heft 15, S. 1113–1120.

Duttweiler, Stefanie/Gugutzer, Robert/Passoth, Jan-Hendrik/Strübing, Jörg (Hg.) (2016): *Leben nach Zahlen. Self-Tracking als Optimierungsprojekt?*, Bielefeld.

Duttweiler Stefanie/Passoth Jan-Hendrik (2016): Self-Tracking als Optimierungsprojekt?, in: Duttweiler, Stefanie/Gugutzer, Robert/Passoth, Jan-Hendrik/Strübing, Jörg (Hg.): *Leben nach Zahlen. Self-Tracking als Optimierungsprojekt?*, Bielefeld, S. 9–45.

Ehmann, Eugen/Selmayr, Martin (Hg.) (2018): *DS-GVO. Datenschutz-Grundverordnung*, München.

Engeler, Malte (2022): Der Konflikt zwischen Datenmarkt und Datenschutz. Eine ökonomische Kritik der Einwilligung, in: *Neue Juristische Wochenschrift (NJW)*, S. 3398–3405.

Europäische Kommission (2023): *Verordnung (EU) 2023/2854 des Europäischen Parlaments und des Rates vom 13. Dezember 2023 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung sowie zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie (EU) 2020/1828 (Datenverordnung)*, https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32023R2854 [21.5.2024].

Europäische Kommission (2022): *Verordnung (EU) 2022/868 des Europäischen Parlaments und des Rates vom 30. Mai 2022 über europäische Daten-Governance und zur Änderung der Verordnung (EU) 2018/1724 (Daten-Governance-Rechtsakt)*, Amtsblatt L 152/1, https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32022R0868 [21.5.2024].

Europäische Kommission (2016): *Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)*, Amtsblatt L 119/1, https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679 [21.5.2024].

Europäische Kommission (2010): *Mitteilung der Europäischen Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen. Gesamtkonzept für den Datenschutz in der Europäischen Union*, KOM (2010) 609 endgültig, https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52010DC0609, [8.1.2024].

Findeis, Charlotte/Salfeld, Benedikt/Voigt, Stella/Gerisch, Benigna/King, Vera/Ostern, Anna Rosa/Rosa, Hartmut (2023): Quantifying self-quantification: A statistical study on individual characteristics and motivations for digital self-tracking in young- and middle-aged adults in Germany, in: *New Media & Society* 25, Heft 9, S. 2300–2320.

Foucault, Michel (1996): *Diskurs und Wahrheit. Die Problematisierung der Parrhesia: 6 Vorlesungen*, gehalten im Herbst 1983 an der Universität von Berkeley/Kalifornien, Berlin.

Foucault, Michel (2005a): Subjekt und Macht, in: Defert, Daniel/Ewald, François (Hg.): *Schriften: In vier Bänden. Bandd 4: 1980–1988*, Frankfurt am Main, S. 269–294.

Foucault, Michel (2005b): Polemik, Politik und Problematisierung. ›Polémique, politique et problématisations‹; (Gespräch mit P. Rabinow, Mai 1984), in: Defert, Daniel/Ewald, François (Hg.): *Schriften: In vier Bänden. Band 4: 1980–1988*, Frankfurt am Main, S. 724–734.

Foucault, Michel (2005c): Die Sorge um die Wahrheit. ›Le souci de la vérité‹ (Gespräch mit F. Ewald, in Magazine littéraire, Nr. 207, Mai 1984, S. 18–2), in: Defert, Daniel/Ewald, François (Hg.): *Schriften: In vier Bänden. Band 4: 1980–1988*, Frankfurt am Main, S. 823–836.

Foucault, Michel (2009): *Die Regierung des Selbst und der anderen: Vorlesung am Collège de France 1982/83*, Frankfurt am Main.

Fuchs, Peter (1997): Adressabilität als Grundbegriff der soziologischen Systemtheorie, in: *Soziale Systeme* 3, S. 57–79.

Funk, Axel (2023): Das Prinzip der Nutzerzentriertheit des Data Act – ein gravierender Strukturfehler. Untersuchung und Bewertung der zentralen Rolle des Nutzers in der Datenökonomie nach der Konzeption des Data Act, in: *Computer und Recht (CR)*, Heft 7, S. 421–427.

Gertenbach, Lars/Mönkeberg, Sarah (2016): Lifelogging und vitaler Normalismus, in: Stefan Selke (Hg.): *Lifelogging*, Wiesbaden, S. 25–43.

Hanloser, Stefan (2023): Informationelle Selbstbestimmung und informationelle Eigenverantwortung – zwei Seiten einer Medaille, in: *Zeitschrift für Datenschutz (ZD)*, Heft 2, S. 65–66.

Hartmann, Bernd J./McGuire, Mary-Rose/Schulte-Nölke, Hans (2023): Datenzugang bei smarten Produkten nach dem Entwurf für ein Datengesetz (Data Act). Rechtliche Rahmenbedingungen für die Vertragsgestaltung, in: *Recht Digital (RDi)*, Heft 2, S. 49–59.

Heinzke, Philippe (2022): Ein neues Datenrecht für die EU: Digitaler Wandel zum Wohle aller?, in: *Betriebs-Berater (BB)* 18, Heft 18, S. 1.

Hennemann, Moritz/Steinrötter, Björn (2022): Data Act – Fundament des neuen EU-Datenwirtschaftsrechts?, in: *Neue Juristische Wochenschrift (NJW)*, Heft 21, S. 1481–1486.

Hörtnagl, Jakob (2019): Subjektivierung in datafizierten Gesellschaften – Dividualisierung als Perspektive auf kommunikative Aushandlungsprozesse in datengetriebenen Zeiten, in: Gentzel, Peter/Krotz, Friedrich/Wimmer, Jeffrey/Winter, Rainer (Hg.): *Das Vergessene Subjekt. Subjektkonstitutionen in Mediatisierten Alltagswelten*. Wiesbaden, S. 135–156.

Hornung, Gerrit/Schomberg, Sabrina (2022): Datensouveränität im Spannungsfeld zwischen Datenschutz und Datennutzung: das Beispiel des Data Governance Acts, in: *Computer und Recht (CR)*, Heft 8, S. 508–516.

Houben, Daniel/Prietl, Bianca (Hg.) (2018): *Datengesellschaft. Einsichten in die Datafizierung des Sozialen*, Bielefeld.

Hutter, Michael/Teubner, Gunther (1994): Der Gesellschaft fette Beute. Homo juridicus und homo oeconomicus als kommunikationserhaltende Fiktionen, in: Fuchs, Peter/Göbel, Andreas (Hg.): *Der Mensch — das Medium der Gesellschaft?*, Frankfurt am Main, S. 110–145.

Karg, Moritz (2019): DSGVO Art. 4 Nr. 1., in: Simitis, Spiros/Hornung, Gerrit/Spiecker genannt Döhmann, Indra (Hg.): *Datenschutzrecht. DSGVO mit BDSG*, Baden-Baden.

Kelsen, Hans (1960): *Reine Rechtslehre. Mit einem Anhang: Das Problem der Gerechtigkeit*, zweite Auflage, Wien.

Lemke, Thomas (1997): *Eine Kritik der politischen Vernunft: Foucaults Analyse der modernen Gouvernementalität*, Berlin.

Luhmann, Niklas (1981): Subjektive Rechte: Zum Umbau des Rechtsbewußtseins für die moderne Gesellschaft, in: Ders. (Hg.): *Gesellschaftsstruktur und Semantik: Studien zur Wissenssoziologie der modernen Gesellschaft*, Band 2, Frankfurt am Main, S. 45–104.

Lupton, Deborah (2016): *The quantified self. A sociology of self-tracking*, Cambridge.

Mayer-Schönberger, Viktor (2009): *Delete: The virtue of forgetting in the digital age*, Princeton.

Mau, Steffen (2017): *Das metrische Wir. Über die Quantifizierung des Sozialen*, Berlin.

Mendelsohn, Juliane/Richter, Philipp (2023): § 20 Plattformspezifische Vorgaben des Data Acts, in: Steinrötter, Björn (Hg.): *Europäische Plattformregulierung. DSA | DMA | P2B-VO | DGA | DA | AI Act | DSM-RL*, Baden-Baden, S. 544–563.

Menke, Christoph (2008): Subjektive Rechte: Zur Paradoxie der Form, in: *Zeitschrift für Rechtssoziologie* 29, Heft 1, S. 81–108.

Menke, Christoph (2015): *Kritik der Rechte*, Berlin.

Möslein, Florian/Beise, Clara (2022): Datensouveränität als Privatautonomie, in: Augsberg, Steffen/Gehring, Petra (Hg.): *Datensouveränität. Positionen zur Debatte*, Frankfurt am Main, S. 103–120.

Ott, Michaela (2015): *Dividuationen. Theorien der Teilhabe*, Berlin.

Paulitz, Tanja (2005): *Netzsubjektivität/en. Konstruktionen von Vernetzung als Technologien des sozialen Selbst: eine empirische Untersuchung in Modellprojekten der Informatik*, Münster.

Podszun, Rupprecht/Pfeifer, Clemens (2022): Datenzugang nach dem EU Data Act: Der Entwurf der Europäischen Kommission, in: *Gewerblicher Rechtsschutz und Urheberrecht (GRUR)*, Heft 13, S. 953–961.

Raunig, Gerald (2015): *Dividuum. Maschinischer Kapitalismus und molekulare Revolution, Band 1*, Wien.

Reckwitz, Andreas (2020): *Die Gesellschaft der Singularitäten. Zum Strukturwandel der Moderne*, zweite Auflage, Berlin.

Richter, Heiko/Slowinski, Peter R. (2019): The Data Sharing Economy: On the Emergence of New Intermediaries, in: *International Review of Intellectual Property and Competition Law (IIC)* 50, Heft 1, S. 4–29.

Rose, Nikolas (1996): *Inventing our selves: psychology, power, and personhood*, Cambridge.

Roßnagel, Alexander (2021): Grundrechtsschutz in der Datenwirtschaft. Vorsorgepflichten in der Data-Governance, in: *Zeitschrift für Rechtspolitik (ZRP)*, Heft 6, S. 173–176.

Rücker, Daniel/Dienst, Sebastian (2021): § 6 Daten, in: Bräutigam, Peter/Kraul, Torsten (Hg.): *Internet of Things. Rechtshandbuch*, München.

Saar, Martin (2013): Analytik der Subjektivierung. Umrisse eines Theorieprogramms, in: Gelhard, Andreas/Alkemeyer, Thomas/Ricken, Norbert (Hg.): *Techniken der Subjektivierung*, Paderborn, S. 17–27.

Savary, Fiona (2023): § 19 Plattformspezifische Vorgaben des Data Governance Acts, in: Steinrötter, Björn (Hg.) (2023): *Europäische Plattformregulierung. DSA | DMA | P2B-VO | DGA | DA | AI Act | DSM-RL*, Baden-Baden, S. 521–543.

Schaupp, Simon (2016): *Digitale Selbstüberwachung. Self-Tracking im kybernetischen Kapitalismus*, Heidelberg.

Serres, Michel (1998): *Die fünf Sinne. Eine Philosophie der Gemenge und Gemische*, Frankfurt am Main.

Schildbach, Roman (2022): Zugang zu Daten der öffentlichen Hand und Datenaltruismus nach dem Entwurf des Daten-Governance-Gesetzes. Datenwirtschaftsrecht IV: Mehrwert für das Teilen von Daten oder leere Hülle?, in: *Zeitschrift für Datenschutz (ZD)*, Heft 3, S. 148–153.

Schweitzer, Doris (2018): Die Subjektwerdungen der juristischen Person. Subjektivierungstheoretische Überlegungen zur rechtlichen Personalisierung von Kollektiven,

in: Bröckling, Ulrich u.a. (Hg.): *Jenseits der Person. Zur Subjektivierung kollektiver Subjekte*, Bielefeld, S. 175–193.

Schweitzer, Doris (2017): Die digitale Person: Die Anrufung des Subjekts im »Recht auf Vergessenwerden«, in: *Österreichische Zeitschrift für Soziologie* 42, Heft 3, S. 237–257.

Selke, Stefan (2014): *Lifelogging. Warum wir unser Leben nicht digitalen Technologien überlassen sollten*, Berlin.

Seyfert, Robert/Roberge, Jonathan (Hg.) (2017): *Algorithmuskulturen. Über die rechnerische Konstruktion der Wirklichkeit*, Bielefeld.

Specht-Riemenschneider, Louisa/Hennemann, Moritz (2023): *Data Governance Act: DGA*, Baden-Baden.

Specht-Riemenschneider, Louisa/Blankertz, Aline/Sierek, Pascal/Schneider, Ruben/Knapp, Jakob/Henne, Theresa (2021): Die Datentreuhand. Ein Beitrag zur Modellbildung und rechtlichen Strukturierung zwecks Identifizierung der Regulierungserfordernisse für Datentreuhandmodelle, in: *MultiMedia und Recht – Beilage (MMR-Beil.)*, Heft 6, S. 25–48.

Steinrötter, Björn (2023): Verhältnis von Data Act und DS-GVO. Zugleich ein Beitrag zur Konkurrenzlehre im Rahmen der EU-Digitalgesetzgebung, in: *Gewerblicher Rechtsschutz und Urheberrecht (GRUR)*, Heft 4, S. 216–226.

Steinrötter, Björn (Hg.) (2023): *Europäische Plattformregulierung. DSA | DMA | P2B-VO | DGA | DA | AI Act | DSM-RL*, Baden-Baden.

Toffler, Alvin (1980): *The Third Wave*, London.

Vesting, Thomas (2021): *Gentlemen, Manager, Homo Digitalis. Der Wandel der Rechtssubjektivität in der Moderne*, Weilerswist-Metternich.

Whitson, Jennifer R. (2015): Foucault's Fitbit: Governance and Gamification, in: Walz, Steffen P./Deterding, Sebastian (Hg.): *The gameful world. Approaches, issues, applications*, Cambridge, S. 339–358.

Zech, Herbert (2012): *Information als Schutzgegenstand*, Tübingen.

Zillien, Nicole/Fröhlich, Gerrit (2018): Reflexive Selbstverwissenschaftlichung. Eine empirische Analyse der digitalen Selbstvermessung, in: Mämecke, Thorben/Passoth, Jan-Hendrik/Wehner, Josef (Hg.): *Bedeutende Daten. Modelle, Verfahren und Praxis der Vermessung und Verdatung im Netz*, Wiesbaden, S. 233–249.

Zugangsinteressen: Offenheit und Nutzungsinteressen zwischen Wissen und Markt

As open as possible? Datenzugänge für die Wissenschaft im Spannungsfeld zwischen Open Science, Datenteilen und Datenkauf

Petra Gehring

Forschung produziert Daten, hat Daten und publiziert Daten. Forschung benötigt aber auch Zugriffe auf Daten, die nicht aus der Wissenschaft stammen. So muss humanmedizinische Forschung mit klinischen Daten aus der regulären Krankenbehandlung, aber auch von Versicherern arbeiten können und die sozialwissenschaftliche Forschung ist auf den Zugang zu Daten über den Arbeitsmarkt wie überhaupt zur Wirtschaft, Daten zum Bildungssystem, zu Sicherheit und Justiz sowie die vielfältigen staatlichen Sozialleistungen angewiesen. Öffentlich getragene Forschung – von dieser ist im Folgenden die Rede[1] – kann nur leisten, was sie leisten soll, wenn sie über die Ressourcen und auch das Recht zum Wissensgewinn auf der Basis zeitgemäßer Methoden tatsächlich verfügt. Für die sogenannte datenintensive Forschung (WR 2020) des Digitalzeitalters gilt das auch. Und eigentlich sogar in gesteigertem Maße. Denn: mehr Daten, verfeinerte Daten, weiterreichend verknüpfbare Daten, einfacher auswertbare und besser vergleichbare Daten nutzen zu können stellt eines der großen Versprechen digitaler (»*Big Data*« oder auch »datengetriebener«) Forschungsmethoden dar.

Der digitale Wandel hat allerdings in der Frage der Datenzugänge für die Wissenschaft eine datenpolitisch spannungsreiche Lage geschaffen. Neben neuen Legislationen, die das Datenhandeln mit wenig Rücksicht auf wissenschaftliche Belange kanalisieren, sehen sich wissenschaftliche Akteure einer Fülle von forschungspolitischen Forderungen, transnationalen Policies und infrastrukturgebundenen Regeln sowie im Bereich digitaler Daten auch neuartigen faktischen Hindernissen gegenüber, welche die Datennut-

1 Die sogenannte Industrieforschung, also Forschung unter dem Dach von Firmen und mit proprietären, von vornherein der kommerziellen Nutzung vorbehaltenen Ergebnissen werte ich als nicht »Wissenschaft« im hier zur Diskussion stehenden (verfassungsrechtlich privilegierten) Sinn.

zung erschweren und auch die Asymmetrien zwischen Datenzugängen, die große Unternehmen und Staaten besitzen, und solchen Datenzugängen, die der Wissenschaft offen stehen, in der Tendenz vergrößern. Es ist von daher kein Zufall, dass man, unter anderem auf Druck von Forschungsorganisationen, in den Jahren 2023/24 erstmals über ein Forschungsdatengesetz für Deutschland diskutiert, das der Wissenschaft den Zugang zu Daten erleichtern soll.

Nachfolgend möchte ich (1) knapp Aspekte des Spannungsfeldes beschreiben, das sich mit dem digitalen Wandel für den Datenzugang rund um Wissenschaft auftut, und dies aus teils technischen, vor allem aber aus datenrechtlichen sowie wissenschafts- und infrastrukturpolitischen Gründen. Ich lege einen Schwerpunkt auf transnationalen Diskursen der Wissenschaftssteuerung entstammende, widerstreitend gedeutete Programmbegriffe, wie Offenheit, Access/Zugang/Hergabe und auch »Forschungsdaten«. Derzeit sind dies überwiegend noch keine Rechtsbegriffe, aber es handelt sich um weiches Recht in einem sich derzeit mittels Standards neu ordnenden Feld. Anschließend werde ich (2) die Auseinandersetzung um den Zugang zu Forschungsdaten als einen Konflikt um die Verrechtlichung des zuvor – in einer für die Wissenschaft konstitutiven Weise – unverrechtlichten Datenhandelns der öffentlich getragenen Forschung deuten. Das datenpolitische Konzept der »Offenheit« lässt sich von daher mit demjenigen einer wissenschaftsgemäßen »Freiheit« der Nutzung und des (nichtkommerziellen) Teilens konfrontieren. In einem dritten Schritt versuche ich dann zum einen (3.1), hinsichtlich der regulatorischen Erfordernisse für das wissenschaftliche Datenhandeln eine Diagnose zu stellen, die zumindest eine Richtung für mögliche Therapien weisen kann: Datenzugangsregeln in der Wissenschaft aber auch die Publikations- und Zugangsregeln an deren Grenzen insbesondere zur Administration und zur Wirtschaft sollten so ausgestaltet werden, dass dem Allmende-Charakter von Forschungsdaten Rechnung getragen wird – und dies, ohne die Wissenschaft entweder zu enteignen oder aber sie Märkten zu überlassen, in denen sie als Datenlieferant, der nur bekommt, wenn er auch gibt bzw. wenn er Daten kaufen kann, der Übermacht von Unternehmen ausgeliefert wird. Zum anderen (3.2) greife ich das in diesem Band von Malte Gruber und Zaïra Zihlmann diskutierte Szenario des »digitalen Zwillings« kurz auf, und zwar als Beispiel dafür, wie sich ein Grenzregime an der Schnittstelle zwischen wissenschaftlicher und kommerzieller Datennutzung technikgetrieben entwickeln könnte. Abschließend (3.3) wage ich mich an Überlegungen, die

das Konzept »digitaler Daten« – im Verhältnis zu den Konzepten »Information« und »Wissen« – betreffen, so wie es derzeit den Forschungsdaten-Diskussionen zugrunde liegt.[2]

1. Spannungsfeld

1.1 Daten *aus* der Wissenschaft

Forschung produziert (»generiert«, »gewinnt«, reichert an/veredelt, verknüpft) und sie benötigt (»nutzt«, »verwendet«, »verarbeitet«) Daten. Der Fall der Daten*produktion* erscheint einfach. Er fügt sich klassischerweise in eine Prozesskette ein, an deren Ende nach einer Fülle von methodischen Vorgehensweisen die Publikation von Forschungsergebnissen steht. Zugrundeliegende Daten werden einer Publikation in dem Maße beigegeben, wie es zum Beleg der Ergebnisse erforderlich ist. Dass datenbasierte Erkenntnisproduktion für die Gesellschaft wie auch Politik, Administration und Wirtschaft wissenschaftlich geprüftes (»wahres«) Wissen liefert, gilt so als hinreichend gesichert. Daten, die für die wissenschaftliche Nachnutzung attraktiv sind, wirft man zudem nicht einfach weg. Sie werden idealerweise in wissenschaftlichen Datenbanken, Repositorien und Archiven aufbewahrt, wo sie für Forschende wie zumeist auch eine interessierte Öffentlichkeit zugänglich bleiben.[3]

Freilich beeinflusst Digitalökonomie den Forschungszyklus. Durch die Digitalität von Daten, durch datenhungrige Analyseverfahren sowie durch eine Verwissenschaftlichung der Datenarbeit in Unternehmen, zu deren Geschäftsmodell das »Sammeln« und Auswerten von Daten geworden ist, und dann eben auch durch politisch gesetzte Vorzeichen haben sich die Interessenslagen verschoben. *Open Science*, ein mehrdeutiges Schlagwort, zeigt dies an. Zum einen sollen Wissenschaftlerinnen und Wissenschaftler welt-

2 Mit den geschilderten Schritten bleiben meine Überlegungen nicht nur ein Versuch, sondern wollen auch provozieren. Mein besonderer Dank geht an Johannes Fournier und Hubertus Neuhausen, auf deren kluge Einwände zu einer ersten Fassung dieses Textes ich hier bereits reagiere.

3 In der Praxis ist Archivierung zur Nachnutzung freilich ein aufwendiger Prozess, für den nur manche Fachkulturen überhaupt über eine geeignete Methodentradition verfügen (vgl. RfII ^{2}2019). Ebenso ist der Betrieb sogenannter Informationsinfrastrukturen (Bibliotheken, Datenzentren, Sammlungen, Archive) analog wie digital kostenintensiv, was den Möglichkeiten der öffentlich getragenen Wissenschaft bei der Datenbereithaltung naturgemäß Grenzen setzt.

weit Daten föderieren und teilen können, »Offenheit« soll zum Wohle von Bildung Forschung, also primär gemeinwohlorientiert hergestellt werden. Zum anderen sollen wissenschaftliche Datenbestände aber auch seitens der Wirtschaft nutzbar sein. Die Wissenschaft soll also nach Möglichkeit alle Daten, die sie hat, gerade auch die sogenannten Primärdaten (und zwar jenseits der Funktion als Beleg) zur Nutzung (»Nachnutzung«) durch andere wissenschaftliche und nichtwissenschaftliche Interessierte möglichst früh als *Open Data* publizieren.

Open Science und *Open Data* sind neuartige Forderungen. Sie lassen die Losung *Open Access* zwar anklingen, »open« bezieht sich nun aber eben nicht mehr nur auf den Zugang zu Publikationen. Die Metapher des Öffnens zielt vielmehr auf Formen der Teilhabe am Forschungsprozess selbst (einschließlich wissenschaftlicher Ressourcen), und dies auch zu anderen als lediglich wissenschaftlichen Zwecken. Das hat potenziell erhebliche Folgen für die Wissenschaft selbst, sofern hier – sozusagen auf dem Campus, im Labor, am Schreibtisch, aber eben im Medium des Digitalen – nicht nur Einblicke und Transparenz, sondern auch neue Konkurrenzlagen und Vermarktungskonstellation entstehen.

»Open Data« meint heute zwar vor allem die Gewährung von Datenzugang (etwa zu Repositorien). Mit der Open Access-Bewegung ist der Open Data-Gedanke gleichwohl über die Idee verbunden, Daten sollten durch eigens auf das Mitliefern von Daten bzw. Datenzugängen ausgelegte Data Journals bereitgestellt werden. Ein Open Data Monitoring wird somit nicht durch Zufall durch Großunternehmen wie den Springer Nature-Konzern durchgeführt, die im Namen ihrer »Community« Agenda-Setting betreiben: Wie es gelte, den Anteil an OA-Publikationen zu steigern, so gelte es auch den Anteil an (ebenfalls über den Verlag zugänglichen) Open Data »Publikationen« zu erhöhen. Die Einstellung der Wissenschaftler sei positiv, es fehle freilich an Anreizen und Anerkennung – noch honoriere das Wissenschaftssystem selbst den Einsatz für Open Data nicht genug (vgl. Digital Science u.a. 2023).

Die UNESCO hat *Open Science* weltweit postuliert und auch – die Rolle der Wirtschaft dabei allerdings umgehend – wie folgt definiert:

»[…] *open science* is defined as an inclusive construct that combines various movements and practices aiming to make multilingual scientific knowledge openly available, accessible and reusable for everyone, to increase scientific collaborations and sharing of information for the benefits of science and society, and to open the processes of scientific knowledge creation, evaluation and communication to societal actors beyond the traditional scien-

tific community. It comprises all scientific disciplines and aspects of scholarly practices, including basic and applied sciences, natural and social sciences and the humanities, and it builds on the following key pillars: open scientific knowledge, open science infrastructures, science communication, open engagement of societal actors and open dialogue with other knowledge systems.« (UNESCO 2021, S. 7)

Die Schöpfungsprozesse wissenschaftlichen Wissens, entsprechende Infrastrukturen wie auch der Austausch unter Wissenschaftlern wären demzufolge – vollumfänglich? – mit der Gesellschaft und »anderen Wissenssystemen« zu teilen.

Politisch ist *Open Science* auch in Europa gewollt, um europäische Unternehmen in der globalen digitalwirtschaftlichen Konkurrenz besser zu stellen. Maßgeblich hat insbesondere die der EU-Diplomatie wirksam vorgelagerte *cOAlition S* (eine interinstitutionelle Aktivität, der sich ein für die EU-Gesetzgebung Vorlagen liefernder, Offenheit im Sinne von »full and immediate Open Access«[4] erzwingender *Plan S* verdankt) ab 2018 den Open Access-Gedanken erneuert. Die Metapher der Offenheit zitiert die in den 2000er Jahren zunächst in den wissenschaftlichen Fachgemeinschaften selbst erhobene Forderung nach flächendeckendem internetbasiertem (und auch kostenlosem) Zugang zu digitalen und digitalisierten Publikationen. Wie weit nun auch Daten in einem ähnlichen Wortsinn »zu publizieren« wären, ist eine operativ wie auch in wissenschaftsfunktionaler Hinsicht unklare, vielleicht sogar irreführende Frage. Ob Open Science tatsächlich bedeuten kann, jenseits des Publizierens klassischer Forschungsbeiträge (oder auch von Daten in dafür ausgelegten Journals) schlichtweg alle für Forschungszwecke angelegten Datenbanken sei es nur global »für die Wissenschaft« oder eben auch für Nicht-Forschende zu öffnen, dürften die meisten Fachleute von vornherein bezweifeln, nicht nur aus Machbarkeitsgründen, sondern weil dies den wissenschaftlichen Wettbewerb berührt – und digitale Daten im Forschungsdatenzyklus eben auch nicht nur sogenannte »Rohdaten«, Sensor- oder Messdaten, sondern auch Meta- und Prozessdaten, Textdaten, Forschungskommunikationsdaten und höchstpersönliche Datenspuren rund um das Forscherhandeln umfassen. So hat die DFG Open Science als das Zugänglichmachen von »Forschungsergeb-

4 https://www.coalition-s.org/ [12.7.2024].

nissen« definiert und signalisiert, dass nicht wirklich alle Daten auf dem Weg zu diesen Ergebnissen offen zu sein haben.[5]

Die Offenheitsmetapher hat jedenfalls aber einen guten Klang und weckt hohe Erwartungen. Sie klingt auch irgendwie gerecht und großzügig, sofern sie eine »Geschlossenheit« insinuiert, die es zu beseitigen gälte. Es wird gleichsam Freigebigkeit angemahnt. Das schafft freilich eine Konfliktlage, da selbstverständlich die »Freiheit« wie auch der innerwissenschaftliche Wettbewerb öffentlich geförderten Forschung gerade auf einem (auch durch die Verfassung bekräftigten) Schutzraum und auf Privilegien beruht, die unter anderem den Ausschluss direkter wirtschaftlicher Interessen (»Kommerzialisierung«) sicherstellen sollen wie auch Barrieren gegen zivilgesellschaftliche Interessenslagen (»Politisierung«) oder die Einflussnahme von Regierungen (»Zensur«, »Gleichschaltung«) aufbauen. Freiheit der Wissenschaft ist Schaffung eines Raumes für Autonomie von Forschungsprozessen. Und zunächst, nämlich bis zum verantwortbaren Ergebnis, sind diese auch nur wissenschaftsöffentlich, nicht bereits »veröffentlicht« im Sinne von »publik«. Wissenschaftsfreiheit und weitgehende Vergesellschaftung oder Ökonomisierung der Forschung gehen somit nicht zusammen.

Insofern stellt *Open Science* ein zumindest erklärungsbedürftiges Zielbild dar. Zu fragen ist zudem, welche Vorstellung der Funktion von Wissenschaft ihm zugrunde liegt. War Wissenschaft je geschlossen? Und sollte, kann sie überhaupt gleichsam gläsern sein? Was der Offenheitsforderung Plausibilität verleiht, sind Bildungsideale, die Vorstellung der freien Zirkulation von »Wissen« durch Digitalität. »Offener« Datenzugang oder »geöffnete« Datenbanken, Repositorien oder Archive fügen sich allerdings nicht dem Schema der Publikation von Wissen (vgl. Parsons/Fox 2013). Weder »betritt« man di-

5 Vgl. DFG 2022, S. 5. – Als Ziel nennt die DFG allerdings, es gelte, diese Ergebnisse »offen zugänglich zu machen und damit die bessere Nutzbarkeit durch die Wissenschaft selbst und andere Akteure zu gewährleisten« (ebenda). Dies geht über den Akt des »Publizierens« hinaus. Ebenso schließt sich die DFG dem weiten Open Science-Begriff der UNESCO dennoch an und postuliert, sich »grundsätzlich für den offenen Zugang zu (wissenschaftlichen) Publikationen, Forschungs- und Metadaten, für die Offenheit von Forschungs- und Infrastruktursoftware und – wo sinnvoll – von Forschungsprozessen« einzusetzen. »Gleichzeitig«, heißt es dann einschränkend weiter, »sieht die DFG eine vollumfängliche Offenheit des gesamten wissenschaftlichen Prozesses und der Prozesse der Qualitätssicherung oder der Wissenschaftsbewertung nicht als zielführend an« (ebenda). Die DFG betont auch, Open Science könne ausschließlich unter Berücksichtigung wissenschaftskonstituierender Werte gelingen und dürfe kein Selbstzweck sein (vgl. DFG 2022, S. 11).

gitale Datenbestände lediglich, noch können ungeschulte Personen Datenbestände einfach »lesen«. Sondern man betätigt Datendienste, und die digitale Datennutzung ist Entnahme bzw. Kopie. Ebenso kann man digitale Artefakte – werden nicht aufwendige Vorkehrungen getroffen – vervielfältigen, verändern, manipulieren und seinerseits publizieren. Datennutzung »offen« zu ermöglichen bedeutet also, nicht »Wissen«, sondern Produktionsmittel weiterzugeben, dazuhin einer Software (in der Regel damit auch Softwareanbietern) Daten zur Verarbeitung zu überlassen und auch die Art ihrer Nutzung unkontrolliert und bei unklarer Verantwortungslage hinsichtlich möglicher Folgenketten freizugeben.

Dass Daten »aus« der Wissenschaft kommen, gibt ihnen zudem den unter Umständen trügerischen Rang einer besonderen Verlässlichkeit und Qualität – auch dies aufgrund einer falschen Analogie von Daten und Wissen. Denn *Open Data*-Bestände haben ja gerade nicht den Charakter methodischer Ergebnisse von Forschung, es handelt sich um Halbzeug, mit welchem man methodisch richtig umgehen muss. In den Händen von Laien können sich gute Daten rasch in Fake verwandeln. So sind insbesondere irrige, missverständliche oder verfälschende Nutzungen von Daten, die aber der Quelle »Wissenschaft« zugeschrieben werden, für die Reputation der Wissenschaft eine nicht zu unterschätzende Gefahr. Dass die radikal verstandene »offene« Nutzbarkeit auch die Überlassung von in der Wissenschaft produzierten Daten an kommerzielle Wettbewerber umfassen würde, wurde schon gesagt. Wohlmöglich sogar kostenlos würde man also Konzerne und Konzernforschung unterstützen. Dass nicht nur wissenschaftliche Open Access-Publikationen, sondern sogar lizenzierte Materialien heute regulär zum Training proprietärer Algorithmen genutzt werden, zeigt an, wohin die Reise geht.

»Offen« kann zudem Aneignungsprozesse nach sich ziehen: Was zuvor »offen« war, nehmen sich Dritte, lizenzieren es oder bieten Derivate offener Forschungsdatenbestände als Produkte an. So kann öffentliche Forschung unter Umständen die von ihr selbst produzierten Daten nicht mehr »frei« nutzen, sondern wird mit Barrieren konfrontiert, die Nachnutzende errichten.[6] Auch der schon angesprochene Fall der Nutzung »offener« Daten als Trainingsdaten für KI-Produkte zeigt, wie wenig es hier um die ungehinder-

6 Dieser Fall entweder der Piraterie (etwa »Harvesten« und Lizenzieren von gemeinfreien Bildern) oder der »Veredelung« wissenschaftlicher Datenprodukte, um sie dann durch ein besseres Produkt zu verdrängen, ist durchaus realistisch.

te Zirkulation von Wissen geht: Die Daten finden vielmehr Eingang in Black-Box-Produkte, wobei strukturiertes Maschinenwissen aus Datenbeständen heraus gewonnen wird, die dafür nicht erstellt worden sind. Seitens der Wissenschaft selbst kann man dem nichts Steuerndes mehr entgegensetzen.

Der in Deutschland das Wissenschaftssystem und die Politik beratende Rat für Informationsinfrastrukturen (RfII), dem auch die Autorin angehört, hat dem Schlagwort »Offenheit« den Gedanken der »Souveränität der Wissenschaft« zur Seite gestellt. Das Gremium hat zudem aus der Sicht der Wissenschaft systemrelevante Mindestbedingungen für Datendienste an der Schnittstelle von Wissenschaft und Wirtschaft formuliert, zu welchen auch kommerzielle Datenverbreitungsdienste oder Werkzeuge, die »Offenheit« herstellen sollen (etwa Portale), gehören:

»Der RfII hat hier insbesondere Fallkonstellationen im Blick, in denen der auf Wissenschaftsseite nicht verhandelbare Primat der Forschungsmethodik, der wissenschaftliche Wettbewerb selbst (der im Kern kein wirtschaftlicher, sondern ein auf Urheberschaft gegründeter reputationsorientierter bleibt) oder aber das Erhaltungsinteresse an essentiellen Forschungsdatenbeständen (als – ggf. auch zunächst – *nur* für die Wissenschaft gemeinfreie Ressource) in ein Spannungsverhältnis zu unter Umständen ganz anders gearteten Verwertungs- oder Vermarktungsinteressen geraten kann. Wissenschaftliche Akteure müssen auch in Kooperation mit kommerziell arbeitenden Partnern die Verfügungs- und Definitionshoheit (»Souveränität«) in Fragen behalten können, die a) sowohl die Güte und qualitative Bewertung von genuin durch Forschung erzeugte Daten betreffen als auch b) die Beurteilung der qualitativen Eignung außerhalb von Forschungskontexten bereitgestellter Daten für Zwecke wissenschaftlicher Nutzung betreffen (wie das z.B. in den Forschungsdatenzentren von Ämtern und Behörden geschieht).

Eine Souveränität der (digitalen) Wissenschaft in diesem Sinne kann nach Auffassung des RfII nur erlangt bzw. gesichert werden, wenn die europäischen und nationalstaatlichen politischen Institutionen durch ihre umfangreichen aktuellen Vorhaben zur Regulierung der digitalen Märkte Rahmenbedingungen schaffen, die die Wissenschaft dazu ertüchtigen, mit kommerziellen Anbietern – auch mit multinationalen und außereuropäischen Unternehmen, die digitale Dienstleistungen für die Wissenschaft anbieten – ›auf Augenhöhe‹ zu verhandeln.« (RfII 2021, S. 72)

Dass auch innerwissenschaftlich »offene« Datenzugänge mit den in der Forschung selbst ja gewollten und produktiven Konkurrenzlagen in Einklang gebracht werden müssen, versteht sich ebenfalls. Bislang waren keine rechtlichen Regeln nötig, um Wissenschaftlern den Raum zur eigenen Forschung diesseits eines Weiterverwertungswettbewerbs zu sichern, der mit der Publikation beginnt. Die Beschleunigung des Publizierens (Preprints, Social Media) zeigt aber, dass in einer voll-digitalisierten Wissenschaft die

Zeit zur Qualitätssicherung vor der Publikation tendenziell schrumpft – womit eben auch die Verwertung in Gestalt der Übergabe an Märkte immer früher beginnt.

Der RfII hat, um die »Systemgrenze« zwischen dem forschungstypischen Datenhandeln der Wissenschaft und der (ebenfalls datengestützten) Datenverwendung in der Wirtschaft modellhaft darzustellen, folgendes Schema erstellt:

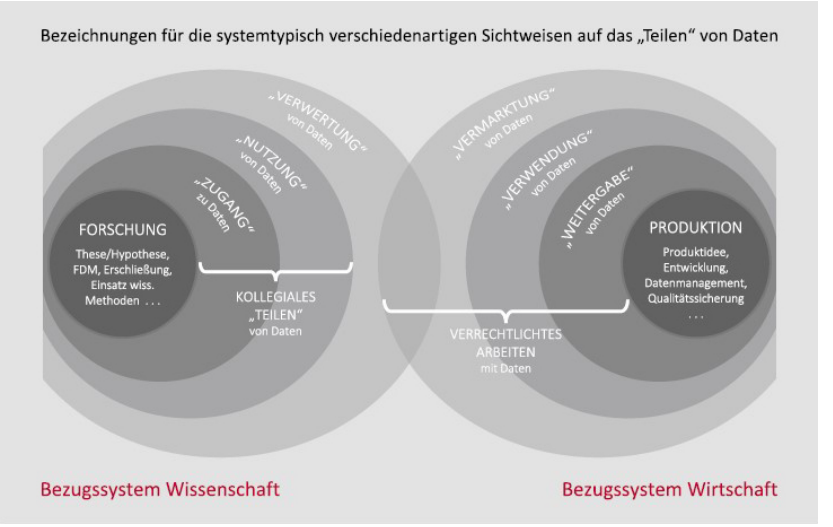

Abb. 1: Systemtheoretisch inspiriertes Schichtenmodell der basalen Praktiken in der Wissenschaft und in der Wirtschaft (jeweils auf dem Weg zu einer »Offenheit« von Daten)
Quelle: RfII 2021, S. 11.

Daten »offen« bereitzustellen, also früh und weitreichend »aus« der Wissenschaft an die Gesellschaft zu übergeben und damit auch für die Verwendung durch die Wirtschaft freizugeben, reduziert im Bezugssystem Wissenschaft tendenziell den Raum des bloß erst kollegialen, innerwissenschaftlichen Teilens – in dem Maße, in welchem die Verwendung der offenen Daten mit dem Ziel der Vermarktung parallel schon einsetzt. Meint *Open Science* einen frühen »Zugang« zu Forschungsdaten auch für Unternehmen ist überdies mit vertraglichen Vereinbarungen zu rechnen – also mit schützenden Datenzugangsregeln und mit Zugangsregeln dann auch für die forschende, kollaborative Nutzung. Digitale Forschungsdateninfrastrukturen schaf-

fen so in der Regel am Ende gerade nicht einfach »offene« Zugänge, sondern gestufte Zugangs- und Nutzungsregimes – auch um der Wissenschaft die für die Forschung benötigten Freiräume zu sichern.

1.2 Daten *für* die Wissenschaft

Dass Forschung auch im Digitalzeitalter weiterhin Zugang zu den – heute: vorzugsweise digitalen – Daten erhält, die sie traditionell etwa im sozialwissenschaftlichen Bereich benötigt, ist ein Problem, welches das Konzept *Open Science* gerade nicht adressiert. *Open Government* ist zwar auch ein existierendes Schlagwort,[7] es wurde jedoch nicht im Sinne einer Öffnung für die Wissenschaft, sondern ebenfalls mit Blick auf Gesellschaft und Wirtschaft geprägt. Weder digitale Märkte noch die Politik stellen derzeit sicher, dass im digitalen Wandel der Datenzugang zu Daten, die die Wissenschaft benötigt, sichergestellt ist (oder auch nur – verglichen mit den Üblichkeiten der vor-digitalen Zeit – sichergestellt bleibt). Sowohl Effekte der Plattformökonomie, also die Herausbildung von kommerziellen Software- und Datenoligopolen, als auch das generell gewachsene kommerzielle Interesse an (auch »ungerichteten«) Datensammlungen und die damit verbundene Wertsteigerung auch exotischer, zuvor nur für die Wissenschaft interessanter Daten, als auch die Belange des digitalen Datenschutzes und die Verlagerung der Regulation von Datenschutz, Dateninhaberschaft und Datennutzung in den transnationalen Raum unterschiedlicher Rechtskulturen haben die Position der Wissenschaft in Deutschland – was Datenzugang angeht – verschlechtert, vor allem faktisch, aber auch de jure.

In vor-digitalen Zeiten nutzten Wissenschaftlerinnen und Wissenschaftler das sogenannte Wissenschaftsprivileg: auf verschiedene geschützte Wissensbestände (etwa von Behörden) darf und soll die öffentlich getragene Wissenschaft zu Forschungszwecken zugreifen. Denn dass auf Daten geforscht wird, ist in öffentlichem Interesse – insbesondere dort, wo Erkenntnisse wiederum der Politik eine Handlungsgrundlage liefern. Nicht selten gehen darüber hinaus immer schon auch Unternehmen gezielte Forschungskooperationen mit der Wissenschaft ein. Zu Zwecken der kollaborativen Industrieforschung werden auf Vertrauens- und Vertragsbasis Wissensbestände und auch Daten geteilt.

7 https://de.wikipedia.org/wiki/Open_Government [22.10.23].

Unter digitalem Vorzeichen haben die Partner, von denen Wissenschaft Datenzugang erwartet, also »Datengeber«, auch Behörden, gute Gründe, den Datenzugang restriktiv zu organisieren. Ein Grund ist die nicht nur einfache Kopierbarkeit, sondern der tatsächlich gefährlich leichte (auch ungewollte) Abfluss digitaler Daten, etwa an kommerzielle Software-Anbieter oder Speicherdienste. Ein anderer Grund ist die durch Verknüpfbarkeit erhöhte Kritikalität von Datensätzen und Datenbeständen. Hierzu gehört der – allerdings auch dank der dazugehörigen Verfahren (Genehmigung durch Datenschutzbeauftragte) inzwischen für das innerwissenschaftliche Arbeiten wirklich sehr restriktiv gehaltene – Datenschutz. Ein dritter, nicht ganz so guter Grund mag auch in einem gesteigerten Bewusstsein für den gefühlt über das, was man früher als Informationswert schätzte, hinausgehenden »Marktwert« von Daten liegen. Alles in allem drohen die Möglichkeiten des Datenzugangs für Wissenschaftlerinnen und Wissenschaftler – auch im Vergleich dazu, was Unternehmen an digitalen Datengewinnungs- und Datenzugangs-Möglichkeiten besitzen – hinter das zurückzufallen, was für das Voranschreiten wissenschaftlicher Arbeit erforderlich wäre. Namentlich um die Konkurrenzfähigkeit öffentlicher Forschung mit der auf »eigenen« Daten immer erfolgreicher forschenden Digitalindustrie ist es schlecht bestellt.

Tatsächlich besitzt Wissenschaft im Bereich digitaler Datenzugänge (noch) keine vergleichbar privilegierte Position, wie sie sie – oft ungeschrieben – in der vor-digitalen Zeit hatte. Datenschutz muss sie sogar ernster nehmen als Firmen, deren AGB aufs Wegklicken angelegt sind. Deutsche Gesetze enthalten auch nur sehr selten Forschungsklauseln (und Regelungen, die überdies auch nicht per se von »Daten« sprechen, sondern von Informationszugang, was Unsicherheiten für konkretes Datenhandeln bedeutet). Neue Digitalgesetze sehen – über das generelle Öffnungsgebot für *Public Sector*-Datensilos[8] hinausgehend – einen Datenzugang für die Wissenschaft erst rudimentär vor (so der Art. 97 des Digital Services Act für »sehr große« Onlinedienste und Suchmaschinen)[9]. Zudem zeichnet sich

8 In Deutschland sind es das Datennutzungsgesetz (DNG) und das Online-Zugangsgesetz (OZG), die einen digitalen Zugang zu Behördendaten postulieren.

9 Der Digital Services Act (DSA) der EU aus dem Jahr 2022 sieht für die Archive sehr großer Online-Plattformen und Online-Suchmaschinen offene Schnittstellen für Forschung zu vom Gesetzgeber gutgeheißenen Zielen und einen Beantragungsweg vor. Ebenso dürfen solche sehr großen digitalen Intermediäre nicht aktiv verhindern, dass Forschende öffentlich zugängliche Daten sammeln, um solche Unternehmen zu beforschen.

ab, dass das kommende europäische Datenrecht sich zunehmend auf sogenannte »Domänen« oder »Sektoren« mittels gesonderter Bestimmungen spezifizierend einstellt. Auch darin liegt eine für die Wissenschaft nicht hilfreiche Entwicklung, denn Forschungsfragen sind keineswegs immer auf Datendomänen oder Sektoren begrenzt. Echte Forschungsklauseln, explizit festgeschriebene Vorrechte für die Wissenschaft also, scheinen von daher zur Absicherung oder auch Schaffung von Datenzugängen in einer digitalisierten Welt der beste Weg zu sein (Specht-Riemenschneider 2021). Es gibt sie indes nur selten. Überdies müssen zu Erlaubnisgesetzen auch Bestimmungen und Infrastrukturen hinzutreten, die den Datenzugang praktisch sichern.[10] Nicht nur in diesem Zusammenhang hat die Rede von »Datenräumen« an Bedeutung gewonnen. Relativ unscharf bezeichnet »Raum« hier eine Sphäre des angemeldeten Zugangs oder auch das Engagement in einem Netzwerk, in welchem Daten unter bestimmten Bedingungen zwischen Akteuren »geteilt« werden (können). Gleichwohl kann die Remote-Nutzung kritischer Behördendaten in Deutschland entweder (noch) gar nicht möglich sein oder nur in stark eingeschränkter Form.

Der Zugang zu Unternehmensdaten ist für die Wissenschaft immer schon nur auf Verhandlungswegen erreichbar gewesen. Wo ein Interesse beider Seiten an Forschungsergebnissen besteht, ist Kooperation möglich, und wo nicht, wird auch nicht kooperiert – wobei die Richtlinien guter wissenschaftlicher Praxis zwar eine Veröffentlichung der Forschungsergebnisse vorsehen, nicht aber der durch Industriepartner geteilten Daten. *Open Data* oder *Open Science*-Forderungen machen so besehen vor Industriekooperationen und Firmengeheimnissen bzw. Unternehmenseigentum Halt. Namentlich die Ingenieurwissenschaften haben die Merkmale einer Kultur der Industrieforschung bislang ins Digitalzeitalter hinein fortschreiben können – so scheint es jedenfalls, wenngleich hierzu kaum öffentliche Diskussionen stattfinden. Einen Sonderfall stellen die Digital Humanities dar, für welche sich insbesondere der Zugang zu digitalen Textkorpora angesichts des Urheberrechtsschutzes schwierig gestaltet.

10 So besitzt Österreich seit kurzem einen gesetzlich abgesicherten Forschungszugang zu Behördendaten, die vorgeschriebene Kompensation der Aufwände für die Betroffene Behörde sorgt aber für derart horrende Kosten, dass Forschungsprojekte hohe Summen mitbringen müssen, um ihr Recht auf Datenzugang zu realisieren. Faktisch ist so Forschung nur möglich, wo der Staat eigens Drittmittel hierfür auslobt.

Forderungen nach einem dringend zu verbessernden Datenzugang für die Wissenschaft kommen jedoch vernehmlich besonders aus den Sozialwissenschaften. Der Rat für Sozial- und Wirtschaftsdaten, der die Belange einer großen Zahl von Forschungsdatenzentren und ihrer wissenschaftlichen Nutzer vertritt, hat mehrmals, zuletzt in den vergangenen beiden Jahren (RatSWD 2022; RatSWD 2023) den verbesserten Zugang zu Forschungsdaten angemahnt. Die quantitative Sozialforschung arbeitet insbesondere mit Daten der öffentlichen Hand, auch zur Wirtschaft. Seltener sind es – sieht man von Nutzungsdaten der großen Internet-Firmen ab – direkt Unternehmensdaten, auf welche die Nachfrage der sozialwissenschaftlichen Forschung sich richtet.

2. Schafft Recht den besseren Zugang?

So offen wie möglich, sei es *in* der, sei es *für* die Forschung: Vor ganz unterschiedlichem Hintergrund greifen Beteiligte zu normierenden, rechtlichen Hebeln. Dem politischen Ziel, wissenschaftliche Datenbestände zu »öffnen«, sollen transnationale Soft Law-Initiativen wie Plan S dienen oder die Überlegungen der UNESCO. Auch die *Public Sector Initiative* (PSI) der EU, auf die das deutsche Datennutzungsgesetz zurückgeht, hat nicht nur für Behördendaten, sondern auch für Daten aus der Wissenschaft Geltung. Es enthält eine Definition von »Forschungsdaten«[11] und postuliert – wo nicht Urheberrechte oder verwandte Schutzrechte bestehen – eine Bereitstellungsverpflichtung, für sogenannte »hochwertige« Datensätze und für Forschungsdaten sogar unentgeltlich. Wenn man so will ist also das DNG ein »Openness«-Gesetz. Eine Wissenschaftsratsempfehlung hat zudem auch das Forscherverhalten in den Blick genommen und ein scharfes Schwert Wissenschaftssteuerung, die Vorgaben für »gute Wissenschaftliche Praxis«, als Weg zur Durchsetzung einer OA-Pflicht ins Spiel gebracht (vgl. WR 2022).

11 »Aufzeichnungen in digitaler Form, bei denen es sich nicht um wissenschaftliche Veröffentlichungen handelt und die im Laufe von wissenschaftlichen Forschungstätigkeiten erfasst oder erzeugt und als Nachweise im Rahmen des Forschungsprozesses verwendet werden oder die in der Forschungsgemeinschaft allgemein für die Validierung von Forschungsfeststellungen und -ergebnissen als notwendig erachtet werden.« § 3, Nr. 10 DNG.

Der Wissenschaft wiederum ihrerseits Datenzugänge zu verschaffen, ist unter den Bedingungen des digitalen Wandels nicht leicht: die unternehmerische Konkurrenz um Daten und der potenzielle Wert von Daten sorgen für Abschottung auch gegenüber Datennutzern, die lediglich wissenschaftliche Interessen haben. Dies macht den Ruf der öffentlich getragenen Forschung nach dem Gesetzgeber verständlich – zumal datengetriebene Forschung so global ist, dass man sich im direkten wissenschaftlichen Wettbewerb auch mit Forschern aus Ländern befindet, die die wissenschaftliche Datennutzung viel liberaler regeln und auch die staatliche Datenerhebung, etwa von Sozial- und Wirtschaftsdaten, systematisch mit dem Ziel einer (auch) forschenden Nutzbarmachung betreiben. Die skandinavischen Länder werden hier oft als Beispiel genannt. Vergleichbares könnte mithilfe eines Forschungsdatengesetzes auch für Deutschland gelingen – dies ist jedenfalls die Hoffnung, die sich derzeit an das im Koalitionsvertrag der Ampelregierung angekündigte Gesetzgebungsvorhaben knüpft.

Mehr *aus* der Forschung herausziehen, mehr *für* die Forschung gewinnen: Es wirken mit diesen heterogenen Zielen aktuell somit gleich zweifach Steuerungsversuche auf das Wissenschaftssystem ein, von zwei Seiten (von »außen« kommend, von »innen« her) und zugunsten ganz unterschiedlicher Interessen. Der bislang informelle Umgang mit Forschungsdaten im Forschungszyklus könnte sich unter einem solchen doppelten Vorzeichen unkoordiniert verändern. Dies allerdings in einer – was die Wucht der Transformationswirkung angeht – ungleichen und, denkt man beides zusammen, wohlmöglich sogar gegenläufigen Weise.

Einerseits fordert *Open Science* eine frühe und dauerhafte Überlassung der Forschungsdaten an Intermediäre sowie die Lizenzierung der Daten als *Common Good*. Zur Absicherung einer wissenschaftseigenen Nutzung bleiben vielleicht Embargofristen übrig oder andere Regeln, jedenfalls sind diese aber *defensiver* Art: nur die nachweislich nötigen Räume für genuine Interessen der Forschenden selber bleiben geschützt. Zur Schaffung des Datenzugangs zu öffentlichen Datenbeständen hingegen ist *offensiv* etwas zu fordern. Hier geht es darum, einen Anspruch der Wissenschaft, der letztlich der Verfassung selbst zu entnehmen ist, in hinreichend wirksame Vorgaben, etwa Forschungsklauseln, zu übersetzen. »Zugang« – im Sinne des Rückbaus rund um digitale Daten entstandenen hohen Nutzungshürden – meint hier also gerade nicht »Offenheit« für alle, sondern selektiven Zugang, dank eines an die spezifische Rolle und Vertrauenswürdigkeit der Wissenschaft gebundenen Privilegs.

Offenkundig kollidieren hier zwei unterschiedliche Regimes: Während man die Daten *aus* der Forschung einem Publizitäts-Regime unterwirft, folgt der Anspruch auf über das ohnehin Öffentliche hinausgehende Daten *für* die Forschung einem Vertrauens- und Vertraulichkeits-Regime. Das Schema des »frei« zugänglichen Wissens steht dem Schema eines Schutzes von Daten oder auch Informationen (als Wissensressourcen) gegenüber.

Digitaler Wandel im Sinne von »Datafizierung«[12] zöge demnach in der Wissenschaft erstens, ganz unterschiedlich motiviert, die schon mehrfach angesprochene Verrechtlichung des Datenhandelns nach sich. Und zweitens verschärfen deren unterschiedliche Stoßrichtungen eine paradoxe Lage: Wissenschaft soll zugleich (als Datengeberin) »offen« sein und (als Datennutzende) »diskret«. Drittens schwindet aber auch der Spielraum zum Umgang mit der Paradoxie, denn zumindest geht der bislang informelle Charakter des innerwissenschaftlichen »Teilens«, jener vom RfII herausgehobene Status der Forschungsdaten als einer zunächst lediglich innerwissenschaftlich gemeinfreien Ressource, im Zuge granularer Prozessstandards und Policies verloren. An die Stelle des bloßen methodengeleiteten Tuns (in welchem Daten ihre funktionale Rolle spielen) tritt eine Art Pflichtenkollision. Denn die Daten sind parallel bereits »Gut«. »Geteilt« werden müssen nun eben doch nicht nur Ergebnisse, sondern bereits die Forschungsressourcen, und dies, je weiter Open Science gehen soll, auch mit Öffentlichkeit und Gesellschaft – es sei denn, man kann sich seitens des Wissenschaftssystems seinerseits auf Rechtspflichten berufen, die dem entgegenstehen: etwa aus dem im DNG genannten Urheberrecht oder einem zum Zweck des Datenzugangs bereits geschlossenen Vertrag mit Datengebern. Die bloße Tatsache der Nutzung zu wissenschaftlichen Zwecken spannt hingegen, wo »Open Science« die Regel ist, keinen Raum der Diskretion mehr auf. In der Terminologie des RfII gesprochen würde der wissenschaftstypische bloße »Zugang« zu Daten sich so womöglich einer Form der »Nutzung« und »Verwertung« angleichen – wenn nicht gar der »Verwendung« von Daten zur »Vermarktung«. Wie ebenso auch die »Öffnung« von Datenbeständen mit einer instantanen Produktform der hierzu geschaffenen Publikate einhergeht – etwa mittels der Vergabe einer »cc«-Lizenz, die schon für den innerwissenschaftlichen Zugang zur quasi normalen, sprich: unvermeidlichen Voraussetzung wird.

12 Siehe den Beitrag von Daniel Lambach in diesem Band.

Praktisch spürbar sind Prozesse dieses Typs beispielsweise im Publikationswesen, das sich unter der Regie von Großverlagen auf alle Redaktions- und Begutachtungsworkflows mit umfassenden Plattformen in einen Vorgang der – stets in irgendeiner Weise bereits lizenzierten – Datenverwertung und -vermarktung transformiert. Aber auch die Durchführung und die Auswertung von Befragungen werden mittels (kommerzieller) Plattformen bereits als voll-verrechtlichter Produktionsvorgang durchgeführt. Auch die Verrechtlichung der sogenannten »Datenspende« durch Einwilligung und Gewährung eines zweckgebundenen Datenzugangs (etwa mittels PIMS, also einem Datenwallet-System, das Einwilligungsmanagement gegebenenfalls an Zahlungen bindet, also eine Verwertung der persönlichen Daten vornimmt) verwandelt die generalisierte Datenhergabe zu einer komplizierten, potenziell fortdauernden Vertragsbeziehung neuer Art.

Was geschieht, wenn in dieser Lage nun die deutsche Bundesregierung ein »Forschungsdatengesetz« plant? Selbst eine Definition von »Forschungsdaten« ist für das Vorhaben bislang nicht bekannt. Da ein Forschungsdatengesetz nicht einfach nur im Stil des DNG als Daten »der« Forschung adressieren kann, dürfte eine Neudefinition aber nötig sein – zumal die Regierung auch ein Gesundheitsdatenutzungsgesetz beschlossen hat, was Abgrenzungsfragen aufwirft. Ob die Regelungsmaterie sich umgekehrt *nur* auf den Datenzugang für die Forschung begrenzen lässt – ob es um eine Art digitalitätsfestes Forschungsprivileg gehen soll – oder aber ob parallel *auch* »Offenheit« (also Datenhergabe durch die Wissenschaft) reguliert werden soll, ist ebenfalls eine spannende Frage. Die Forderung der DFG hierzu lautet, ein etwaiges Forschungsdatengesetz für Deutschland sei »konsequent als ›Datenzugangsgesetz für die Forschung‹« zu konzipieren (DFG 2023, S. 1).[13] Die inzwischen seitens des Bundesministeriums für Bildung und Forschung vorgelegten Eckpunkte für das Regelungsvorhaben (vgl. BMBF 2024) deuten in diese Richtung. Ob das neue Gesetz der im EU-Recht vorgezeichneten Tendenz folgen wird, eine moderierende oder gar genehmigende Stelle in etwaige Zugangsverfahren einzuschalten, ist ebenfalls eine noch offene Frage. Die BMBF-Eckpunkte stellen ein »German Micro Data Center« in Aussicht (vgl. BMBF 2024, S. 3). Die seitens der Ampel-Regierung angekündigte Einrichtung eines »Dateninstituts« ist nicht nur in dieser Hinsicht ebenfalls noch unklar. Man ahnt, dass die Politik sich den Schwierigkeiten der Aufgabe der Schaffung von Datenzugang für die Wis-

13 Vgl. dies unterstützend sowie gegen eine »undifferenzierte Publizitätspflicht«: RfII 2023, S. 9.

senschaft bei gleichzeitiger Herstellung von »Offenheit« der Wissenschaft wohl erst schrittweise bewusst zu werden beginnt.

Die grundsätzlichere Frage danach, was der öffentlich getragenen Wissenschaft durch das Verrechtlichen des wissenschaftsspezifischen Teilens und Nutzens von Daten als solches verloren geht – die Verrechtlichung eines Teilens und Nutzens, das noch gar kein Verwerten oder Vermarkten sein will, aber gemäß den Mustern des Verwertens und Vermarktens verrechtlich wird – ist damit aber noch nicht beantwortet, ja eigentlich noch gar nicht gestellt. Wie passen überhaupt innerwissenschaftliche Allmende und »frei« zugreifender Markt sowie, nennen wir es: *Trust in Science* und *Open Science* zusammen?

3. Weitergehende Überlegungen

3.1 Forschungsdaten als Allmende

Der innerwissenschaftliche Allmende-Charakter von Forschungsdaten korrespondiert zum einen mit der Zünftigkeit akademischen Tuns und knüpft zum anderen auch an die aufklärerische Tradition der Publizität von Forschungsergebnissen an. Publizität bezieht breite Öffentlichkeiten (an Bildung interessierte Köpfe) in das virtuelle Reich der Gelehrsamkeit mit ein. Zum so »allen« angebotenen Wissenserwerb gehört auch das Wissen über »Quellen« und das Zustandekommen von Forschungsergebnissen: »offene« Auskunft umfasst hier auch das Zurverfügungstellen von Berechnungen und von Belegstücken sinnlicher Art. Freilich erfolgte dies nie durch die Übereignung von Belegen an einen Markt, sondern gerade durch deren Zurückbehaltung in der öffentlichen Hand, etwa durch wissenschaftliche Archivierung zur wissenschaftlichen Nutzung oder durch Ausstellung im Sinne eines öffentlichen, aber geschützten Gutes – etwa in Forschungsmuseen. Wissenschaft bringt Wirtschaft also primär durch die Weitergabe von Wissen, nicht aber der wissenschaftseigenen Forschungsressourcen voran. Sie hat vielleicht sogar hinsichtlich dieser Ressourcen eine schützende oder auch eine treuhänderische Funktion.

Heute werden aber eben digitale Daten aus dem öffentlichen Sektor, zu welchem man die Wissenschaft zählt, als sogenannte nicht rivale (nämlich vervielfältigungsfähige) Güter mit der Erwartung verbunden, auch direkt Unternehmen zugänglich gemacht zu werden und somit eine nicht primär

intellektuelle, sondern volkswirtschaftliche Ressource zu sein. Daten sollen somit erstens »publiziert« werden und zweitens auf diesem Wege Unternehmen »offen« zur Verfügung stehen. Man könnte also sagen: Das Leitbild der Allmende wird hier gleich in mehrfacher Hinsicht uminterpretiert. Es geht um »Güter« (nicht um Forschungsvoraussetzungen) und damit auch nicht wirklich um Publizität, sondern um Weitergabe zum Zweck der ökonomischen Verwertung. Ebenso geht es weniger um Einblicke oder Einbeziehung in den innerwissenschaftlichen Prozess als um die Einbeziehung des Datenhandelns der Forschung in Prozesse der Produkt- und Marktgestaltung, also Prozesse unternehmerischen Typs.

Eine rechtlich verfasste *Openness* beruht also vielleicht von der Wissenschaft her gesehen auf der Illusion, das Modell des innerwissenschaftlichen Teilens von Wissen, Information (und dann eben auch: Daten) ließe sich auf eine Weltgesellschaft ausdehnen, die primär die Wirtschaft, des Weiteren die politische Administration und alle weiteren erdenklichen Akteure mit umfasst. Aus wirtschaftspolitischer Sicht schafft *Openness* jedoch vor allem eine global frei zugängliche – und auch der Aneignung fähige – Ressource. Der Allmendecharakter von *Open Science* muss daher durch Lizenzen sogar aktiv erst hergestellt werden, will man das freie Zirkulieren von Wissen, das wir mit Publizität assoziieren, auf der Ebene von Daten garantieren. Mehr schlecht als recht – weil nicht wirklich rechtssicher und zudem unter Umständen auch wieder OA-Großverlage begünstigend – ist derzeit das System der »CC«-Lizenzen zum Standard nicht nur für »offene« Kreativprodukte, sondern auch für die Lizenzierung früher urheberrechtlich geschützter Forschungsergebnisse geworden. Vom Verlust der innerwissenschaftlichen Freiräume ist schon die Rede gewesen. Verschärfend ließe sich aber auch die Diagnose stellen, dass es eine digitale Allmende in Wahrheit weder gibt noch geben kann, solange man digitale Güter als »nicht rival« (und damit streng genommen noch nicht einmal einer Allmende bedürftig) behandelt – und dass digitale Forschungsdaten darüber hinaus zumindest an der Systemgrenze Wissenschaft/Wirtschaft auch durchaus »rivale« Güter sein können, so wie sie es schon im innerwissenschaftlichen Wettbewerb latent bleiben.

Wie immer sich die Lage in konkreten wissenschaftlichen Datendomänen darstellt: »Offene« Wissenschaft oder auch offene Forschungsdatenbestände formen jedenfalls nicht schlichtweg aus den Gegenständen wissenschaftlichen Datenhandelns eine unproblematische Allmende »für alle«. Eher schon wird hier ein neuer Typ von Immaterialgut geschaffen, welches die Wissenschaft für die Wirtschaft der digitalisierten Gesellschaft

bereitzustellen oder auch zu produzieren und zur Verfügung zu stellen hat.[14]

As open as possible, as closed as necessary[15] – das ist eine der Formeln, mittels welcher sich das klassische (nämlich letztlich informellen, jedenfalls nicht verrechtlichten, etwa klagbaren, Regeln bedienende) Forschungsdatenmanagement einer wissenschaftsgemäßen Version von »Openness« versichert. Ob hier nicht doch irgendwann ein strengeres, der Wissenschaft von außen auferlegtes Regime folgen wird, bleibt abzuwarten.

3.2 Digitaler Zwilling – oder: intermediäre Artefakte am Kreuzungspunkt des Datenteilens *aus* der und *für* die Wissenschaft?

Ob ein Forschungsdatengesetz für Deutschland wirklich kommen wird, ist ebenso noch nicht klar. Sicher ist aber, dass auch andersartige Regelwerke einer datengetriebenen Forschung (Praxis-Standards, *soft law*, Ethik) nicht umhinkommen werden, für die Schnittstelle zwischen den Sozialsystemen Wissenschaft und Wirtschaft Festlegungen zu treffen, die über Leitbilder wie »Offenheit« hinausgehen. Vor jener Doppeltendenz einerseits der sehr frühen Preisgabe und Kommerzialisierung von Forschungsdaten *aus* der Wissenschaft und andererseits dem Rückbau von Datenzugangsprivilegien *für* sie habe ich gewarnt. Einerseits droht hier eine Preisgabe von Freiräumen, ohne die Wissenschaft nicht so produktiv sein kann, wie die Gesellschaft es von hier erwartet. Andererseits ist aber auch – wo Daten grundsätzlich nur entweder allen zur Verfügung stehen oder gekauft werden müssen – eine Preisspirale für den Kauf wirklich gehaltvoller Daten nicht unwahrscheinlich, und die Hochschulen sowie andere wissenschaftliche Einrichtungen werden zu den ersten gehören, die teure Daten nicht mehr bezahlen können. Nicht nur die Unzugänglichkeit von Daten, sondern auch das Szenario einer vollständigen Kommerzialisierung von Datenzugriffen fügt den Freiheitsräumen großen Schaden zu, um derentwillen es Bildung und Wissenschaft überhaupt gibt.

---

14 Es passt hierzu, dass es auf Seiten der Wissenschaft als ratsam erkannt worden ist, Forschungsprimärdaten nicht »einfach so« zu öffnen, sondern im Rahmen von *Open Science* zur Weitergabe an Wirtschaft oder Gesellschaft geeignete »Datenprodukte« zu schaffen, welche gewissermaßen didaktisch aufbereitet sind und die spezifische wissenschaftliche Qualität (nämlich: eine kunstgerechte Nutzbarkeit) der Daten sicherstellen (vgl. RfII [2]2019).

15 Vgl. http://eare.eu/open-data/ [12.7.2024].

Es liegt nahe, zur Moderation eines inter-systemischen Interessensausgleichs nicht nur an Gesetze, die Regeln festlegen, sondern auch an Organisationslösungen zu denken, die stärker auf Aushandlungsprozesse setzen. So werden neutrale sogenannte »neue Intermediäre«[16] nicht nur für Datenmärkte ganz generell diskutiert, sondern auch spezifische Datentreuhandmodelle für Forschungsdatenzentren entwickelt.[17] Ob dies gelingt dürfte freilich davon abhängen, ob hinreichend robuste Vertragswerke alle kritischen Punkte (Verwertung, Haftung, Fortbestand des Zugangs) belastbar absichern. Es wird also der (aus Sicht der an niedrigschwelliges, informelles Teilen gewöhnten Wissenschaft bedauerliche) Preis der unter Punkt 2 angesprochenen Verrechtlichung zu zahlen sein.

Mit dem Beitrag von Malte Gruber und Zaïra Zihlmann wird zudem eine noch einmal etwas andere Form des – zumindest möglichen – Rückbaus von Interessenskonflikten an der Grenze Wissenschaft/Wirtschaft (oder auch Wissenschaft/Gesellschaft) denkbar: Genuine Schutzrechte (wohlmöglich sogar »subjektive« Rechte) für sogenannte digitale »Zwillinge« könnten ebenfalls die Rolle einer intermediären Instanz übernehmen.[18] Sowohl personenbezogene als auch gruppenbezogene Datenbestände – vielleicht aber auch Datensammlungen, die für die Wissenschaft eine Schlüsselrolle spielen, etwa sogenannte Referenzkorpora für ganze Forschungsgebiete – wären dann nicht einfach eine beliebig nutzbare Allmende, sondern zugleich in einem näher zu bestimmenden Sinne in ihrer Integrität zu respektieren. Die Metapher des »Körpers« muss hierbei nicht nur auf Medizindaten oder physiologische Daten von Lebewesen begrenzt bleiben. Sondern schützenswerte (virtuelle) »Körper« könnten durchaus dem Wort nach beispielsweise auch die digitalen Zwillinge von Kulturgütern, große Sammlungen von Umwelt- und Biodiversitätsdaten oder auch wissenschaftlich aufbereitete, standardisierte, nachhaltig gepflegte (und dadurch unikale) erd- und klimawissenschaftliche Datensammlungen oder Datenarchive sein.

Wird allerdings das Angebot gemeinschaftlich respektierter, gleichsam als solcher eine neue, zu respektierende Integrität »verkörpernder« digitaler Artefakte auch zu einem entsprechenden – ja ebenfalls neuartigen –

16 Mit dem Data Governance Act (DGA) hat die EU rechtspolitisch einen Anreiz zur Schaffung solcher Entitäten geschaffen.

17 Das deutsche Bundesministerium für Forschung (BMBF) hat in diesem Feld in den letzten Jahren mehrere Projektförderlinien ausgeschrieben.

18 Ich spinne hier eine Idee von Malte Gruber – mit Dank – ein wenig weiter.

Rechtsschutz führen? Hier sind allenfalls Spekulationen möglich, und es ist noch nicht einmal zu sagen, ab wann wohl eine derartige Fragestellung ernstlich in forschungspolitische und juristische Debatten Eingang finden werden wird.

3.3 Daten – Information – Wissen

Digitalpolitik gleitet, so scheint es jedenfalls, zwischen verschiedenen Deutungen digitaler Prozesse hin und her. Teils behandelt man »Daten« wie »Information«, teils wie »Güter«, teils als »Wissen«, teils werden sie als unterschiedsloser Bestandteil digitaler »Prozesse« (oder auch funktionierender Algorithmik) thematisiert. Ebenso schwanken Aussagen über Forschungsdaten zwischen einem funktionalen Datenbegriff, der auf die wissenschaftsspezifische Rolle von Daten für den methodengeleiteten Erkenntnisgewinn abzielt (so die Definition im DNG), und einer substanzhaften Vorstellung von Daten als intrinsisch bereits (auch ökonomisch und lebensweltlich) werthaltigem »Rohstoff«, einem »Gut« oder einer »Ressource«.

Dieses Schwanken zwischen Abstraktion und Stofflichkeits-Denken ist keineswegs wirklich metaphorisch, denn ein »wörtlicheres« oder irgendwie vereindeutigtes Datenverständnis gibt es nicht. Das Schwanken lässt sich auch nicht einfach abstreifen, sondern es beschreibt eine Mehrfachbetrachtung in der Sache: Man fasst Digitalität tatsächlich mal so, mal so auf. Und betroffen ist dann nicht nur die Rede über Daten, sondern auch diejenige über Information oder Wissen: Auch diese stellte man sich zeitweilig stoffartig vor. Bevor man von den Daten als dem *neuen Öl* (nämlich Rohöl) gesprochen hat, gab es schon die Vorstellung von der »Information«, die gleichsam durch die Informationsgesellschaft »strömt«, sowie vom »Wissen«, welches die durch Vernetzung steigerbare Ressource der »Wissensgesellschaft« sei.

Die Trias »Wissen – Information – Daten« entstammt der Informationswissenschaft, zählt inzwischen aber auch zu den vermeintlich ausgehärteten, ausgehend von den »Daten« als eine Art Basis pyramiden- oder stufenartig hierarchisierten Grundbegriffen des interdisziplinären Anwendungsfaches *Data Science*.[19] Es könnte eine Nebenfolge des inneren Schwankens

19 Der wissenschaftstheoretische Status von Data Science ist ähnlich unklar wie die dazugehörigen Erläuterungen. Hier ein Beispiel aus dem Portal *Schlüsselbegriffe der Digitalisierung* der Bun-

der drei Großbegriffe sein, dass man sie neben der Suggestion einer festen Ordnung, in der sie zueinander stehen, so behandelt hat, als ließen sie sich verlustfrei ineinander überführen: Wissen besteht aus Information und Information aus Daten, ergo wären Daten gleichsam feinpixeliges Wissen und umgekehrt viele Daten auch viel Wissen (weil viel Information). Ähnlich scheinen dann die »Offenheit« von Daten und diejenige von Information wie auch Wissen irgendwie das Gleiche zu sein.

Weiß man von daher im Bereich politischer Steuerungsversuche für den Umgang mit Forschungsdaten, ob man überhaupt von »Daten« sprechen möchte, wo man »Daten« sagt? Wird womöglich von »offenen Daten« gesprochen, obwohl man eigentlich frei zirkulierendes Wissen meint – oder haben, anders ausgedrückt, an »Daten« interessierte Akteure eine Offenheitsforderung auf Daten ausgedehnt, die eigentlich nur im Bereich des Wissens legitim ist? Noch einmal anders gefragt: Ist die Vorstellung, Daten könnten und sollten genau in der Weise »für alle da sein« wie auch die Information (aus Informationssystemen) oder das Wissen (der Wissenschaft) »allen« zur Verfügung stehen sollte und potenziell »allen« nützt?

Zweifel scheinen angebracht. Wie man den Schutz von (kritischen) Informationen nicht einfach mit dem Schutz (digitaler) Daten gleichsetzen kann, ist auch die Ineinssetzung von Daten und Wissen naiv – wobei in der Annahme einer Trennbarkeit von Forschungsdaten und Wissen ebenso eine Fehlvorstellung steckt, die für das Wissenschaftssystem gefährlich ist. Wer digitale Daten »hat«, kann aus diesen Informationen gewinnen und (so man letztere methodisch be- und verarbeitet) möglicherweise auch wissenschaftlich gehärtetes Wissen. Digitale Daten allein »sagen« jedoch zunächst einmal nur Maschinenprozessen etwas, so dass man im Grunde – politisch alles andere als trivial – eine Art Infrastruktur-Apriori überspringt, wenn man die Daten der Wissenschaft mit deren Wissen (oder überhaupt etwas Wissenschaftsspezifischem) identifiziert. Ohne Metadaten keine Daten; oder: keine Daten ohne sogenannte »Ontologie«; oder: Daten bedürfen der Kontextualisierung – Aussagen wie diese drücken von daher ein Problem aus, dem sich auch ein mögliches Forschungsdatengesetz stellen muss. Es

---

desregierung: »Data Science (Datenwissenschaft) ist eine angewandte, interdisziplinäre Wissenschaft, die das Ziel verfolgt, *Wissen* aus *Daten* zu generieren, um *Informationen* zu filtern, *Prozesse* zu automatisieren und *Entscheidungen* zu optimieren.« https://www.bundesregierung.de/breg-de/themen/digitalisierung/digitale-schluesselbegriffe-kurz-erklaert-2127606 [2.11.2023] – Hervorhebungen von mir, pgg.

spricht in seinem Titel eben gerade nicht von Wissen oder auch nur von Information, sondern lediglich von deren Teil-Äquivalenten im maschinellen Kontext.

Das wiederum heißt dennoch nicht, dass man die »Daten« quasi schon vor der Klammer der Wissensproduktion folgenlos aus dem Wissenschaftssystem herausziehen oder herauskopieren kann. Vielmehr würde eine verfrühte und ungefilterte Appropriation und Vermarktung (wie auch die Effekte einer Verrechtlichung, die »wilder« Appropriation wie auch Barrieren des Datenzugangs zur Rückgewinnung wissenschaftlicher Spielräume entgegenwirken will) durchaus die Grundlagen und die Autonomie der wissenschaftlichen Informationsgewinnung und Wissensarbeit zerstören. Das Datenhandeln der Forschung ist ja seinerseits in fragiler Weise wettbewerblich – und auch dieser Wettbewerb braucht Schutz: Schutz vor Verzerrungen, Einflussnahme, Entwertung. An der Stelle, an welcher die Daten aus einer offenen Wissenschaft abgeflossen sind, »fehlen« sie zwar nicht *als Daten*. Es steht aber infrage, was sie – *als Information* mit eigenständigem Neuigkeitswert betrachtet – für die Welt des wissenschaftlichen Wissens (noch) erbringen können. Denn Information verschwindet zwar durch Weitergabe nicht völlig, verändert aber, anders als man es von Daten sagen würden, mit der Weitergabe ihren Charakter und ihren Wert.

Offenheit bleibt auch in dieser Hinsicht eine nicht nur suggestive, sondern auch durch ein Übermaß an Vagheit irreführende Losung. Von daher wäre es dringend zu wünschen, nicht allein die Forderung nach offenen Daten oder offener Wissenschaft zu erheben, sondern auch darüber zu diskutieren, welche Informationshoheit, welche genuinen Produktionsmittel (etwa Daten und eigenständige Verfahren und Infrastrukturen zur Datenverarbeitung) sowie welche Informationsressourcen die Wissenschaft benötigt, um ein nach wie vor wirklich wissenschaftlich zu nennendes Wissen zu produzieren.

Literatur

BMBF [= Bundesministerium für Bildung und Forschung] (2024): *Eckpunkte BMBF Forschungsdatengesetz*, https://www.bmbf.de/SharedDocs/Downloads/de/2024/240306_eckpunktepapier-forschungsdaten.html [23.3.2024].

DFG [= Deutsche Forschungsgemeinschaft] (2023): *Die Wissenschaft braucht ein Forschungsdatengesetz! Positionierung der Deutschen Forschungsgemeinschaft (DFG)*, Bonn, https://www.dfg.de/download/pdf/foerderung/grundlagen_dfg_foerderung/forschungsdaten/stellungnahme_forschungsdatengesetz.pdf [23.3.2024].

DFG [= Deutsche Forschungsgemeinschaft] (2022): *Open Science als Teil der Forschungskultur. Positionierung der Deutschen Forschungsgemeinschaft*, https://zenodo.org/records/7193838 [20.4.2024].

Digital Science/Springer Nature/Figshare (Hg.) (2023): *The State of Open Data 2023. Global attitudes towards open data*, https://digitalscience.figshare.com/articles/report/The_State_of_Open_Data_2023/24428194 [23.3.2024].

Parsons, Mark A./Fox, Peter A. (2013): Is Data Publication the Right Metaphor?, in: *Data Science Journal*, Special Issue 12, S. 32–46.

RatSWD [= Rat für Sozial- und Wirtschaftsdaten] (2023): *Forschungsdatengesetz: Was zentral ist*, https://www.konsortswd.de/wp-content/uploads/RatSWD_Positionspapier_Forschungsdatengesetz_Was_zentral_ist.pdf [23.3.2024].

RatSWD (2022): *Positionspapier des RatSWD: Eckpunkte für ein Forschungsdatengesetz*, 14.6.2022, https://www.konsortswd.de/wp-content/uploads/RatSWD-Positionspapier-Eckpunkte-fuer-ein-Forschungsdatengesetz.pdf [23.3.2024].

RfII [= Rat für Informationsinfrastrukturen] (2023): *Anforderungen an die Ausgestaltung eines Forschungsdatengesetzes und eines Dateninstituts*, Göttingen, https://rfii.de/download/rfii-diskussionsimpuls-forschungsdatengesetz-2023/ [23.3.2024].

RfII (2021): *Nutzung und Verwertung von Daten im wissenschaftlichen Raum. Empfehlungen zur Ausgestaltung von Datendiensten an der Schnittstelle von Wissenschaft und Wirtschaft*, Göttingen, https://rfii.de/download/nutzung-und-verwertung-von-daten-im-wissenschaftlichen-raum-september-2021/ [23.3.2024].

RfII (2019): *Herausforderung Datenqualität – Empfehlungen zur Zukunftsfähigkeit von Forschung im digitalen Wandel*, zweite Auflage, Göttingen, https://rfii.de/download/herausforderung-datenqualitaet-november-2019/ [23.3.2024].

Specht-Riemenschneider, Louisa (2021): *Studie zur Regulierung eines privilegierten Zugangs zu Daten für Wissenschaft und Forschung durch die regulatorische Verankerung von Forschungsklauseln in den Sektoren Gesundheit, Online-Wirtschaft, Energie und Mobilität*, https://www.jura.uni-bonn.de/fileadmin/Fachbereich_Rechtswissenschaft/Einrichtungen/Lehrstuehle/Specht/Dateien/2021-08-25-LSR.pdf [23.3.2024].

UNESCO (2021): *UNESCO Recommendation on Open Science*, https://unesdoc.unesco.org/ark:/48223/pf0000379949.locale=en [23.3.2024].

WR [= Wissenschaftsrat] (2022): *Empfehlungen zur Transformation des wissenschaftlichen Publizierens zu Open Access*, Köln, https://www.wissenschaftsrat.de/download/2022/9477-22.html [23.3.2024].

WR (2020): *Zum Wandel in den Wissenschaften durch datenintensive Forschung*, Köln, https://www.wissenschaftsrat.de/download/2020/8667-20.html [23.3.2024].

Big-Tech-Data: Zugangsnotwendigkeit und Zugangsausgestaltung nach dem Digital Markets Act[1]

Lars Pfeiffer

I. Einleitung

Wir bewegen uns heute in einer »Welt überbordender Datenmengen«[2] und ein Großteil dieser Daten – so die Europäische Kommission – befindet sich »derzeit in der Hand einer kleinen Zahl großer Technologieunternehmen.«[3] Unrecht hat sie damit vermutlich nicht, wie einzelne Kennzahlen veranschaulichen: So waren im Jahr 2021 mit Google, Facebook, Netflix, Apple, Amazon und Microsoft lediglich sechs Unternehmen für über die Hälfte des gesamten weltweiten Netzwerkverkehrs (mit)verantwortlich.[4] Google Search vereint circa 91,5 Prozent des weltweiten Markts für Suchmaschinen auf sich[5] und verarbeitet dabei rund 6,3 Millionen Suchanfragen in der Minute.[6] Die Video-Sharing-Plattform YouTube – ebenfalls in der Hand von Google – wurde im November 2023 31,4 Milliarden Mal besucht.[7] Der weltweit größte Online-Marktplatz Amazon verbucht jeden Monat weit über zwei Milliarden Webseiten-Besuche[8] und auch die Marken des Meta-Konzerns können mit beeindruckenden Zahlen aufwarten: So konnte Facebook im letzten Quartal 2023 täglich durchschnittlich 2,11 Milliarden aktive Nutzer aufweisen[9]

1 Dieser Beitrag ist sowohl aus der Mitwirkung des Autors in der ZEVEDI-Projektgruppe »Datenzugangsregeln« als auch aus der Mitarbeit in dem vom Bundesministerium für Bildung und Forschung (BMBF) geförderten Projekt »Privatsphärenfreundliche Geschäftsmodelle für die Plattformökonomie (PERISCOPE)« (FKZ: 16KIS1481) entstanden.

2 Schweitzer 2019a, S. 569.

3 Europäische Kommission 2020a, S. 3.

4 Fitri 2022.

5 Statista.com 2024a.

6 Statista.com 2024b.

7 Statista.com 2024c.

8 Statista.com 2024d.

9 Statista.com 2024e.

und im Oktober 2020 wurden weltweit täglich 100 Milliarden Nachrichten über den Kurznachrichtendienst WhatsApp ausgetauscht.[10] Entscheidend bei der Kenntnisnahme solcher Zahlen ist deren Kontextualisierung mit der Funktionsweise der Daten- und Aufmerksamkeitsökonomie. Jeder Webseitenbesuch, jede Suchanfrage, jede versendete Nachricht, jede abgeschlossene Transaktion und jeder Videoaufruf bedeuten für den jeweils verwendeten Dienst ein Mehr an Aktivität und Nutzungszeit und damit auch einen Zuwachs von Nutzungsdaten, die wiederum gewinnbringend zur Verbesserung bestehender sowie auch zur Entwicklung neuer Dienste genutzt werden (können). Diese »Datenschätze« der digitalen Plattformen unterliegen in der Regel dem faktisch exklusiven Zugriff des Plattformbetreibers und diejenigen, die durch ihre Nutzung der Plattform maßgeblich zur Generierung der Daten beitragen, profitieren davon regelmäßig nicht.[11] Wegen der zunehmenden Bedeutung von Daten als notwendigem Input für datenbasierte Geschäftsmodelle ergeben sich daraus negative Auswirkungen auf private Nutzer, gewerbliche Nutzer sowie Wettbewerber digitaler Plattformen, weshalb sich der europäische Gesetzgeber mit dem Erlass der Verordnung (EU) 2022/1925 vom 14. September 2022 über bestreitbare und faire Märkte im digitalen Sektor und zur Änderung der Richtlinien (EU) 2019/1937 und (EU) 2020/1828 (Gesetz über digitale Märkte; im Folgenden: Digital Markets Act (DMA)) unter anderem für die Einführung gesetzlich normierter Datenzugangsansprüche entschieden hat.

Der Schwerpunkt dieses Beitrags liegt in der Betrachtung, welche Datenzugangsansprüche zu wessen Gunsten und zu wessen Lasten Einzug in die Verordnung gefunden haben, welches – zumindest in dem Ausmaß regelmäßig plattformspezifische – Problemfeld mit den jeweiligen Ansprüchen adressiert wird, ob das jeweils gewählte Vorgehen erfolgsversprechend zu sein scheint sowie darin, welche Hürden und offenen Fragen sich bei der Geltendmachung und der Umsetzung der Zugangsansprüche ergeben.[12] Zur besseren Nachvollziehbarkeit dieser Betrachtungen erfolgt in Abschnitt II zunächst eine Analyse der ökonomischen Besonderheiten digitaler Plattformen, ihren Datennutzungsinteressen und Datenzugangs-

10 Statista.com 2024 f.

11 Vgl. Wischmeyer/Herzog 2020, S. 288.

12 Dieser Beitrag vertieft mit Fokus auf den DMA die vom Autor an anderer Stelle veröffentlichten, übersichtsartigen Ausführungen zu den insgesamt in den neuen plattformspezifischen Rechtsakten der EU enthaltenen datenzugangsbezogenen Vorschriften in der Plattformökonomie, siehe dazu Pfeiffer 2024.

vorteilen sowie den datenbezogenen Marktmachtmissbrauchspotentialen und -anreizen, die sich für bestimmte Arten digitaler Plattformen ergeben. Insgesamt zielt dieser Beitrag also darauf ab, die unterschiedlichen Facetten von datenzugangsbezogenen Fragen, die in diesem Sammelband adressiert werden, um eine Perspektive anzureichern, die sich der Referenzmaterie des Datenzugangs bei marktbeherrschenden digitalen Plattformen vor dem Hintergrund des DMA widmet.

II. Digitale Plattformen und Daten

Digitale Plattformen vereinfachen oder ermöglichen die Interaktion zwischen zwei oder mehr getrennten, dennoch voneinander abhängigen Nutzergruppen, die miteinander durch den jeweils von der Plattform erbrachten Dienst über das Internet verbunden sind.[13] Zwar können sie in zahlreiche unterschiedliche Arten unterteilt werden,[14] ihr einendes Element bleibt jedoch ihre Vermittlungsfunktion.[15] Welche Marktteilnehmer miteinander in Verbindung gebracht werden und welcher Natur – technisch, kommerziell oder sozial[16] – die jeweils ermöglichte Interaktion ist, ist dabei irrelevant. Entscheidend ist die Reduktion der bei der Etablierung eines solchen Austauschs entstehenden Transaktionskosten[17] und der sich daraus ergebende Mehrwert für die unterschiedlichen Plattformnutzer, die vormals wegen zu hoher Transaktionskosten nicht miteinander in Verbindung getreten sind.[18]

1. Eigenschaften digitaler Plattformen

Wohl beginnend mit den Arbeiten aus dem Jahr 1985 von *Katz* und *Shapiro* zu Netzwerkeffekten und deren wettbewerblichen Implikationen,[19] besteht

13 Definition in Anlehnung an OECD 2019, S. 21; ähnlich Kieß 2023, S. 74.
14 Siehe beispielhaft die unterschiedlichen Ansätze von Hein/Böhm/Krcmar 2019, S. 183; Greiner/Teubner/Weinhardt 2018, S. 59.
15 Schweitzer/Fetzer/Peitz 2016, S. 4.
16 Vgl. Engert 2018, S. 305.
17 Siehe dazu Gasser 2021, S. 37.
18 Evans/Schmalensee 2013, S. 2.
19 Katz/Shapiro 1985.

in der wirtschaftswissenschaftlichen Literatur mittlerweile weitestgehend Konsens bezüglich der wesentlichen ökonomischen Charakteristika, die alle digitalen Plattformen typischerweise kennzeichnen. Aufbauend auf der oben vorgenommenen Begriffsbestimmung ist zunächst die Zwei- oder Mehrseitigkeit der von den Betreibern digitaler Plattformen bedienten Märkte hervorzuheben.[20] Darunter ist der Umstand zu verstehen, dass der Nutzen, den eine Marktseite aus der Plattformnutzung gewinnt, von der Anzahl der Teilnehmer auf der anderen Marktseite abhängt.[21] Verdeutlicht am Beispiel eines Markplatzes für mobile Anwendungen bedeutet das: Der Nutzen, der für Endanwender, die auf der Suche nach neuen Anwendungen sind, mit der Verwendung eines bestimmten App Stores einhergeht, wird vor allem durch die Anzahl der Entwickler unterschiedlicher Anwendungen beeinflusst. Damit zusammenhängend ist als nächste wesentliche Eigenschaft digitaler Plattformen das Vorliegen von Netzwerkeffekten zu nennen.[22] Bei diesen Effekten ist zu differenzieren zwischen direkten und indirekten Netzwerkeffekten.[23] Direkte Netzwerkeffekte beschreiben Situationen, in denen der Mehrwert einer Plattformnutzung für den Akteur einer Marktseite von der Anzahl der Akteure auf derselben Marktseite abhängt.[24] Indirekte Netzwerkeffekte liegen hingegen dann vor, wenn der Mehrwert der Plattformnutzung von der Anzahl der Akteure auf der anderen Marktseite abhängt.[25] Da die unterschiedlichen Marktseiten miteinander effizient in Verbindung gebracht werden wollen, hat bei Plattformgeschäftsmodellen zugleich auch ein Wandel der Wertschöpfungsstrategien stattgefunden. Während vormals produktzentrierte Strategien im Vordergrund standen, werden nunmehr plattformzentrierte Wertschöpfungsstrategien verfolgt,[26] womit der Fokus auf die Generierung möglichst vieler Interaktionen und Aktivitäten gelegt wird.[27]

Um sicherzustellen, dass die Interaktionen der unterschiedlichen Marktseiten auch tatsächlich über die eigene Plattform und nicht über

20 Teilweise auch als die »ökonomische Basis« digitaler Plattformen bezeichnet, vgl. Hein/Böhm/Krcmar 2019, S. 187.

21 Ausführlich dazu Armstrong 2006, S. 668; Rysman 2009, S. 125.

22 OECD 2019, S. 22.

23 Motta/Peitz 2020, S. 10 ff.; Schweitzer/Fetzer/Peitz 2016, S. 4.

24 Schweitzer/Fetzer/Peitz 2016, S. 4; Motta/Peitz 2020, S. 10; so auch bereits Katz/Shapiro 1985, S. 424.

25 Caillaud/Julien 2003, S. 309 f.; Schweitzer/Fetzer/Peitz 2016, S. 4 f.

26 Hein/Böhm/Krcmar 2019, S. 182.

27 Jaekel 2017, S. 113 ff.

Dritte erfolgen, ist für Plattformbetreiber darüber hinaus deren Fähigkeit zur Verhinderung von Multi-Homing durch die Nutzer relevant, also der Parallelnutzung mehrerer Plattformen zu demselben Zweck.[28] Während das Vorliegen von Wechselbewegungen zwischen verschiedenen Plattformen für eine höhere Wettbewerbsintensität auf dem jeweiligen Markt spricht, lässt ein Mangel derselben in der Regel auf einen weitestgehend monopolisierten Markt schließen.[29] Ob ein Nutzer mehrere unterschiedliche Plattformen zu demselben oder zumindest ähnlichen Zweck in Anspruch nimmt, hängt maßgeblich von den damit einhergehenden Wechselkosten ab.[30] Diese Kosten sind nicht rein pekuniär zu verstehen, sondern vielmehr als sämtlicher Aufwand und sämtlicher Nutzenverlust, der mit der Abkehr von einer Plattform einhergeht.[31] Auch der mit einem Dienstwechsel regelmäßig verbundene Datenverlust – im Fall von sozialen Netzwerken beispielsweise der Verlust der gesamten »virtuellen Einrichtung"[32] oder im Fall von Plattformen, bei denen Reputationssysteme eine wesentliche Rolle spielen (etwa Verkäuferbewertungen auf Transaktionsplattformen), der Verlust bislang gesammelter Bewertungen[33] – stellt eine Form der Wechselkosten dar. Ist die Summe der subjektiv wahrgenommenen Wechselkosten ausreichend hoch, kann sich für die Nutzer ein Lock-In-Effekt ergeben: Sie finden sich in einem Abhängigkeitsverhältnis zu einer bestimmten Plattform wieder, dem sie nicht mehr – zumindest ohne signifikante Nachteile in Kauf zu nehmen – entkommen können.[34] Erschwerend kommt zudem die Wirkungsweise der Netzwerkeffekte hinzu, denn diese bestimmen maßgeblich den Nutzen, der sich aus der Plattformnutzung für einen Teilnehmer ergibt. Um von der Nutzung einer neuen Plattform zumindest in einem der Nutzung der vorherigen Plattform vergleichbaren Maß profitieren zu können, müssen sich die Plattformnutzer daher als Gruppe(n) koordiniert für einen Plattformwechsel entscheiden. Insofern verstärken sich Netzwerkeffekte und Wechselkosten gegenseitig.[35]

28 Siehe dazu Dewenter/Linder 2017, S. 75.
29 Ausführlich dazu Louven 2019, S. 779, Rn. 21 ff.
30 Dewenter/Linder 2017, S. 75.
31 Ausführlich dazu Nocun 2018, S. 53.
32 Ebd.; siehe auch OECD 2019, S. 24.
33 Bamberger/Lobel 2017, S. 1067.
34 Nocun 2018, S. 54.
35 Bamberger/Lobel 2017, S. 1068 f.

2. Datennutzungsinteressen, Datenzugangsvorteile und datenzugangsbezogener Machtmissbrauch

Wie für die gesamte Digitalwirtschaft zu konstatieren, gilt auch und insbesondere für digitale Plattformen, dass der Zugriff auf und die Fähigkeit zur Auswertung von große(n) Datenmengen (mit)entscheidend für ihren ökonomischen Erfolg ist. Im Vordergrund stehen dabei in erster Linie die Nutzungsdaten aller auf einer Plattform beteiligten Akteure.[36] Aus diesen Daten werden – maßgeblich abhängig vom jeweiligen Geschäftsmodell und damit auch der Monetarisierungsstrategie[37] – Erkenntnisse abgeleitet, um Geschäftsprozesse zu verbessern, Risiken zu reduzieren, Marktmacht auszuweiten und Innovationen zu heben.[38]

Aus der Position der Plattformbetreiber als Vermittler und Infrastrukturbereitsteller resultieren signifikante Datenzugangsvorteile.[39] Unabhängig davon ob beispielsweise Suchmaschinenanfragen durchgeführt, über Online-Marktplätze Transaktionen abgeschlossen oder Filme und Musik über Streamingdienste und Videoplattformen aufgerufen werden: die Betreiber digitaler Plattformen sind in der Lage, sämtliches Verhalten der auf ihrer Plattform aktiven Akteure zu erfassen, darauf aufbauend Erkenntnisse zu positiven wie auch negativen Markttrends, gesamtgesellschaftlichen Interessenslagen, erfolgreichen und minder erfolgreichen Werbestrategien u. v. m. abzuleiten und in der Folge vielversprechendere strategische Wege einzuschlagen. Den gewerblichen Nutzern digitaler Plattformen stehen diese datenbasierten Erkenntnismöglichkeiten regelmäßig nicht oder nur sehr eingeschränkt zur Verfügung. Wegen faktischer Zwänge zur Nutzung digitaler Plattformen – etwa weil eine bestimmte Plattform als einziges Zugangstor zu einer bestimmten Kunden- bzw. Nutzergruppe dient – können gewerbliche Nutzer nicht anders, als sich bei der Frage nach eigenen Datenzugangsmöglichkeiten den Regeln des Plattformbetreibers zu unterwerfen.[40] Zwar können diese durch den Plattformbetreiber gesetzten Regeln durchaus auch eine Offenlegung bestimmter Daten zugute der Plattformnutzer umfassen: So wird in der Literatur zu Recht darauf hingewiesen,

36 So unter anderen Crémer/de Montjoye/Schweitzer 2019, S. 25.

37 Siehe dazu Kieß 2023, S. 78 f.

38 Vgl. Veldkamp 2023, S. 1547.

39 Busch 2019, S. 794.

40 Zutreffend ist daher unter diesen Umständen die Bezeichnung der digitalen Plattformen als »private Gesetzgeber«, vgl. Schweitzer 2019b, S. 1; siehe dazu auch Hoffer/Lehr 2019, S. 19.

dass es unter Umständen auch im wirtschaftlichen Eigeninteresse der Plattformbetreiber liegen kann, Dritten einen Zugang zu Daten einzuräumen, die eigentlich ihrem eigenen, faktisch exklusiven Zugriff unterliegen. Befinden sich Plattformbetreiber in einem kompetitiven Markt und gehört die Bereitstellung bestimmter Datensätze zum Werteversprechen gegenüber ihren gewerblichen Nutzern, so muss sich dieses datenpreisgabebezogene Werteversprechen an dem der Wettbewerber messen lassen, anderenfalls schließen sich die Nutzer einer anderen Plattform mit für sie vorteilhafterem Werteversprechen an.[41] Mangelt es in dem betrachteten Markt allerdings an einem wirksamen Wettbewerb, entfällt dieser korrigierende Einflussparameter – eine Vergleichbarkeit mit anderen Diensten ist nicht gegeben und insofern findet auch keine »Sanktionierung« durch Abwanderung der Nutzer statt.[42]

Die vorteilhaften Datenzugangsmöglichkeiten der Plattformbetreiber stehen zudem in einer engen Wechselwirkung mit den im vorherigen Abschnitt beschriebenen Plattformcharakteristika. Dieses Phänomen, das regelmäßig anhand von Umschreibungen wie »Daten-Netzwerkeffekte«[43], »Nutzer-Rückkopplungsschleife und […] Monetarisierungs-Rückkopplungsschleife«[44] oder auch »datengetriebene indirekte Netzwerkeffekte«[45] skizziert wird, beschreibt kurz gefasst Folgendes: Die umfassenden Datenzugriffs- und -nutzungsmöglichkeiten ermöglichen den Plattformbetreibern die (Fort-)Entwicklung besserer Dienste und Produkte. Dies ist in der Regel gleichzusetzen mit einer Nutzensteigerung für die Plattformnutzer, womit sich für bestehende Nutzer die Anreize zum Verlassen der Plattform verringern, da sie mit höheren Wechselkosten konfrontiert sind bzw. – anders ausgedrückt – sich stärkeren Lock-In-Effekten ausgesetzt sehen. Neben der intensivierten Bindung bereits existierender Nutzer sorgen die verbesserten Dienste zugleich für die Generierung neuer Nutzer. Mehr Nutzer und mehr auf den Diensten verbrachte Nutzungszeit führen wiederum zu gesteigerten Datenaufkommen, womit man wieder am Ausgangspunkt der Schleife angekommen ist. Im Ergebnis führt diese Wechselwirkung zur Intensivierung der ohnehin bestehenden Monopolisierungstendenzen auf

41 Vgl. Gineikyte/Barcevicius/Cibaite 2021, S. 40 f.

42 Siehe zur mangelnden wettbewerblichen Disziplinierung durch Abwanderung von Endnutzern bei Gatekeeper-Plattformen auch Kieß 2023, S. 314.

43 Schweitzer u.a. 2018, S. 12.

44 Monopolkommission 2021, Rn. 17.

45 Prüfer 2020, S. 6.

plattformdominierten Märkten, mindestens jedoch zu einer Erhöhung der Markteintrittsbarrieren für Dritte.[46]

Diese Monopolisierungstendenzen resultieren in einer Situation, in der für marktbeherrschende Betreiber digitaler Plattformen die Möglichkeit zum Machtmissbrauch besteht. Problematisch wird dieses Missbrauchspotential zwar erst, wenn es ergänzt wird durch Anreize, von diesem Potential auch tatsächlich Gebrauch zu machen.[47] Allerdings sind auch solche Anreize in plattformdominierten Märkten in der Regel stärker ausgeprägt als auf herkömmlichen Märkten.[48] Das zeigt sich exemplarisch an einem typischen Fall missbräuchlichen Verhaltens der Betreiber digitaler Plattformen, der Selbstbegünstigung als einer Form des Behinderungsmissbrauchs.[49] Diesem Fall kommt wegen der Doppelrolle, die einige Plattformbetreiber einnehmen, eine besondere Bedeutung zu[50] – denn für solche vertikal integrierten Plattformen, die beispielsweise Marktplatzbetreiber und zugleich Anbieter von Produkten und Dienstleistungen auf dem Marktplatz oder Suchmaschinenbetreiber und zugleich Gegenstand einer Suchanfrage sind, entstehen zwangsläufig Anreize zur Selbstbegünstigung.[51] Beispielhaft dafür stehen die Bevorzugung des eigenen Shopping-Vergleichsdienstes durch Google,[52] das selbstbegünstigende Verhalten von Google und Apple im Play- respektive AppStore[53] sowie auch Googles Geschäftspraktiken im Bereich der Online-Werbevermittlung in den von der Europäischen Kommission aufgenommenen Adtech- und AdSense-Verfahren.[54] Exemplarisch für den zweiten typischen Missbrauchsfall, den »datenspezifische[n] Konditionenmissbräuche[n]«[55] als einer Form des Ausbeutungsmissbrauchs, steht das vieldiskutierte Facebook-Verfahren.[56] In diesem stellte der BGH unter anderem fest, dass das Vorliegen asymmetrischer indirekter Netzwerkef-

46 Monopolkommission 2021, Rn. 17, 75 f.; Prüfer 2020, S. 6; Veldkamp 2023, S. 1550 zufolge liegt dieser Prozess »at the heart of the promise and concerns about the data economy.«

47 Mendelsohn/Budzinski 2023, Rn. 9.

48 Schweitzer u.a. 2018, S. 93, 111.

49 Ausführlich dazu Hutchinson/Treščáková 2022; dazu, dass Selbstbegünstigung als Behinderungsmissbrauch einzuordnen ist, siehe Hacker 2022, S. 1281; ebenso Schweitzer u.a. 2018, S. 128.

50 Burchardi 2022, S. 611.

51 Mendelsohn/Budzinski 2023, Rn. 9; siehe auch Haucap 2020, S. 22.

52 Siehe dazu Burchardi 2022, S. 611; Graef 2019, S. 454 f.; Volmar 2019, S. 412.

53 Siehe dazu Bostoen/Mândrescu 2020, S. 434 ff.

54 Siehe dazu Kestler 2023, S. 463 ff.

55 Kieß 2023, S. 206.

56 Ausführlich dazu Jackwerth 2022; Haus/Cesarano 2020.

fekte Anreize für Facebook setze, die als Ergebnis seiner Vormachtstellung auf dem Markt für soziale Netzwerke existierenden Verhaltensspielräume durch die Ausweitung seiner Datennutzungsbedingungen derart auszunutzen, dass es seine Position auf der anderen Marktseite – dem Markt für Online-Werbung – verbessern kann.[57] Es bestünden keine Zweifel an dem missbräuchlichen Charakter der von Facebook verwendeten Nutzungsbedingungen, die vorsahen, dass eine Nutzung des Dienstes nur dann möglich ist, wenn die Plattform die Befugnis erhält, »außerhalb von facebook.com generierte nutzer- und nutzergerätebezogene Daten« mit den aus der Facebook-Nutzung selbst entstehenden Daten zu verknüpfen und zu verarbeiten.[58] Dieses Beispiel verdeutlicht zugleich die enge Verbindung von Ausbeutungs- und Behinderungsmissbrauch. Die unangemessene Benachteiligung der Endnutzer stellt nicht nur ihnen gegenüber einen Ausbeutungsmissbrauch dar, vielmehr ist zugleich eine Behinderungswirkung im Online-Werbemarkt festzustellen, da die Qualität des dortigen Angebots maßgeblich von einem umfassenderen Datenzugang profitiert.[59]

III. Zwischenfazit: Notwendigkeit legislativer Intervention

Die Gemengelage an datenbezogenen und marktmachtbedingten Problemen in der Plattformökonomie hat ein regulatorisches Eingreifen erforderlich gemacht. Die Vergangenheit hat gezeigt, dass unter anderem das Zusammenspiel aus stark ausgeprägten (Daten-)Netzwerkeffekten, hohen Lock-In-Effekten bei unzureichenden Multi-Homing-Möglichkeiten und die damit einhergehenden Abhängigkeitslagen der unterschiedlichen Nutzergruppen zu einer Quasi-Gesetzgeber-Position der Plattformbetreiber und damit zu erheblichen Missbrauchsmöglichkeiten derselben führt. Da es den – insbesondere vertikal integrierten – Plattformen zugleich auch nicht an Anreizen zur Ausnutzung dieser Möglichkeiten mangelt, haben diese Möglichkeiten in der Praxis ihren Ausdruck sowohl in den gegenüber ihren gewerblichen Nutzern und Wettbewerbern, als auch gegenüber den privaten Endnutzern an den Tag gelegten Verhaltensweisen gefunden.

57 BGH, KVR 69/19 – Beschluss vom 23. Juni 2020 = GRUR 2020, S. 1321 f., Rn. 42 ff.
58 BGH, KVR 69/19 – Beschluss vom 23. Juni 2020 = GRUR 2020, S. 1321 f., Rn. 53.
59 Vgl. Haus/Cesarano 2020, S. 525.

Sofern es um die Regulierung von Datenzugangsansprüchen als Mittel zur Eindämmung einzelner plattformspezifischer Problemfelder geht, ist auf unterschiedliche Interessen mit unterschiedlichem Gewicht Rücksicht zu nehmen. So ist etwa eine Differenzierung nach Art der Daten aus mehrfacher Perspektive erforderlich. Unter dem Blickpunkt der Aufrechterhaltung von Investitionsanreizen stellt sich die Frage, ob nicht nur von den Nutzern freiwillig bereitgestellte und bei ihrer Dienstnutzung generierte Daten verpflichtend geteilt werden sollten, sondern auch aus diesen Daten abgeleitete Ergebnisse.[60] Aus Perspektive der Erforderlichkeit der Öffnung bestimmter Datenbestände stellt sich die Frage, ob die Datensets (mit vertretbarem Aufwand) replizierbar sind oder nicht, denn nur bei nicht replizierbaren Datensets, denen eine Bedeutung für einen bestimmten Markt zukommt, steigt auch die Gefahr eines Marktverschlusses.[61] Auch eine Differenzierung nach Zugangspetent sowie dessen jeweiliger Verwendungsabsicht ist erforderlich, da davon maßgeblich die Einschätzung abhängt, wie weit der Zugangsgegenstand zu fassen ist.[62] Und selbstverständlich muss auch die Effektivität einzelner Datenzugangsansprüche mit Blick auf die Erreichung des jeweils beabsichtigten Ziels berücksichtigt werden – regelmäßig wird diese beispielsweise bei individuell wahrzunehmenden Datenportabilitätsrechten hinterfragt.[63] Insgesamt gilt: Jedem Datenzugangsanspruch steht auch eine Datenteilungspflicht gegenüber, und jede Pflicht zur Datenteilung stellt zugleich auch einen Grundrechtseingriff dar,[64] der sich insofern an den üblichen Schranken messen lassen muss.

IV. Datenzugang nach dem Digital Markets Act

Der europäische Gesetzgeber hat mit dem DMA die wesentlichen Eigenschaften digitaler Plattformen und das von ihnen ausgehende Missbrauchspotential als Anlass dafür genommen, die größten ihrer Art einem

60 Siehe dazu unter anderen Schweitzer 2019a, S. 571; Crémer/de Montjoye/Schweitzer 2019, S. 8; Wais 2023, S. 604; siehe auch Richter/Globocník 2022, Rn. 35; diesbezüglich werden zudem regelmäßig Free-Riding-Bedenken geäußert, siehe etwa Krämer 2018, S. 468; Gineikyte/Barcevicius/Cibaite 2021, S. 40; Tombal 2020, S. 73.

61 Schweitzer u.a. 2018, S. 17.

62 Siehe auch Schweitzer 2019a, S. 571.

63 Siehe dazu Abschnitt IV 3.2.3.

64 Hartl/Ludin 2021, S. 536; Wischmeyer/Herzog 2020, S. 289.

gesonderten, weitgehenden Regulierungsrahmen zu unterwerfen. Zwar stehen Datenzugangsansprüche nicht im Vordergrund der Verordnung, dennoch kommt ihnen eine gewichtige Rolle bei der Adressierung unterschiedlicher plattformspezifischer Problemstellungen zu. Nach einer allgemeinen Einführung in Ziel, Regulierungsansatz und Anwendungsbereich der Verordnung folgt eine Betrachtung der einzelnen neu eingeführten Datenzugangsansprüche mit einem deutlichen Fokus auf den Fragen, welche derzeitigen Unzulänglichkeiten mit ihnen jeweils behoben bzw. abgeschwächt werden sollen, welche Daten jeweils Gegenstand des Zugangsanspruchs sind, unter welchen technischen, finanziellen und sonstigen Modalitäten der Anspruch zu gewähren ist und welche Hürden und offenen Fragen sich bei der Umsetzung und Geltendmachung der einzelnen Ansprüche ergeben.

1. Ziel und Regulierungsansatz

Das übergeordnete Ziel, das mit dem DMA verfolgt wird, stellt die Sicherstellung von Bestreitbarkeit und Fairness – zwei durchaus auslegungsbedürftigen Begriffen[65] – in plattformdominierten Märkten dar. Indem beides gewährleistet wird, soll gem. Art. 1 Abs. 1 DMA zu einem reibungslosen Funktionieren des Binnenmarktes beigetragen werden. Als Kompetenzgrundlage hat sich der europäische Gesetzgeber beim Erlass der Verordnung daher auf die Binnenmarktkompetenz des Art. 114 AEUV gestützt, nicht hingegen auf Art. 103 AEUV, woraus der Charakter der Verordnung als Instrument zur Binnenmarktförderung und nicht als wettbewerbsrechtliches Instrument deutlich wird.[66] Gleichwohl ist die wettbewerbsrechtliche Inspiration unverkennbar, nicht zuletzt, da die umfangreichen Verhaltenspflichten in den Art. 5–7 DMA größtenteils auf abgeschlossenen oder laufenden kartellrechtlichen Verfahren beruhen.[67] In Anerkennung der Unzulänglichkeiten des Kartellrechts in Bezug auf dessen Fähigkeit zur zeitnahen Adressierung insbesondere der die Big-Tech-Plattformunterneh-

65 Sich damit eingehend auseinandersetzend Mendelsohn/Budzinski 2023, Rn. 23 ff.

66 Siehe dazu Podszun 2023, Rn. 14; dass der europäische Gesetzgeber die inhaltliche Nähe des DMA zum Wettbewerbsrecht und damit einhergehend auch potentielle Abgrenzungsprobleme erkannt hat, zeigt sich auch in den Erw.Gr. 10 und 11 DMA.

67 Herbers/Savary/Gröf 2023, S. 151; Podszun/Bongartz/Langenstein 2021, S. 65 sprechen von einem »random ›best of‹ competition law cases.«

men umgebenden Wettbewerbsprobleme stellen die Verhaltenspflichten nunmehr ein regulatorisches ex ante Instrument dar.[68] Fortan sollen damit keine zeitaufwändigen Verfahren mehr durchlaufen werden müssen, vielmehr handelt es sich um konkrete Regelungen mit einem »self-executing«-Charakter.[69]

2. Anwendungsbereich

Der Pflichtenkatalog des DMA beschränkt sich in persönlich-sachlicher Hinsicht gem. Art. 1 Abs. 2 DMA auf zentrale Plattformdienste, die von Gatekeepern für in der Union niedergelassene gewerbliche Nutzer oder in der Union niedergelassene oder aufhältige Endnutzer bereitgestellt oder angeboten werden. Zentrale Plattformdienste sind in Art. 2 Nr. 2 lit. a-j DMA abschließend aufgeführt und umfassen Online-Vermittlungsdienste, Online-Suchmaschinen, Online-Dienste sozialer Netzwerke, Video-Sharing-Plattform-Dienste, nummernunabhängige interpersonelle Kommunikationsdienste, Betriebssysteme, Webbrowser, virtuelle Assistenten, Cloud-Computing-Dienste sowie Online-Werbedienste, einschließlich Werbenetzwerke, Werbebörsen und sonstige Werbevermittlungsdienste. Nahezu alle der in dieser Liste genannten zentralen Plattformdienste werden in den Art. 2 Nr. 5–13 DMA legaldefiniert.

Allein die Einstufung eines digitalen Dienstes als zentraler Plattformdienst genügt jedoch nicht, um dem Pflichtenkanon des DMA zu unterliegen. Notwendig ist vielmehr, dass dieser Dienst ein wichtiges Zugangstor zu Endnutzern darstellt und von einem Gatekeeper betrieben wird, anderenfalls bestünden gem. Erw.Gr. 15 DMA keine ernsten Bedenken bezüglich ihrer Bestreitbarkeit oder der Verwendung unfairer Praktiken. Für die Bestimmung eines Betreibers zentraler Plattformdienste als Gatekeeper – vorzunehmen durch die Kommission im Rahmen der ihr nach Art. 3 Abs. 4 oder 8 i.V.m. Abs. 9 DMA zugeschriebenen Kompetenz – sind in Art. 3 Abs. 1 lit. a-c DMA zunächst drei qualitative Kriterien vorgesehen, die kumulativ erfüllt sein müssen. Voraussetzung ist demnach, dass das Unternehmen gem. lit. a einen erheblichen Einfluss auf den Binnenmarkt hat, dass es gem. lit.

68 Siehe Kumkar 2022, Rn. 4 ff.; Achleitner 2022, S. 360; ausführlich zur regulatorischen Idee noch zum Kommissionsentwurf Podszun/Bongartz/Langenstein 2021, S. 61 ff.

69 Herbers 2022, Rn. 2.

b einen zentralen Plattformdienst bereitstellt, der gewerblichen Nutzern als wichtiges Zugangstor zu Endnutzern dient, und dass es gem. lit. c hinsichtlich seiner Tätigkeiten eine gefestigte und dauerhafte Position innehat oder absehbar ist, dass es eine solche Position in naher Zukunft erlangen wird.

Diese qualitativen Kriterien werden begleitet von quantitativen Schwellenwerten nach Art. 3 Abs. 2 lit. a-c DMA, deren Erreichen die widerlegbare[70] Vermutung begründen, dass der Plattformbetreiber die jeweiligen qualitativen Kriterien erfüllt. So ist – etwas verkürzt dargestellt – gem. Art. 3 Abs. 2 lit. a DMA von einem erheblichen Einfluss auf den Binnenmarkt i.S.v. Art. 3 Abs. 1 lit. a DMA auszugehen, wenn in jedem der vergangenen drei Geschäftsjahre in der Union ein Jahresumsatz von mindestens 7,5 Milliarden Euro erzielt wurde oder die durchschnittliche Marktkapitalisierung im vergangenen Geschäftsjahr mindestens 75 Milliarden Euro betrug. Von der Bereitstellung eines zentralen Plattformdienstes, der gewerblichen Nutzern als wichtiges Zugangstor zu Endnutzern i.S.v. Art. 3 Abs. 1 lit. b DMA dient, ist gem. Art. 3 Abs. 2 lit. b DMA dann auszugehen, wenn der zentrale Plattformdienst im vergangenen Geschäftsjahr mindestens 45 Millionen aktive Endnutzer und mindestens 10.000 jährlich aktive gewerbliche Nutzer hatte. Und das dritte Kriterium, wonach der Plattformbetreiber für die Benennung als Gatekeeper eine gefestigte und dauerhafte Position i.S.v. Art. 3 Abs. 1 lit. c DMA innehaben muss, wird gem. Art. 3 Abs. 2 lit. c DMA dann als erfüllt angesehen, wenn die Schwellenwerte des Art. 3 Abs. 2 lit. b DMA in jedem der vergangenen drei Geschäftsjahre erreicht wurden. Die für die Kommission zur Einstufung notwendigen Informationen nach Art. 3 Abs. 2 DMA müssen die Plattformbetreiber innerhalb der in Art. 3 Abs. 3 DMA genannten Fristen aktiv und eigenständig übermitteln. Über Form, Inhalt und sonstige Einzelheiten dieser Meldungen gibt Anhang I der Durchführungsverordnung (EU) 2023/814 der Kommission vom 14. April 2023 Aufschluss.[71] Bis zur ersten Deadline am 03. Juli 2023 hat die Kommission nach eigenen Angaben diesbezüglich Meldungen von sieben Unternehmen erhalten, namentlich Alphabet, Amazon, Apple, ByteDance, Meta, Microsoft und Samsung. Am 06. September 2023 folgten die ersten Benennungen durch die Kommission: Bis auf Samsung wurden alle der genannten Plattformen als Gatekeeper benannt und insgesamt 22 zentrale Plattformdienste dieser Unternehmen aufgeführt. Dazu gehören unter anderem Tiktok (ByteDance), Google

70 Zur Vermutungswiderlegung siehe Krauskopf/Brösamle 2023, Rn. 8–12.
71 Europäische Kommission 2023b.

Maps, Google Play, Youtube und Chrome (Google), LinkedIn und Windows (Microsoft) sowie der Amazon Marketplace.[72]

3. Die einzelnen Zugangsansprüche

Der europäische Gesetzgeber adressiert mit jedem der in Art. 6 Abs. 8–11 DMA enthaltenen Datenzugangsansprüche unterschiedliche Probleme. Für diese Vorschriften gilt dasselbe wie auch für die gesamten Verpflichtungen der Art. 5–7 DMA: Es liegt ein »Sammelsurium verschiedener Anliegen« vor, das keiner besonderen Systematik zu unterliegen scheint.[73] Von einem zum nächsten Anspruch differieren entweder Verpflichteter und/oder Begünstigter, die jeweils umfassten Daten, die (technischen) Modalitäten der Zugangsgewährung, etwaige monetäre Kompensationszahlungen – oder alles gemeinsam. Mit Blick auf die Maßnahmen, mit denen die Gatekeeper ihre neuen datenzugangsbezogenen Verpflichtungen erfüllen können, kommt darüber hinaus der Kommission eine besondere Bedeutung zu. Zum einen wird ihr nach Art. 8 Abs. 2 UAbs. 2 DMA die Kompetenz zum Erlass konkretisierender Durchführungsrechtsakte eingeräumt, zum anderen kann sie mit den Gatekeepern auf deren Ersuchen hin in einen gem. Art. 8 Abs. 3 DMA vorgesehenen »regulatorischen Dialog« treten, der dazu dient, schnell, gemeinsam und verbindlich offene regulatorische Fragen zu klären.[74]

3.1 Art. 6 Abs. 8 DMA – Daten- und Instrumentenzugang im Online-Werbemarkt

Als erste näher zu betrachtende Vorschrift normiert Art. 6 Abs. 8 DMA einen Anspruch von Werbetreibenden und Herausgebern sowie von diesen beauftragten Dritten gegenüber Gatekeepern, ihnen Zugang zu deren Leistungsmessungsinstrumenten und zu den aggregierten und nicht-aggregierten Daten einzuräumen, die sie benötigen, um ihre eigene unabhängige Überprüfung des Werbeinventars vorzunehmen.

---

72 Europäische Kommission 2023a; ausführlich zu den von Seiten verschiedener Gatekeeper gegen ihre Benennung vorgebrachten Argumenten sowie zum Umgang der Kommission mit diesen Argumenten Higer/Patt 2024, S. 81 ff.

73 So in Bezug auf die Verpflichtungen der Art. 5–7 DMA Podszun 2023, Rn. 36.

74 Ausführlich zu Sinn, Verbindlichkeit und Verfahren dieses regulatorischen Dialogs Seeliger 2023, Rn. 40–48.

3.1.1 Problem: Der Online-Werbemarkt als Musterbeispiel für Marktmacht und Intransparenz

Zweifelsohne bringt Online-Werbung eine ganze Reihe an Vorteilen für unterschiedliche Akteure mit sich. Vor allem aber stellt sie eine Möglichkeit zur Umsatzgenerierung dar, die für eine Vielzahl von Diensteanbietern unerlässlich geworden ist. Unabhängig davon, ob es sich um Betreiber eines sozialen Netzwerks oder einer Nachrichtenwebseite handelt – wer Verbrauchern seinen Dienst »kostenfrei« anbieten möchte, sieht sich der Notwendigkeit ausgesetzt, sich anderweitig zu finanzieren.[75] Wie schon zu Beginn dieses Beitrags dargestellt gilt auch hier, dass die Generierung von möglichst viel Aufmerksamkeit für den eigenen Dienst im Sinne von auf dem Dienst verbrachter Nutzungszeit durch möglichst viele Nutzer entscheidend ist. Einerseits kann dadurch mehr Werbung auf den eigenen Werbeflächen angezeigt werden und dadurch das Umsatzpotential gesteigert werden,[76] andererseits werden die bei der Dienstnutzung anfallenden Daten zur Verbesserung der Genauigkeit von personalisierter Werbung genutzt.

Die Akteure des Online-Werbemarktes, die auch durch die Vorschrift des Art. 6 Abs. 8 DMA als Datenzugangsberechtigte adressiert werden – also Publisher, d.h. Anbieter von Werbeflächen wie beispielsweise Webseiten- oder App-Betreiber,[77] und Werbetreibende, die auf der Suche nach geeigneten Werbeflächen für ihre Anzeigen sind – können miteinander entweder direkt agieren oder dafür auf Intermediäre, vor allem im Rahmen des sogenannten Programmatic Advertisings,[78] zurückgreifen.[79] Im Bereich des Programmatic Advertisings konkurrieren mehrere Publisher miteinander darum, ihre Werbeflächen an Werbetreibende zu verkaufen und nehmen dafür eine ganze Reihe an Intermediären in Anspruch, die den komplexen Prozess der automatisiert und in Echtzeit erfolgenden Auswahl einer für den jeweiligen Rezipienten passenden Werbeanzeige und der Festlegung des dafür durch den Werbetreibenden zu entrichtenden Entgelts übernehmen.[80] Die aus

75 Vgl. Fast/Schnurr/Wohlfahrt 2019, Rn. 20.

76 CMA 2020, Rn. 5.1.

77 Bundeskartellamt 2022, Rn. 24.

78 Bundeskartellamt 2023, Rn. 23; die CMA verwendet anstelle des Begriffs des Programmatic Advertisings den des Open Display Markets, vgl. CMA 2020, Rn. 5.116.

79 Teilweise wird bei der Option des Vertriebs durch Intermediäre noch differenziert zwischen einer Vermittlung »eher herkömmlicher Prägung« und Programmatic Advertising im engeren Sinne, vgl. Bundeskartellamt 2022, Rn. 44.

80 CMA 2020, Rn. 5.204.

der Gesamtheit dieser Intermediäre bestehende Wertschöpfungskette[81] behält für die Vermittlungsleistung rund 35 Prozent des Betrags, den der Werbetreibende an den Publisher zahlt, als sog. »ad tech tax«[82] ein.[83] Um erfolgreich als Vermittler in dieser Wertschöpfungskette partizipieren zu können, sind umfassende Datenzugriffs- und Datenauswertungsmöglichkeiten unerlässlich – ebenso wie für Publisher generell beim Display-Marketing, da der Erfolg von Werbemaßnahmen bei diesem Werbekanal im Besonderen auf möglichst passgenauer personalisierter Werbung beruht.[84] Im Gegensatz dazu kommt dem umfassenden Zugriff auf Nutzungsdaten bei dem weiteren in Betracht kommenden Werbekanal, der suchgebundenen Werbung, eine weniger herausgehobene Bedeutung zu.[85] Stattdessen sind Art und Anzahl der Suchanfragen ausschlaggebend – ohne einen gewissen Erfolg bei der Generierung von Suchanfragen kann auch nicht erfolgreich suchgebundene Werbung angezeigt werden.[86] Insofern ist in Anbetracht von Googles Marktstellung auf dem Suchmaschinenmarkt[87] auch die analoge Marktmacht auf dem Markt für Suchmaschinenwerbung nicht weiter verwunderlich.[88]

Unabhängig davon, welcher Werbekanal betrachtet wird, gilt: Die Anbieterseite von Werbedienstleistungen ist hochkonzentriert, mit Google und Meta von besonders marktmächtigen Plattformunternehmen besetzt und insgesamt von Informationsasymmetrien geprägt. Das führt unter anderem zu nicht nachvollziehbaren Preisgestaltungen, teilweise überhöhten Preisen und einer mangelnden Bestimmbarkeit des Erfolgs von Werbemaßnahmen.[89] Insbesondere Letzteres stellt einen wichtigen Faktor bei der Entscheidung der Werbetreibenden darüber, wie sie ihr Werbebudget einsetzen wollen, dar.[90] Wie die Competition and Markets Authority (CMA) in ihrer Marktuntersuchung festgestellt hat, lassen allerdings weder Facebook noch Google eine unabhängige Überprüfung ihres Werbeinventars mit

81 Ausführlich dazu CMA 2020, Rn. 5.205 ff.
82 CMA 2020, Rn. 2.67.
83 So die CMA 2020, Rn. 5.237; siehe auch die Verweise der CMA auf ähnliche Ergebnisse aus anderen Studien in Rn. 5.238.
84 Ebd., Rn. 5.127.
85 Ebd.
86 Vgl. ebd., Rn. 5.57.
87 Siehe dazu ausführlich Abschnitt IV 3.4.1.
88 Ausführlich dazu CMA 2020, Rn. 5.45 ff.
89 Ebd., Rn. 5.138.
90 Vgl. ebd., Rn. 45.

Blick auf Qualität und Effektivität der digitalen Werbung zu.[91] Folgerichtig forderte sie bereits 2020: »In relation to verification, Google and Facebook should give advertisers access to the tools or information necessary to carry out their own, independent verification of advertising purchased on the inventory owned and operated by Google and Facebook […].«[92]

3.1.2 Gegenstand und Modalitäten des Zugangsanspruchs

In Reaktion auf die oftmals intransparenten und undurchsichtigen Bedingungen bei den von Gatekeepern erbrachten Werbedienstleistungen (vgl. Erw.Gr. 58 DMA) hat der europäische Gesetzgeber mit Art. 6 Abs. 8 S. 1 DMA einen Zugangsanspruch für Werbetreibende und Herausgeber sowie von diesen beauftragten Dritten normiert.[93] Der Anspruch erstreckt sich sowohl auf die vom Gatekeeper selbst verwendeten Instrumente zur Leistungsmessung als auch auf alle aggregierten und nichtaggregierten Daten, die für eine eigene unabhängige Überprüfung des Werbeinventars, also »alle aus Sicht des Werbetreibenden platzierten Werbungen bzw. alle aus Sicht des Publishers verkauften Werbeflächen«[94], benötigt werden (beispielsweise die Konversionsrate[95]). Das den Datenzugangsanspruch einschränkende Kriterium stellt insofern die Erforderlichkeit der jeweiligen Daten für die eigene Überprüfung dar. Diese Beschränkung ist nicht nur in Bezug auf den Umfang der offenzulegenden Daten relevant, sondern auch bezüglich der Art und Weise der Datenbereitstellung. Diese muss gem. Art. 6 Abs. 8 S. 2 DMA so erfolgen, dass Werbetreibende und Herausgeber ihre eigenen Überprüfungs- und Messinstrumente einsetzen können, um die Leistung der von den Gatekeepern bereitgestellten zentralen Plattformdienste zu bewerten. Damit dürfte in der Regel die Anforderung verbunden sein, die Daten in maschinenlesbarer Form bereitzustellen,[96] jedenfalls aber derart, dass sich die Daten ohne weiteren Aufwand in die eigenen Instrumente der Zugangsberechtigten einfügen lassen.[97] Darüber hinaus müssen Gatekeeper den Zugang nur auf Antrag gewähren und sämtlichen Zugangsbegehren

91 Ebd., Rn. 53.
92 Ebd., Rn. 104.
93 Die Vorschrift muss darüber hinaus in Verbindung mit Art. 5 Abs. 9 und 10 DMA gesehen werden, die ebenfalls auf eine Erhöhung von Transparenz im Online-Werbemarkt abzielen.
94 Wolf-Posch 2023, Rn. 167.
95 Hacker 2022, S. 1279.
96 So Wolf-Posch 2023, Rn. 169.
97 So Louven 2023, Rn. 119.

kostenlos nachkommen – unabhängig davon, ob sich diese auf ihre Instrumente zur Leistungsmessung oder auf die zur Verwendung eigener Leistungsmessungsinstrumente erforderlichen Daten beziehen.

3.1.3 Bewertung, Hürden und offene Fragen

Der Zugangsanspruch aus Art. 6 Abs. 8 DMA dient in erster Linie Transparenzzwecken.[98] Während zuversichtlich davon ausgegangen werden kann, dass für die Begünstigten der Vorschrift – den Werbetreibenden und Herausgebern – künftig tatsächlich mehr Gewissheit hinsichtlich des Erfolgs und der Kosten einzelner Werbemaßnahmen bestehen wird,[99] ist in Bezug auf die mit der infolge des Abbaus der bestehenden Informationsasymmetrien (mindestens mittelbar) verbundenen Hoffnung eines zunehmenden Wettbewerbs im Online-Werbemarkt[100] jedoch Skepsis angebracht. Bei hochkonzentrierten Märkten nützt ein Mehr an Transparenz wenig, wenn keine (adäquaten) Alternativen bestehen, zu denen (sinnvollerweise) gewechselt werden könnte.[101] Mehr Wettbewerb auf dem Online-Werbemarkt würde allerdings voraussetzen, dass konkurrierende Anbieter von Online-Werbedienstleistungen entweder (im Bereich des Display-Marketings) in der Lage sind, auf Basis umfassender Datenbestände ähnlich treffsichere personalisierte Werbung zu ermöglichen,[102] oder (im Bereich der suchgebundenen Werbung) eine vergleichbare Zahl an Suchanfragen zu generieren.[103] Für dieses Problem hält Art. 6 Abs. 8 DMA keine Lösung parat, weshalb nicht davon ausgegangen werden kann, dass ein Mehr an Transparenz tatsächlich einen positiven Effekt auf die »Wechselfähigkeit und -willigkeit«[104] von Werbetreibenden und Herausgebern haben wird und sich insofern an den Vormachtstellungen von Meta und Google etwas ändern wird. Lediglich mit Blick auf das Wettbewerbsumfeld im von Google

98 Ebd. Rn. 106; Wolf-Posch 2023, Rn. 160.

99 Wobei sich der Informationsgewinn in Bezug auf die Kosten auch und in erster Linie aus Art. 5 Abs. 9 und 10 DMA ergibt.

100 Vgl. Wolf-Posch 2023, Rn. 160; König 2023, Rn. 77.

101 Auch die CMA hat das Zusammenspiel von höherer Wettbewerbsintensität und Transparenz in Bezug auf einen möglichen Preisdruck auf die durchschnittliche Ad Tech Tax in Höhe von 35 Prozent hervorgehoben, vgl. CMA 2020, Rn. 15.

102 Vgl. CMA 2020, Rn. 5.127: »[…] access to valuable user data that enables more granular audience targeting is a key dimension of competition.«

103 Vgl. ebd., Rn. 5.57.

104 Wolf-Posch 2023, Rn. 160.

dominierten Markt für suchgebundene Werbung könnten sich in dieser Hinsicht Synergieeffekte mit dem Datenzugangsanspruch aus Art. 6 Abs. 11 DMA ergeben.

3.2 Art. 6 Abs. 9 DMA – erweiterte Datenportabilität für Endnutzer

Der nächste gegen Gatekeeper gerichtete Datenzugangsanspruch kommt Endnutzern und von diesen beauftragten Dritten zugute und findet sich in Art. 6 Abs. 9 DMA. In der Sache handelt es sich (in mehrfacher Hinsicht) um eine Erweiterung des bereits aus Art. 20 DSGVO bekannten Rechts auf Datenportabilität.

3.2.1 Problem: Endnutzer-Abhängigkeiten und Lock-In-Effekte

Das Art. 6 Abs. 9 DMA zugrundeliegende Problem bedarf an dieser Stelle deutlich weniger Erörterung als die zuvor in Bezug auf Art. 6 Abs. 8 DMA skizzierte Gemengelage. Wie bereits in Abschnitt II dargestellt führen unterschiedliche Plattformcharakteristika dazu, dass sich Nutzer digitaler Plattformen hohen Wechselkosten und damit Lock-In-Situationen ausgesetzt sehen. Diese Aspekte und das mit solchen Lock-In-Effekten, die sich aus der mangelnden Möglichkeit zur Datenmitnahme ergeben, einhergehende Potential der Gatekeeper, die Bestreitbarkeit ihrer zentralen Plattformdienste oder das Innovationspotential des Digitalsektors zu untergraben, waren ausweislich Erw.Gr. 59 DMA Anlass dafür, eine Ergänzung des aus Art. 20 DSGVO bekannten Rechts auf Datenportabilität zu normieren, das den Endnutzern digitaler Plattformen zugutekommt.

3.2.2 Gegenstand und Modalitäten des Zugangsanspruchs

Konkret enthält Art. 6 Abs. 9 DMA die Verpflichtung des Gatekeepers, Endnutzern und von ihnen beauftragten Dritten auf ihren Antrag hin kostenlos die effektive Übertragbarkeit der Daten, die vom Endnutzer bereitgestellt oder durch die Tätigkeit des Endnutzers im Zusammenhang mit der Nutzung des betreffenden zentralen Plattformdienstes generiert werden, zu ermöglichen. Diese Pflicht umfasst zudem die kostenlose Bereitstellung von Instrumenten, die die effektive Nutzung der Datenübertragbarkeit erleichtern sowie die Gewährleistung eines permanenten Echtzeitzugangs zu diesen Daten. Tatsächlich stellt dieser Zugangsanspruch in unterschiedlicher Hinsicht eine deutliche Ergänzung von Art. 20 DSGVO dar – nämlich sowohl

in Bezug auf die Zugangsberechtigten, den Zugangsgegenstand als auch die Art und Weise der Zugangsgewährung. Zugangsberechtigt sind nicht mehr nur natürliche Personen, sondern unter Art. 6 Abs. 9 DMA zugleich auch juristische Personen, da der Endnutzerbegriff gem. Art. 2 Nr. 20 DMA beide Arten unter sich vereint. In Bezug auf die Modalitäten der Zugangsgewährung fällt auf, dass die in Art. 20 DSGVO vorgesehene Datenbereitstellung in einem strukturierten, gängigen und maschinenlesbaren Format im DMA nun einer Zielbestimmung in Form der Ermöglichung einer effektiven Übertragbarkeit der Daten gewichen und zudem der in Art. 20 Abs. 2 DSGVO vorgesehene Vorbehalt der technischen Machbarkeit entfallen ist.

Der letzte wesentliche Unterschied betrifft die Daten, die Gegenstand des Zugangsanspruchs sind. Bestanden zu Art. 20 DSGVO noch rege Diskussionen dahingehend, ob unter den einem Verantwortlichen bereitgestellten Daten auch solche Daten zu verstehen sind, die durch die Nutzung des Dienstes generiert wurden,[105] wurde dieser Diskussion in Bezug auf den Zugangsanspruch unter Art. 6 Abs. 9 DMA vorweggegriffen, indem im Normtext klargestellt wurde, dass sich der Anspruch auch auf alle Daten erstreckt, die durch die Tätigkeit des Endnutzers im Zusammenhang mit der Nutzung des betreffenden zentralen Plattformdienstes generiert wurden. Dass Nutzungsdaten nunmehr explizit mit einbezogen werden, ist in Anbetracht ihrer besonderen Relevanz[106] zwar zu begrüßen, gleichwohl dürfte sich die Diskussion um den Umfang der erfassten Daten nicht insgesamt erledigt, sondern lediglich verschoben haben: Die neue Streitfrage liegt nun darin, ob aus den bereitgestellten Daten und Nutzungsdaten abgeleitete Daten ebenfalls durch den Gatekeeper bereitzustellen sind. Diesbezüglich gehen erste Einschätzungen bereits auseinander – teilweise werden abgeleitete Daten vom Anwendungsbereich der Vorschrift ausgeschlossen,[107] teilweise wird jedoch auch argumentiert, dass sie in Anbetracht des Zwecks der Vorschrift umfasst seien.[108] Für den Ausschluss abgeleiteter Daten aus dem Anwendungsbereich des Art. 6 Abs. 9 DMA spricht jedoch mindestens das Argument der Aufrechterhaltung von Investitionsanreizen. Denn während Nutzungsdaten als mehr oder weniger kostenloses Beiprodukt an-

105 Siehe dazu statt vieler Geminn 2020, S. 309 f.

106 Auf den »besonderen Bedeutungszuwachs« solcher »automatisch generierter Nutzungsdaten« in der Datenökonomie hinweisend Schweitzer 2019a, S. 571.

107 Wolf-Posch 2023, Rn. 185; Brandt/Grewe 2023, S. 930.

108 So Louven 2023, Rn. 129.

fallen, setzt die Generierung neuer Erkenntnisse aus diesen Nutzungsdaten in der Regel nicht zu vernachlässigende Anfangsinvestitionen voraus.[109]

3.2.3 Bewertung, Hürden und offene Fragen

Eine Bewertung des erweiterten Portabilitätsrechts für Endnutzer nach Art. 6 Abs. 9 DMA muss erneut vor allem mit Blick auf den mit der Vorschrift verfolgten Zweck erfolgen. Ausweislich Erw.Gr. 59 DMA liegt dieser in der Förderung der Fähigkeit zum Anbieterwechsel und zur Parallelnutzung unterschiedlicher Dienste; mittelbar dann auch auf der Sicherstellung der Bestreitbarkeit der von Gatekeepern dominierten Plattformmärkte.[110] Als explizite Ergänzung des Datenportabilitätsrechts aus Art. 20 DSGVO, dessen Charakter als »Schnittstelle zwischen Wettbewerbs- und Datenschutzrecht«[111] mit einer »Verwandtschaft […] qua Regelungsintention«[112] gemeinhin anerkannt ist, ist die Verortung im DMA zunächst zu begrüßen, da dadurch »überschießendes Wettbewerbsrecht« im Datenschutzrecht vermieden wird.[113] Vielversprechend ist darüber hinaus, dass mit dem neuen Portabilitätsanspruch viel der berechtigten Kritik an der Konstruktion von Art. 20 DSGVO aufgegriffen wurde – etwa durch die Ausdehnung auch auf juristische Personen,[114] die Klarstellung um die Erstreckung auf Nutzungsdaten, den Verzicht auf den Vorbehalt der technischen Machbarkeit[115] sowie die Zugangsermöglichung über einen Echtzeitzugang.[116]

Dennoch bleibt offen, ob sich das neue Portabilitätsrecht in der Praxis als effektiv erweisen wird. Hinsichtlich der Eignung zur Förderung der Bestreitbarkeit plattformdominierter Märkte bleiben mindestens zwei Hindernisse bestehen. Das erste liegt in der Grundkonzeption eines jeden individuell wahrzunehmenden Datenübertragbarkeitsrechts, das (auch) zur Förderung der Wettbewerbsintensität gedacht ist: Jeder Endnutzer muss einzeln beantragen, dass die durch seine Dienstnutzung generierten Daten an Emp-

109 Schweitzer u.a. 2018, S. 152; siehe auch Brandt/Grewe 2023, S. 930.
110 Siehe dazu auch Wolf-Posch 2023, Rn. 179.
111 Sperlich 2017, S. 377.
112 Schröder 2019, S. 18.
113 Kieß 2023, S. 181 f.
114 Diesen noch fordernd Haucap 2018, S. 474.
115 Siehe dazu Krämer 2018, S. 467 f.
116 Schweitzer/Metzger 2023, S. 340.

fänger seiner Wahl übertragen werden.[117] Die Effektivität hängt daher davon ab, dass genügend Individuen von ihrem Portabilitätsrecht Gebrauch machen.[118] Zum anderen stehen die datenteilenden Gatekeeper nicht in der Pflicht, die Daten nach der Übertragung zu löschen. Selbst wenn alle Endnutzer von ihrem Portabilitätsrecht Gebrauch machen würden, verliert der Gatekeeper keinerlei Daten und verfügt daher unverändert über einen wesentlichen Wettbewerbsvorteil.[119]

3.3 Art. 6 Abs. 10 DMA – Datenzugang für gewerbliche Nutzer

Mit Art. 6 Abs. 10 DMA hat der europäische Gesetzgeber einen Art. 6 Abs. 9 DMA vergleichbaren Datenzugangsanspruch für gewerbliche Nutzer von zentralen Plattformdiensten, die durch Gatekeeper erbracht werden, geschaffen.

3.3.1 Problem: Mangelnde Datenteilhabe gewerblicher Nutzer

Auch in Bezug auf das mit dieser Vorschrift adressierte Problem kann im Wesentlichen auf die allgemeinen Ausführungen in Abschnitt II verwiesen werden. Gewerbliche Plattformnutzer sehen sich – bedingt von ihren Abhängigkeitsverhältnissen von so manchen Plattformen – ebenso häufig wie private Endnutzer mit für sie unvorteilhaft ausgestalteten Bedingungen konfrontiert, die die Art und Weise sowie das Ausmaß ihres Zugriffs auf durch ihre Mitwirkung generierte Daten betreffen und denen sie sich unterwerfen müssen.[120] Dabei besteht eine Verpflichtung für Anbieter von Online-Vermittlungsdiensten – ungeachtet ihrer Größe und wirtschaftlichen Leistungsfähigkeit – zu mehr Transparenz in Bezug

117 Ausführlich dazu, warum das »mit Blick auf das Problem der Monopolisierung datengetriebener Märkte ein eher zahnloses Instrument« ist, Prüfer 2020, S. 9.

118 Siehe dazu Krämer/Senellart/de Streel 2020, S. 60; treffend auch die Verortung als »collective action problem« bei Gill/Metzger 2022, S. 233; insofern findet sich auch hier die von Brieske/Schweitzer in diesem Band herausgearbeitete Adressierung des Menschen als »dividuelles Subjekt«, da das Individuum eben nicht nur in seinen individuellen (Daten-)Kontrollfähigkeiten gestärkt werden soll, sondern ihm zudem eine »Infrastruktur- und Gemeinwohlverantwortung zugeschrieben wird.«

119 Siehe dazu Prüfer 2020, S. 9; auch an anderer Stelle wird die Eignung zur Herausforderung der aus Datenvorteilen resultierenden Marktposition von Gatekeepern bezweifelt, vgl. Schweitzer u.a. 2022, S. 201; Schweitzer/Metzger 2023, S. 353.

120 Ausführlich dazu anhand des Beispiels des von Apple verwendeten App Tracking Transparency Frameworks König 2023, Rn. 37.

auf die Datenzugangsausgestaltung für gewerbliche Nutzer durch Art. 9 P2B-VO schon seit 2019. Art. 6 Abs. 10 DMA ergänzt diese Transparenzverpflichtung nun durch eine explizite Datenteilungspflicht der Gatekeeper.[121] Nicht ohne Weiteres zu beantworten ist, ob mit der Vorschrift primär eine Förderung der Fairness der Geschäftsbeziehungen zwischen Gatekeepern und gewerblichen Nutzern intendiert ist,[122] oder nicht doch in erster Linie eine Förderung der Bestreitbarkeit des von dem jeweiligen Gatekeeper dominierten Marktes[123] verfolgt wird.

3.3.2 Gegenstand und Modalitäten des Zugangsanspruchs

Entgegen vereinzelt anklingender Auffassungen erfolgt durch Art. 6 Abs. 10 DMA nicht bloß eine Ausdehnung des Kreises der Anspruchsberechtigten aus Art. 6 Abs. 9 DMA auf gewerbliche Nutzer und von diesen ermächtigten Dritten.[124] Der Datenzugangsanspruch für gewerbliche Nutzer aus Art. 6 Abs. 10 DMA umfasst einen effektiven, hochwertigen und permanenten Echtzeitzugang zu sowie das Recht zur Nutzung von aggregierten und nichtaggregierten Daten, personenbezogenen und nichtpersonenbezogenen Daten, die im Zusammenhang mit der Nutzung der betreffenden zentralen Plattformdienste durch die gewerblichen Nutzer sowie den Endnutzern, die die Angebote dieser gewerblichen Nutzer in Anspruch nehmen, bereitgestellt oder generiert werden. Dabei sind auch solche Daten erfasst, die bei der Nutzung von Diensten, die zusammen mit den jeweiligen zentralen Plattformdiensten oder zu deren Unterstützung erbracht werden, anfallen. Zwar liegen zweifelsohne Gemeinsamkeiten zwischen Art. 6 Abs. 9 und 10 DMA vor, so werden etwa ähnliche Probleme und Lösungsansätze adressiert, beide Zugangsansprüche sind antragsabhängig und beide Ansprüche sind durch die Gatekeeper kostenlos zu erfüllen. Bereits bei der ersten näheren Betrachtung fallen allerdings auch einige größere und kleinere Unterschiede auf. So stellt sich etwa die Frage, welche zusätzlichen Anforderungen an den in Abs. 10 vorgesehenen »effektiven, hochwertigen und permanenten Echtzeitzugang« zu stellen sind, da die Kriterien der Effektivität und der Hochwertigkeit des Echtzeitzugangs in Abs. 9 keinen

121 Siehe dazu auch Wolf-Posch 2023, Rn. 252.
122 So Louven 2023, Rn. 143.
123 So wohl Wolf-Posch 2023, Rn. 205.
124 So jedoch Gasser/Hegener 2023, Rn. 76.

Einzug erhalten haben.[125] Daneben geht auch die Einbeziehung von Daten, die nicht bei der Nutzung der zentralen Plattformdienste selbst, sondern bei der Nutzung von Komplementärdiensten generiert werden, über Abs. 9 hinaus. Der wohl relevanteste Unterschied beider Vorschriften – abgesehen von den unterschiedlichen Zugangsberechtigten – liegt jedoch darin, dass dem gewerblichen Nutzer kein Recht auf direkte Übertragbarkeit der Daten zu Dritten eingeräumt wird.[126] Ausreichend ist wohl das Zugänglichmachen, beispielsweise als Download,[127] weitere Anforderungen an Datenformat und -qualität ergeben sich dann insbesondere aus der in Abs. 10 ebenfalls enthaltenen Verpflichtung der Gatekeeper, auch die Nutzung der Daten zu ermöglichen.[128]

In Bezug auf die Daten, die Gegenstand des Zugangsanspruchs sind, kann zunächst festgehalten werden, dass lediglich bereitgestellte Daten und Nutzungsdaten, nicht jedoch abgeleitete Daten vom Anwendungsbereich erfasst sind.[129] Dafür spricht nicht nur das bereits im Kontext des Portabilitätsrechts für Endnutzer gem. Art. 6 Abs. 9 DMA angeführte Argument der Aufrechterhaltung von Investitionsanreizen, sondern darüber hinaus auch eine im Gesetzgebungsprozess erfolgte Änderung in den Erwägungsgründen. So war in Erw.Gr. 55 S. 2 des Kommissionsentwurfs zum DMA[130] (DMA-KOM-E) mit Blick auf die von gewerblichen Nutzern und Endnutzern bereitgestellten und generierten Daten noch der Einschub enthalten, dass dafür »unter anderem auch aus solcher Nutzung Daten abgeleitet [werden]«, bei denen gem. Erw.Gr. 55 S. 3 DMA-KOM-E sichergestellt werden müsse, »dass gewerbliche Nutzer Zugang zu den auf diese Weise generierten Daten haben […].« Der in Erw.Gr. 55 S. 2 DMA-KOM-E enthaltene Verweis auf die abgeleiteten Daten ist im entsprechenden Erw.Gr. 60 der finalen Fassung des DMA jedoch nicht mehr enthalten. Treffend ist daher die Beschreibung des Zugangsgegenstands als durch die »eigene gewerbliche

125 Ausführlich zu diesen Kriterien Wolf-Posch 2023, Rn. 231–242; an anderer Stelle wird der Gedanke aufgeworfen, dass sich argumentative Ähnlichkeiten zu Selbstbevorzugungsverboten ergeben und insofern als Mindestanforderung eine Zugangsausgestaltung analog des Zugangs, über den der Gatekeeper selbst verfügt, denkbar wäre, siehe Louven 2023, Rn. 153.

126 So auch Wolf-Posch 2023, Rn. 210, 229; anderer Ansicht wohl Schweitzer/Metzger 2023, S. 338, 340.

127 Wolf-Posch 2023 Rn. 210, 229.

128 Ebd., Rn. 230.

129 Ebd., Rn. 216; Louven 2023, Rn. 147.

130 Vgl. Europäische Kommission 2020b.

Tätigkeit generierte[s] Datenpaket.«[131] Dem gewerblichen Nutzer kommt der Zugangsanspruch nur in Bezug auf alle Daten zu, die im Zusammenhang mit seiner eigenen Plattformnutzung oder bei der Inanspruchnahme seiner über die Plattform angebotenen Dienstleistungen durch die Endnutzer generiert wurden.[132] Ausgeschlossen vom Anwendungsbereich sind daher Datensätze, die aggregierte Daten aller Endnutzer einer Plattform enthalten.[133] Zuletzt stellt die Vorschrift auch in Bezug auf personenbezogene Daten klar, dass sie Teil des Zugangsanspruchs sind.[134] Der Zugang zu ihnen darf durch die Gatekeeper allerdings gem. Art. 6 Abs. 10 S. 2 DMA nur dann gewährt werden, wenn sie unmittelbar mit der Nutzung der vom antragsberechtigten gewerblichen Nutzer über den zentralen Plattformdienst angebotenen Produkte oder Dienstleistungen durch die Endnutzer im Zusammenhang stehen und sofern der Endnutzer dieser Weitergabe durch eine Einwilligung zugestimmt hat.[135] Um etwaigen Schwierigkeiten bei der Einholung der dafür erforderlichen Einwilligungen vorwegzugreifen, ist den Gatekeepern gem. Art. 13 Abs. 5 S. 2 DMA untersagt, die Einholung der Einwilligung durch den gewerblichen Nutzer aufwändiger auszugestalten, als es bei den Gatekeeper-eigenen Diensten der Fall ist.

3.3.3 Bewertung, Hürden und offene Fragen

Sofern der Datenzugangsanspruch für gewerbliche Nutzer nach Art. 6 Abs. 10 DMA eine Förderung der Bestreitbarkeit der von Gatekeepern dominierten Märkte bezwecken soll, ist wegen des Ausschlusses von aggregierten Datensätzen, die über solche Daten hinausgehen, an deren Generierung der einzelne gewerbliche Nutzer partizipiert hat, Skepsis angebracht. Der Zugangsanspruch zielt lediglich auf einen Bruchteil der den Gatekeepern zur Verfügung stehenden Daten ab. Insofern können die Gatekeeper selbst unverändert auf unvergleichlich größere Datenmengen zugreifen, weshalb keine relevante Reduktion ihres daraus resultierenden Wettbewerbsvorteils zu erwarten ist.[136] Gleichwohl könnte sich eine solche in bestimmten Situa-

131 Wolf-Posch 2023, Rn. 215.

132 Dies als folgerichtiges Ergebnis bei Anknüpfung an die »Datenursächlichkeit« einordnend Wais 2023, S. 603 f.

133 Wolf-Posch 2023, Rn. 215.

134 Siehe dazu auch Louven 2023, Rn. 148.

135 Der Rückgriff auf andere Erlaubnistatbestände aus Art. 6 Abs. 1 UAbs. 1 DSGVO dürfte damit ausgeschlossen sein, vgl. Louven 2023, Rn. 149.

136 Siehe dazu auch die Überlegungen von Prüfer 2020, S. 9; Schweitzer/Metzger 2023, S. 353.

tionen in der Kombination mit dem in Art. 6 Abs. 2 DMA für Gatekeeper normierten Verwendungsverbot nicht-öffentlicher Daten im Wettbewerb mit gewerblichen Nutzern ergeben.[137] Offene Fragen bestehen auch in Bezug auf diesen Datenzugangsanspruch in erster Linie mit Blick auf die technischen Modalitäten der Datenbereitstellung.[138] Dazu gehören unter anderem die Fragen, welches »Mehr« an Anforderungen Art. 6 Abs. 10 DMA an den Echtzeitzugang im Vergleich zu Art. 6 Abs. 9 DMA verlangt sowie, welche Anforderungen sich vor dem Hintergrund, dass Gatekeeper nicht nur zur Teilung der Daten, sondern auch zur Ermöglichung ihrer Nutzung verpflichtet sind, an Datenformat und -qualität ergeben.

3.4 Art. 6 Abs. 11 DMA – Datenzugang für und gegen Suchmaschinenbetreiber

Der letzte im DMA enthaltene Datenzugangsanspruch findet sich in Art. 6 Abs. 11 DMA und kommt Wettbewerbern von Gatekeepern, die Online-Suchmaschinen betreiben, zugute.

3.4.1 Problem: Monopolisierter Markt für Online-Suchmaschinen

Mit Art. 6 Abs. 11 DMA hat der europäische Gesetzgeber die Bedeutung von Daten für den extrem monopolisierten Markt für Online-Suchmaschinen anerkannt – wie bereits in der Einleitung mit aufgenommen verfügt Google über einen weltweiten Marktanteil von rund 92 Prozent – und daher ebenfalls dem Regelungsbereich der Verordnung unterworfen.[139] Der wichtigste Qualitätsparameter, der die Wettbewerbsfähigkeit von Suchmaschinenbetreibern bestimmt, ist die wahrgenommene Relevanz der infolge einer Suchanfrage angezeigten Ergebnisse.[140] Und eine wichtige Rolle bei der Optimierung dieser Relevanz spielen die sogenannten »click-and-query data«.[141] Nach Einschätzung der *CMA* führt die größere Zahl an Suchanfragen

137 Darauf hinweisend, dass die beiden Vorschriften in Kombination miteinander gesehen werden müssen, Louven 2023, Rn. 142; mit Blick auf die Ausgestaltung der Vorschriften im Kommissionsentwurf wurde dem Dreiklang aus dem Datenverwendungsverbot, dem Zugangsrecht des gewerblichen Nutzers sowie dem Portabilitätsrecht des Endnutzers (das in der Fassung auch noch explizit den gewerblichen Nutzern zugutekommen sollte) sogar teilweise das Potential als »game changer« eingeräumt, vgl. Lundqvist 2021, S. 240.

138 Siehe auch Wolf-Posch 2023, Rn. 241.

139 Siehe dazu bereits Kerber 2021, S. 547.

140 CMA 2020, Rn. 3.13.

141 Ebd., Rn. 3.66.

zu einer Verbesserung von Googles Fähigkeit, relevantere Suchergebnisse im Vergleich zu denen seiner Wettbewerber anzuzeigen. Besonders deutlich trete dieser Effekt bei seltenen bzw. ungewöhnlichen Suchanfragen auf.[142] Alles in allem führe der Mangel an einem dem von Google vergleichbaren Umfang von »click-and-query data« zu einer verminderten Fähigkeit von Drittanbietern von Suchmaschinen, mit Google in den Wettbewerb zu treten.[143] Auch Erw.Gr. 61 DMA stellt die Bedeutung des Zugangs zu Ranking-, Anfrage-, Klick- und Ansichtsdaten für den erfolgreichen Betrieb einer Online-Suchmaschine heraus. Das Fehlen eines solchen stelle »ein beträchtliches Hindernis für einen Markteintritt oder eine Expansion dar, das die Bestreitbarkeit von Online-Suchmaschinen untergräbt«, weshalb Dritten ein solcher Zugang eingeräumt werden solle, um sie zur Optimierung ihrer Dienste und dadurch in ihrer Fähigkeit, »die Position der relevanten zentralen Plattformdienste angreifen [zu] können«, zu bestärken.

3.4.2 Gegenstand und Modalitäten des Zugangsanspruchs

Im Konkreten werden Gatekeeper gem. Art. 6 Abs. 11 DMA dazu verpflichtet, Drittunternehmen, die selbst Online-Suchmaschinen bereitstellen, auf deren Antrag hin Zugang zu Ranking-, Anfrage-, Klick und Ansichtsdaten in Bezug auf unbezahlte und bezahlte Suchergebnisse, die von Endnutzern über ihre Online-Suchmaschinen generiert werden, einzuräumen. Während auch diesem Zugangsanspruch erst auf Antrag der Zugangsberechtigten nachzukommen ist, wird von den Gatekeepern hier – im Gegensatz zu den Datenteilungspflichten aus den Art. 6 Abs. 8–10 DMA – keine kostenlose Bereitstellung der Daten erwartet, stattdessen ist der Zugang nur unter FRAND-Bedingungen (FRAND = fair, reasonable and non-discriminatory) einzuräumen.[144] Die Möglichkeit zur Erhebung von Entgelten für die Datenbereitstellung erscheint gerechtfertigt, nicht nur, weil die Gatekeeper nunmehr dazu verpflichtet werden, aktiv zur unmittelbaren Förderung der Angreifbarkeit ihrer eigenen Marktposition beitragen zu müssen, sondern auch wegen des sehr breit gefassten Zugangsgegenstands, an dessen Generierung die Zugangspetenten noch nicht einmal partizipiert haben.[145]

142 Ebd., Rn. 3.79.

143 Ebd.

144 Ausführlich zu Leitlinien zu diesen FRAND-Bedingungen, die sich aus der bisherigen Entscheidungspraxis ableiten lassen, Wolf-Posch 2023, Rn. 264 ff.

145 König 2023, Rn. 42.

Dieser wird lediglich dadurch eingegrenzt, dass die Daten einen »Bezug auf Suchergebnisse haben müssen.«[146] Ansonsten sind beispielsweise weder Beschränkungen auf zur Verbesserung von Online-Suchmaschinen notwendige oder nützliche Daten, noch auf Daten bestimmter Aktualitätsgrade vorgesehen.[147] Zudem erstreckt sich der Anwendungsbereich auch auf personenbezogene Daten, die gem. Art. 6 Abs. 11 S. 2 DMA zu anonymisieren sind – wobei die Anonymisierung gem. Erw.Gr. 61 DMA so erfolgen soll, dass weder Qualität noch Nutzbarkeit der Daten wesentlich beeinträchtigt werden.[148]

3.4.3 Bewertung, Hürden und offene Fragen

Als Datenzugangsanspruch, von dem unmittelbar Wettbewerber von Gatekeepern, die Online-Suchmaschinen betreiben, profitieren sollen, ist Art. 6 Abs. 11 DMA gänzlich anders gelagert als die bisher betrachteten Zugangsansprüche. Vorbehaltlich der zahlreichen noch offenen Fragen insbesondere mit Blick darauf, ob die Gatekeeper bspw. auch unter dieser Vorschrift einen Echtzeitzugang einräumen müssen[149] und wann die vom Gatekeeper angewandten Zugangsbedingungen den FRAND-Bedingungen gerecht werden, ist dieser Vorschrift wegen ihres breit gefassten Zugangsgegenstands Potential dahingehend einzuräumen, dass andere als die größten Anbieter von Online-Suchmaschinen auf Basis der dadurch erlangten Daten ihre eigenen Dienste verbessern können. In Anbetracht des Zielkonflikts, der sich aus der geforderten sicheren Anonymisierung personenbezogener Daten auf der einen und der Befähigung der Anbieter konkurrierender Online-Suchmaschinen zur Verbesserung ihrer Dienste auf Basis möglichst gut nutzbarer Datensätze auf der anderen Seite ergibt,[150] kommt – wie so häufig, wenn es um die Frage der Zulässigkeit der Weitergabe personenbezogener Daten geht – dem Aspekt der rechtssicheren Anonymisierung eine besondere Bedeutung zu. Hier ist zu hoffen, dass die Kommission entweder gemeinsam mit den Gatekeepern auf dem Weg des in Art. 8 Abs. 3 DMA vorgesehenen regulatorischen Dialogs oder alleine durch Wahrnehmung ihrer Kompetenz zum

146 Louven 2023, Rn. 165.
147 Vgl. Wolf-Posch 2023, Rn. 269 ff.
148 Kritisch zur Brauchbarkeit solcher wirksam anonymisierter Daten Hacker 2022, S. 1280 f.
149 Siehe dazu König 2023, Rn. 42.
150 Darauf bereits zum Kommissionsentwurf hinweisend Kerber 2021, S. 547.

Erlass von konkretisierenden Durchführungsrechtsakten nach Art. 8 Abs. 2 UAbs. 2 DMA eine adäquate Lösung entwirft.

V. Fazit und Ausblick

Der europäische Gesetzgeber hat mit dem DMA erste Schritte zurückgelegt, um die Daten der größten digitalen Plattformen unterschiedlichen Akteuren zugute zu öffnen und dadurch fairere und besser bestreitbare Märkte in der Plattformökonomie zu gewährleisten. Die vier näher betrachteten Datenzugangsansprüche in den Art. 6 Abs. 8–11 DMA weisen eine grundlegend gemeinsame Stoßrichtung auf, indem sie die Machtungleichgewichte, die sich aus den Eigenschaften digitaler Plattformen mit Bezug zu Fragen des Datenzugangs ergeben, adressieren und insbesondere eine Teilhabe von Endnutzern und gewerblichen Nutzern an solchen Daten ermöglichen, an deren Generierung sie selbst partizipiert haben. Im Einzelnen unterscheiden sich die jeweiligen Vorschriften jedoch erheblich, sowohl bezüglich der konkret adressierten Problemstellungen (so fokussieren Art. 6 Abs. 8 und 11 DMA sich explizit auf den Online-Werbemarkt respektive den Markt für Online-Suchmaschinen),[151] als auch bei näherer Betrachtung einzelner Aspekte der Zugangsmodalitäten (beispielhaft sei nochmals auf die unterschiedlichen Formulierungen in Bezug auf die Einräumung eines Echtzeit-Datenzugangs in Art. 6 Abs. 9 und 10 DMA hingewiesen). Auch der Aspekt der Aufrechterhaltung von Investitionsanreizen für die zur Datenteilung Verpflichteten hat in den Vorschriften auf unterschiedliche Art Berücksichtigung erfahren: Im Rahmen der Art. 6 Abs. 9 und 10 DMA durch die Beschränkung der Zugangsberechtigten auf lediglich solche Akteure, die selbst an der Generierung der von den Ansprüchen erfassten Daten partizipiert haben und im Rahmen des Zugangsanspruchs zu Suchmaschinen-Daten gemäß Art. 6 Abs. 11 DMA durch die dort vorgesehene Möglichkeit, unter FRAND-Bedingungen eine Kompensation für die Datenbereitstellung zu verlangen. Inwiefern sich die neuen Regelungen zur Erreichung der mit ihnen jeweils verfolgten Ziele eignen, wird sich zwar erst noch in der Praxis zeigen müssen – mindestens die vorgesehenen Echtzeit-Datenzugänge

151 Die von Brieske/Schweitzer in diesem Band festgestellte Verortung subjektiver Rechte »in ganz spezifische Problemkonstellationen« (dort in Bezug auf DSGVO, DGA und DA) ist insofern auch mit Blick auf den DMA zu identifizieren.

scheinen jedoch vielversprechend zu sein hinsichtlich der Befähigung von Wettbewerbern zur Entwicklung datenbasierter Konkurrenzprodukte.[152] Für eine Reihe an offenen (Auslegungs-)Fragen – insbesondere mit Bezug zu den Modalitäten der Zugangsgewährung sowie den jeweils umfassten Daten – stehen mit dem Instrument des regulatorischen Dialogs in Art. 8 Abs. 3 DMA sowie der Kompetenz der Kommission gem. Art. 8 Abs. 2 UAbs. 2 DMA zum Erlass von Durchführungsrechtsakten, in denen sie Maßnahmen festlegen kann, mit denen die Gatekeeper ihren Verpflichtungen aus Art. 6 und 7 DMA wirksam nachzukommen haben, zumindest schon Lösungsansätze bereit. In Anbetracht des massiven Kompetenzaufwuchses der Kommission in den letzten Jahren[153] bleibt allerdings zu hoffen, dass sie von diesen Optionen auch angemessen Gebrauch machen kann. Diese Hoffnung gilt für andere Aspekte nicht, wie etwa die im Kontext des Art. 6 Abs. 8 DMA angesprochene Frage, ob ein Mehr an Wissen bezüglich des Erfolgs und der Kosten von Werbemaßnahmen dazu geeignet ist, tatsächlich positiv auf die Wechselfähigkeit der Werbetreibenden und Herausgeber einzuzahlen. Alles in allem ist abschließend noch einmal hervorzuheben, dass die hier näher betrachtete Big-Tech-Regulierung durch den DMA in der Gesamtschau mit weiteren aktuellen Rechtsakten gesehen werden muss. Beispielhaft können hier die Aufnahme der Datenzugangsverweigerung als missbräuchliches Verhalten von marktbeherrschenden Unternehmen in § 19 Abs. 2 Nr. 4 GWB,[154] die Pflicht von sehr großen Online-Plattformen zur Berücksichtigung ihrer datenbezogenen Praxis bei der Ermittlung der von ihnen ausgehenden systemischen Risiken gem. Art. 34 Abs. 2 UAbs. 1 lit. e DSA, die größen- und umsatzunabhängigen Transparenzverpflichtungen aus der P2B-VO, sowie der Ausschluss von Gatekeepern von den im Data Act vorgesehenen Datenzugriffsmöglichkeiten gem. Art. 5 Abs. 3 sowie Art. 6 Abs. 2 lit. d DA genannt werden.

152 Auf die Notwendigkeit eines Echtzeitzugangs bereits 2019 hinweisend Schweitzer 2019a, S. 577.
153 Siehe exemplarisch die Übersicht von Pfeiffer/Helmke 2023.
154 Siehe hierzu Huerkamp/Nuys 2021.

Literatur

Achleitner, Ranjana A. (2022): Digital Markets Act beschlossen: Verhaltenspflichten und Rolle nationaler Wettbewerbsbehörden, in: *Neue Zeitschrift für Kartellrecht (NZKart)*, Heft 7, S. 359–366.

Armstrong, Mark (2006): Competition in two-sided markets, in: *The RAND Journal of Economics (RJE)*, Heft 3, S. 668–691.

Bamberger, Kenneth A./Lobel, Orly (2017): Platform Market Power, in: *Berkeley Technology Law Journal (BTLJ)*, Heft 3, S. 1052–1092.

Bostoen, Friso/Mândrescu, Daniel (2020): Assessing abuse of dominance in the platform economy: a case study of app stores, in: *European Competition Journal (ECJ)*, S. 431–491.

Brandt, Elena/Grewe, Max (2023): Datenportabilität 2.0. Neue Vorgaben im Zuge der EU-Digitalstrategie, in: *Multimedia und Recht (MMR)*, Heft 12, S. 928–932.

Bundeskartellamt (2022): Sektoruntersuchung Online-Werbung. Diskussionsbericht, Az. B6-25/18, Bonn.

Bundeskartellamt (2023): Sektoruntersuchung Online-Werbung. Zusammenfassender Abschlussbericht, Az. B6-25/18, Bonn.

Burchardi, Sophie (2022): Die Selbstbegünstigung von Plattformunternehmen im Fokus des Kartell- und Regulierungsrechts, in: *Neue Zeitschrift für Kartellrecht (NZKart)*, Heft 11, S. 610–616.

Busch, Christoph (2019): Mehr Fairness und Transparenz in der Plattformökonomie? Die neue P2B-Verordnung im Überblick, *Gewerblicher Rechtsschutz und Urheberrecht (GRUR)*, Heft 8, S. 788–796.

Caillaud, Bernard/Jullien, Bruno (2003): Chicken & egg: competition among intermediation service providers, in: *The RAND Journal of Economics (RJE)*, Heft 2, S. 309–328.

CMA [= Competition and Markets Authority] (2020): *Online platforms and digital advertising. Market study final report*, 1. Juli 2020, https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study [29.4.2024].

Crémer, Jacques/de Montjoye, Yves-Alexandre/Schweitzer, Heike (2019): *Competition policy for the digital era*, Luxemburg, https://op.europa.eu/de/publication-detail/-/publication/21dc175c-7b76-11e9-9 f05-01aa75ed71a1 [29.4.2024].

Dewenter, Ralf/Linder, Melissa (2017): Bestimmung von Marktmacht in Plattformmärkten, in: *List Forum für Wirtschafts- und Finanzpolitik*, Heft 2, S. 67–87.

Engert, Andreas (2018): Digitale Plattformen, in: *Archiv für die civilistische Praxis (AcP)*, Heft 2–4, S. 305–374.

Europäische Kommission (2023a): *Digital Markets Act: Commission designates six gatekeepers*, Pressemitteilung, 6. September 2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4328 [29.4.2024].

Europäische Kommission (2023b): Durchführungsverordnung (EU) 2023/814 der Kommission vom 14. April 2023 zur Festlegung detaillierter Vorschriften für die Durchführung bestimmter Verfahren durch die Kommission nach der Verordnung (EU) 2022/1925 des Europäischen Parlaments und des Rates (Text von Bedeutung für den

EWR), Amtsblatt L 102 vom 17.04.2023, https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32023R0814 [29.4.2024].

Europäische Kommission (2020a): *Eine europäische Datenstrategie*, COM (2020) 66 final, Brüssel, https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52020DC0066 [29.4.2024].

Europäische Kommission (2020b): Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über bestreitbare und faire Märkte im digitalen Sektor, COM (2020) 842 final, Brüssel.

Evans, David S./Schmalensee, Richard (2013): The Antitrust Analysis of Multi-Sided Platform Businesses, in: *NBER Working Papers*, No. 18783, http://www.nber.org/papers/w18783 [29.04.2024].

Fast, Victoria/Schnurr, Daniel/Wohlfahrth, Michael (2019): Marktmacht durch Daten: Eine Analyse aus ökonomischer Perspektive, in: Specht-Riemenschneider, Louisa/Werry, Nikola/Werry, Susanne (Hg.): *Datenrecht in der Digitalisierung*, Berlin, S. 745–778.

Fitri, Afiq (2022): Big Tech now accounts for more than half of global internet traffic, in: *Tech Monitor*, 16. Februar 2022, https://techmonitor.ai/technology/networks/big-tech-accounts-for-over-half-of-global-internet-traffic [29.4.2024].

Gasser, Lucas/Hegener, Jochen (2023): § 6 Verhaltenspflichten für Torwächter (Art. 5–7 DMA), in: Schmidt, Jens P./Hübener, Fabian (Hg.): *Das neue Recht der digitalen Märkte. Digital Markets Act (DMA)*, Baden-Baden.

Gasser, Lucas (2021): Der Marktstrukturmissbrauch in der Plattformökonomie. Informationsasymmetrien als Ausgangspunkt eines Verstoßes gegen Art. 102 AEUV, Baden-Baden.

Geminn, Christian L. (2020): Betroffenenrechte verbessern. Überarbeitungsbedarf der Datenschutz-Grundverordnung, in: *Datenschutz und Datensicherheit (DuD)*, Heft 5, S. 307–311.

Gill, Daniel/Metzger, Jakop (2022): Data Access Through Data Portability. Economic and Legal Analysis of the Applicability of Art. 20 GDPR to the Data Access Problem in the Ecosystem of Connected Cars, in: *European Data Protection Law Review (EDPL)*, Heft 3, S. 221–237.

Gineikyte, Vaida/Barcevicius, Egidijus/Cibaite, Guoda (2021): *Business user and third-party access to online platform data*, Analytical Paper 5 of the EU Observatory on the Online Platform Economy.

Graef, Inge (2019): Differentiated Treatment in Platform-to-Business Relations: EU Competition Law and Economic Dependence, in: *Yearbook of European Law (YEL)*, S. 448–499.

Greiner, Ben/Teubner, Timm/Weinhardt, Christof (2018): Grundfragen der Plattformökonomie – wie man Vertrauen designt, in: Blaurock, Uwe/Schmidt-Kessel, Martin/Erler, Katharina (Hg.): *Plattformen. Geschäftsmodelle und Verträge*, Baden-Baden, S. 59–75.

Hacker, Philipp (2022): KI und DMA – Zugang, Transparenz und Fairness für KI-Modelle in der digitalen Wirtschaft, in: *Gewerblicher Rechtsschutz und Urheberrecht (GRUR)*, Heft 17–18, S. 1278–1285.

Hartl, Andreas/Ludin, Anna (2021): Recht der Datenzugänge. Was die Datenstrategien der EU sowie der Bundesregierung für die Gesetzgebung erwarten lassen, in: *Multimedia und Recht (MMR)*, Heft 7, S. 534–538.

Haucap, Justus (2020): Plattformökonomie: neue Wettbewerbsregeln – Renaissance der Missbrauchsaufsicht, in: *Wirtschaftsdienst*, Heft 13, S. 20–29.

Haucap, Justus (2018): Daten als Wettbewerbsfaktor, in: *Wirtschaftsdienst*, Heft 7, S. 472–477.

Haus, Florian C./Cesarano, Carlos D. (2020): Ausbeutungs- und Behinderungsmissbrauch in zweiseitigen Märkten – zugleich Anmerkung zum Beschluss des BGH in Sachen Facebook, in: *Neue Zeitschrift für Kartellrecht (NZKart)*, Heft 10, S. 521–525.

Hein, Andreas/Böhm, Markus/Krcmar, Helmut (2019): Digitale Plattformen, in: Dahm, Markus H./Thode, Stefan (Hg.): *Strategie und Transformation im digitalen Zeitalter. Inspirationen für Management und Leadership*, Wiesbaden, S. 181–200.

Herbers, Björn (2022): Der Digital Markets Act (DMA) kommt – neue Dos and Don'ts für Gatekeeper in der Digitalwirtschaft, in: *Recht Digital (RDi)*, Heft 6, S. 252–259.

Herbers, Björn/Savary, Fiona/Gröf, Sophia C. (2023): Die Revolution der Digitalregulierung in Aktion – Umsetzung des Digital Markets Act durch die EU, Gewerblicher Rechtsschutz und Urheberrecht, in: *Gewerblicher Rechtsschutz und Urheberrecht in der Praxis (GRUR-Prax)*, Heft 6, S. 151–153.

Higer, Daniel/Patt, Constantin (2024): »Kampf gegen Windmühlen« – ist eine Abwendung der Gatekeeper-Benennung nach dem DMA tatsächlich überhaupt möglich?, in: *Neue Zeitschrift für Kartellrecht (NZKart)*, Heft 2, S. 78–84.

Hoffer, Raoul/Lehr, Leo A. (2019): Onlineplattformen und Big Data auf dem Prüfstand. Gemeinsame Betrachtung der Fälle Amazon, Google und Facebook, in: *Neue Zeitschrift für Kartellrecht (NZKart)*, Heft 1, S. 10–20.

Huerkamp, Florian/Nuys, Marcel (2021): Datenzugang nach § 19 Abs. 2 Nr. 4 GWB n.F. – Geglückte »Klarstellung«?, in: *Neue Zeitschrift für Kartellrecht (NZKart)*, Heft 6, S. 327–332.

Hutchinson, Christophe S./Treščáková Diana (2022): Tackling gatekeepers' self-preferencing practices, in: *European Competition Journal (ECJ)*, Heft 3, S. 567–590.

Jackwerth, Karin (2022): Great expectations: the Facebook case and subsequent legislative approaches to regulate large online platforms and digital markets, in: *Journal of Intellectual Property, Information Technology and E-Commerce Law (JIPITEC)*, Heft 3, S. 200–223.

Jaekel, Michael (2017): Die Macht der digitalen Plattformen. Wegweiser im Zeitalter einer expandierenden Digitalsphäre und künstlicher Intelligenz, Wiesbaden.

Katz, Michael L./Shapiro, Carl (1985): Network Externalities, Competition, and Compatibility, in: *American Review of Economics (Am. Econ. Rev.)*, Heft 3, S. 424–440.

Kerber, Wolfgang (2021): Datenrechtliche Aspekte des Digital Markets Act. Datenwirtschaftsrecht I: Vorschlag einer Ex-ante-Regulierung von Gatekeeper-Plattformen, in: *Zeitschrift für Datenschutz (ZD)*, Heft 10, S. 544–548.

Kestler, Lukas (2023): Strukturelle Abhilfemaßnahmen – erste (An-)Zeichen einer neuen Zeit?, in: *Neue Zeitschrift für Kartellrecht (NZKart)*, Heft 9, S. 463–467.

Kieß, Fabian (2023): Regulierung von digitalen Plattform-Ökosystemen. Implikationen durch § 19a GWB und Digital Markets Act, Baden-Baden.

König, Carsten (2023): § 13 Verhaltenspflichten für Torwächter, in: Steinrötter, Björn (Hg.): *Europäische Plattformregulierung. DSA | DMA | P2B-VO | DGA | DA | AI Act | DSM-RL*, Baden-Baden.

Krämer, Jan (2018): Datenschutz 2.0 – ökonomische Auswirkungen von Datenportabilität im Zeitalter des Datenkapitalismus, in: *Wirtschaftsdienst*, Heft 7, S. 466–469.

Krämer, Jan/Senellart, Pierre/de Streel, Alexandre (2020): *Making Data Portability More Effective for the Digital Economy. Economic Implications and Regulatory Challenges*, Centre on Regulation in Europe (CERRE) Report, https://cerre.eu/wp-content/uploads/2020/07/cerre_making_data_portability_more_effective_for_the_digital_economy_june2020.pdf [29.4.2024].

Krauskopf, Johanna/Brösamle, Markus (2023): § 4 Benennung als Torwächter (Art. 3 DMA), in: Schmidt, Jens P./Hübener, Fabian (Hg.): *Das neue Recht der digitalen Märkte. Digital Markets Act (DMA)*, Baden-Baden.

Kumkar, Lea K. (2022): Der Digital Markets Act nach dem Trilog-Verfahren. Neue Impulse für den Wettbewerb auf digitalen Märkten, in: *Recht Digital (RDi)*, S. 347–354.

Louven, Sebastian (2023): Art. 6 DMA, in: Gersdorf, Hubertus/Paal, Boris P. (Hg.): *BeckOK Informations- und Medienrecht*, 41. Edition, Stand 01.08.2023, München, Rn. 1–210.

Louven, Sebastian (2019): Marktmacht durch Daten: Eine Analyse aus rechtswissenschaftlicher Perspektive, in: Specht-Riemenschneider, Louisa/Werry, Nikola/Werry, Susanne (Hg.): *Datenrecht in der Digitalisierung*, Berlin, S. 779–820.

Lundqvist, Björn (2021): The Proposed Digital Markets Act and Access to Data: A Revolution, or Not?, in: *International Review of Intellectual Property and Competition Law (IIC)*, S. 239–241.

Mendelsohn, Juliane/Budzinski, Oliver (2023): § 2 Hintergrund, Ziele und wettbewerbspolitische Einordnung des DMA, in: Schmidt, Jens P./Hübener, Fabian (Hg.): *Das neue Recht der digitalen Märkte. Digital Markets Act (DMA)*, Baden-Baden.

Monopolkommission (2021): *Sondergutachten 82. Empfehlungen für einen effektiven und effizienten Digital Markets Act. Sondergutachten der Monopolkommission gemäß § 44 Abs. 1 Satz 4 GWB*, Bonn, https://www.monopolkommission.de/images/PDF/SG/sg_dma_volltext.pdf [29.4.2024].

Motta, Massimo/Peitz, Martin (2020): *Intervention triggers and underlying theories of harm. Expert advice for the Impact Assessment of a New Competition Tool*, Luxemburg, https://op.europa.eu/de/publication-detail/-/publication/0165 f92c-14dd-11eb-b57e-01aa75ed71a1/language-en [29.4.2024].

Nocun, Katharina (2018): Datenschutz unter Druck. Fehlender Wettbewerb bei sozialen Netzwerken als Risiko für den Verbraucherschutz, in: Roßnagel, Alexander/Friedewald, Michael/Hansen, Marit (Hg.): *Die Fortentwicklung des Datenschutzes. Zwischen Systemgestaltung und Selbstregulierung*, Wiesbaden, S. 39–58.

OECD [= Organization for Economic Development and Cooperation] (2019): *An Introduction to Online Platforms and their Role in the Digital Transformation*, Paris, https://www.

oecd.org/innovation/an-introduction-to-online-platforms-and-their-role-in-the-digital-transformation-53e5 f593-en.htm [29.4.2024].

Pfeiffer, Lars (2024): Datenzugang in der Plattformökonomie: Regulierungsinstrumente in P2B-VO, DMA und DSA, in: Buchheim, Johannes/Kraetzig, Viktoria/Mendelsohn, Juliane/Steinrötter, Björn (Hg.): *Plattformen. Grundlagen und Neuordnung des Rechts digitaler Plattformen*, Baden-Baden, S. 53–75.

Pfeiffer, Lars/Helmke, Jan T. (2023): Die Digitalrechtsakte der EU (DGA, DSA, DMA, KI-VO-E und DA-E) – Teil IV, in: *ZD-Aktuell*, Heft 11, S. 01206.

Podszun, Rupprecht (2023): Einleitung, in: ders. (Hg.): *Digital Markets Act. Gesetz über digitale Märkte*, Baden-Baden.

Podszun, Rupprecht /Bongartz, Philipp/Langenstein, Sarah (2021): The Digital Markets Act: Moving from Competition Law to Regulation for Large Gatekeepers, in: *Journal of European Consumer and Market Law (EuCML)*, Heft 2, S. 60–67.

Prüfer, Jens (2020): *Die Datenteilungspflicht. Innovation und fairer Wettbewerb auf datengetriebenen Märkten*, Studie im Auftrag der Friedrich-Ebert-Stiftung, Bonn, https://library.fes.de/pdf-files/fes/15990.pdf [29.4.2024].

Richter, Heiko/Globocník, Jure (2022): Rechte an Daten und Datenzugangsrechte, in: Chibanguza, Kuuya J./Kuß, Christian/Steege, Hans (Hg.): *Künstliche Intelligenz. Recht und Praxis automatisierter und autonomer Systeme*, Baden-Baden, S. 93–110.

Rysman, Marc (2009): The Economics of Two-Sided Markets, in: *Journal of Economic Perspectives (JEP)*, Heft 3, S. 125–143.

Schröder, Meinhard (2019): ›Paradigm Shift‹ im Datenschutzrecht? – Wirtschaftsverwaltungsrechtliche Instrumente in der Datenschutz-Grundverordnung, in: Krönke, Christoph (Hg.): *Regulierung in Zeiten der Digitalwirtschaft*, Tübingen, S. 13–28.

Schweitzer, Heike (2019a): Datenzugang in der Datenökonomie. Eckpfeiler einer neuen Informationsordnung, in: *Gewerblicher Rechtsschutz und Urheberrecht (GRUR)*, Heft 6, S. 569–580.

Schweitzer, Heike (2019b): Digitale Plattformen als private Gesetzgeber. Ein Perspektivwechsel für die europäische »Plattform-Regulierung«, in: *Zeitschrift für Europäisches Privatrecht (ZEuP)*, Heft 1, S. 1–12.

Schweitzer, Heike/Metzger, A (2023): Data Access under the Draft Data Act, Competition Law and the DMA: Opening the Data Treasures for Competition and Innovation?, in: *Gewerblicher Rechtsschutz und Urheberrecht International (GRUR Int.)*, Heft 4, S. 337–356.

Schweitzer, Heike/Metzger, Axel/Blind, Knut/Richter, Heiko/Niebel, Crispin/Gutmann, Frederik (2022*): Data access and sharing in Germany and in the EU: Towards a coherent legal framework for the emerging data economy. A legal, economic and competition policy angle*, Study on behalf of the BMWK, Final Report, 8. Juli 2022.

Schweitzer, Heike/Haucap, Justus/Kerber, Wolfgang/Welker, Robert (2018): *Modernisierung der Missbrauchsaufsicht für marktmächtige Unternehmen*, Baden-Baden.

Schweitzer, Heike/Fetzer, Thomas/Peitz, Martin (2016): *Digitale Plattformen: Bausteine für einen künftigen Ordnungsrahmen*, Zentrum für Europäische Wirtschaftsforschung (ZEW), Discussion Paper No. 16–042, http://ftp.zew.de/pub/zew-docs/dp/dp16042.pdf [29.4.2024].

Seeliger, Daniela (2023): Art. 8, in: Podszun, Rupprecht (Hg.): *Digital Markets Act. Gesetz über digitale Märkte*, Baden-Baden.

Sperlich, Tim (2017): Das Recht auf Datenübertragbarkeit, in: *Datenschutz und Datensicherheit (DuD)*, Heft 6, S. 377–377.

Statista.com (2024a): *Market share of leading search engines worldwide from January 2015 to January 2024*, 12. Februar 2024, https://www.statista.com/statistics/1381664/worldwide-all-devices-market-share-of-search-engines/ [29.4.2024].

Statista.com (2024b): *Media usage in an internet minute as of December 2023*, 2. Januar 2024, https://www.statista.com/statistics/195140/new-user-generated-content-uploaded-by-users-per-minute/ [29.4.2024].

Statista.com (2024c): *Anzahl der Visits von youtube.com von Mai 2019 bis November 2023*, 2. Januar 2024, https://de.statista.com/statistik/daten/studie/1021459/umfrage/anzahl-der-visits-pro-monat-von-youtube/ [29.4.2024].

Statista.com (2024d): *Worldwide visits to Amazon.com from July 2023 to December 2023*, 13. Februar 2024, https://www.statista.com/statistics/623566/web-visits-to-amazoncom [29.4.2024].

Statista.com (2024e): *Anzahl der Daily Active Users (DAUs) von Facebook weltweit vom 1. Quartal 2009 bis zum 4. Quartal 2023*, 2. Februar 2024, https://de.statista.com/statistik/daten/studie/222135/umfrage/taeglich-aktive-facebook-nutzer-weltweit/ [29.04.2024].

Statista.com (2024 f): *Anzahl der versendeten WhatsApp-Nachrichten pro Tag weltweit in ausgewählten Monaten von Oktober 2011 bis Oktober 2020*, 29. Januar 2024, https://de.statista.com/statistik/daten/studie/868733/umfrage/anzahl-der-taeglich-verschickten-whatsapp-nachrichten-weltweit/ [29.4.2024].

Tombal, Thomas (2020): Economic Dependence and Data Access, in: *International Review of Intellectual Property and Competition Law (IIC)*, S. 70–98.

Veldkamp, L (2023): Valuing Data as an Asset, in: *Review of Finance (RoF)*, Heft 5, S. 1545–1562.

Volmar, Maximilian (2019): *Digitale Marktmacht*, Baden-Baden.

Wais, Hannes (2023): Datenzugang des gewerblichen Plattformnutzers und Grundlagen der Privatautonomie, in: *Zeitschrift für Europäisches Privatrecht (ZEuP)*, Heft 3, S. 582–606.

Wischmeyer, Thomas/Herzog, Eva (2020): Daten für alle? – Grundrechtliche Rahmenbedingungen für Datenzugangsrechte, in: *Neue Juristische Wochenschrift (NJW)*, Heft 5, S. 288–293.

Wolf-Posch, Anna (2023): Art. 6 Abs. 8–11, in: Podszun, Rupprecht (Hg.): *Digital Markets Act. Gesetz über digitale Märkte*, Baden-Baden.

Zugangsverschränkungen: Neue Datenwelt und die alte Welt der Körper

Die Datafizierung der Welt[1]

Daniel Lambach

Einleitung

Diskussionen über die Datafizierung der Gesellschaft sind inzwischen allgegenwärtig (Houben/Prietl 2018, Mayer-Schönberger/Cukier 2013). Orakelte man noch vor nicht allzu langer Zeit von der »Wissensgesellschaft«, der »Informationsgesellschaft« oder der »Netzwerkgesellschaft«, ergänzt der Begriff der »Datengesellschaft« seit neuestem diesen Reigen an Gesellschaftsdiagnosen.[2] In der Datengesellschaft ergeben sich Sorgen über den Schutz individueller Daten und der Privatsphäre, rechtliche Probleme der Lokalisierbarkeit der Daten sowie datenethische Fragen. Dies sind offenkundig wichtige Herausforderungen für die Sozial-, Rechts- und Geisteswissenschaften. So ist auch dieser Sammelband als eine weitere Auseinandersetzung mit der Frage zu verstehen, wer Zugang zu welchen Daten haben soll.

Datafizierung bezeichnet den Prozess, in dem verschiedene Aspekte des Lebens in Daten überführt und abgebildet werden (Mayer-Schönberger/Cukier 2013). Dies ist keine Neuigkeit – schon immer wurden Dinge gezählt, vermessen und berechnet. Neu ist jetzt vor allem die Skala des Phänomens (»big data«) sowie die automatisierte maschinelle Verarbeitung dieser Daten und deren Weiterverarbeitung in neue Daten. Beispiele aus der Arbeits- und Gesellschaftswelt gibt es genug, von der Überwachung des Arbeitsverhaltens am Computer im Homeoffice bis zur Sammlung hochpersönlicher Gesundheitsdaten durch Smartwatches. Das Ausmaß dieses Prozesses ist so groß,

1 Ich danke Jasmin Brieske, Petra Gehring, Lars Pfeiffer und Doris Schweitzer für die hilfreichen Kommentare zu früheren Versionen des Textes.

2 Ich danke Petra Gehring für diesen Hinweis. Über die tiefere Bedeutung dieses Komplexitätsrückschritts von Wissen über Information zu Daten ließe sich noch sehr viel mehr diskutieren.

dass es jenseits von mehr Quantität auch eine neue Qualität annimmt. Datafizierung verändert die Gesellschaft.

Datafizierung ist jedoch ein allgegenwärtiger Prozess, der über menschliche Daten hinaus geht. In Datafizierungsdiskussionen wird aber diese Totalität des Prozesses nicht immer angemessen reflektiert. Der Fokus ist oft anthropozentrisch und die Daten, um die es in diesen Diskussionen geht, personenbezogen. Ich bestreite nicht, dass personenbezogene Daten und deren Regulierung eminent wichtige Probleme von grundsätzlicher Relevanz für unser Zusammenleben sind. Wie Jasmin Brieske und Doris Schweitzer in diesem Band argumentieren, verändert die Datafizierung den durch die Gesellschaft ausgeübten Prozess der Subjektivierung. Daher liegt das Befassen mit Daten anhand von deren Verknüpftheit mit Personen nahe. Allerdings argumentiere ich, dass wir zusätzlich zu diesen bereits stattfindenden Diskussionen auch die Datafizierung nicht-menschlicher Objekte stärker wahrnehmen sollten: die Umwelt, Maschinen, natürliche Phänomene, Tiere. Auch Algorithmen und Daten selbst erzeugen ständig neue Metadaten oder Paradaten. In diesem Beitrag befasse ich mich mit der Datafizierung der Umwelt, sowohl der natürlichen als auch der gebauten. Meine Grundannahme ist analog zu der Aussage von Brieske und Schweitzer: Gesellschaften haben bestimmte Beziehungen zu ihrer Umwelt, schaffen Umwelten, prägen sie, geben ihnen Bedeutung. Datafizierung verändert auch diesen Prozess der »Umweltivierung« der Umwelt. Wenn ich hierbei von Datafizierung spreche, dann meine ich die neoliberale, kapitalistische, westliche Spielart dieses Phänomens, die von Verwissenschaftlichung, Managerialismus und dem Streben nach Inwertsetzung geprägt ist.

Barry Ryan schildert eindrücklich, wie datengetriebene Konzepte mariner Raumplanung unseren Umgang mit den Ozeanen verändern: »Maritime spatial planning tends to standardize or routinize sea-space. […] By being able to scientifically analyse, plan and predict the usage of space it acquires an economic worth. A hierarchy of value is constructed – some spaces are deemed to be more productive than other spaces and a market comes into being. […] This structure is designed to manage vast three-dimensional, inhospitable environments through a network of secure routes connecting orderly, gentrified sites. The socio-technical imaginary at stake is a global network of secured zones that act as rational hubs of wealth creation and environmental management in the maritime sphere« (Ryan 2015, S. 579–580). Vergleichbare Prozesse finden wir in der Erstellung digitaler Karten und Katastersysteme,

der Vermessung von Umweltphänomenen (Wetter, Klima, Böden usw.), der Digitalisierung von Bauten oder der Anfertigung von Statistiken über landwirtschaftliche Produktivität, Größe und Bewegung von Fisch- und Vogelschwärmen etc.

Im Umgang mit der Datafizierung besteht ein grundsätzlicher Wertekonflikt. Die philosophische Grundfrage ist, ob unser »Weltwissen« Teil eines globalen Gemeingutes (*global commons*) ist bzw. sein sollte oder ob Teile dieses Wissens legitimerweise Privateigentum sein sollten. Die erste Position steht hinter dem aufklärerischen Ideal einer Wissenschaft, die durch freien Austausch von Theorien, Daten, Methoden und Ergebnissen zu einem Menschheitsprojekt des wissenschaftlichen Fortschritts beiträgt. Selbst in der schwersten Phase des Kalten Krieges fand sich die internationale Forschungsgemeinschaft zum Internationalen Geophysikalischen Jahr 1957–58 zusammen, das große Fortschritte z. B. in der Polarforschung erbrachte (Collis/Dodds 2008). »Weltdatenzentren« sorgten für den Austausch gewonnener Daten über Blockgrenzen hinweg. Demgegenüber steht eine eher ökonomisch motivierte Sichtweise, die für die zumindest teilweise Privatheit gewonnener Daten argumentiert. Diese Position betont den Aufwand, der mit dem Sammeln und Kuratieren von Daten verbunden ist und setzt auf Eigentumsrechte, um Anreize für Innovation und Inwertsetzung zu geben. Man muss hier sicherlich differenzieren. Daten über das Erdsystem verdienen einen anderen rechtlichen und ethischen Status als Daten über einen industriellen Kontrollprozess, der sich auf einem privaten Firmengelände abspielt. In diesem Text schere ich alles über einen Kamm, weil ich herausstellen möchte, wie groß die Datensphäre im Bereich nicht-menschlicher Daten ist. Man darf dabei nur nicht vergessen, dass dieser Bereich von *more-than-human*-Daten ein heterogenes Konstrukt ist, das unterschiedliche Arten von Daten zusammenfasst.

Mittels des Begriffs der Datensphäre wählt dieser Beitrag eine räumliche Perspektive auf den Prozess der Datafizierung, welcher im folgenden Abschnitt näher erläutert und begründet. Damit möchte ich vor allem zwei Dinge erreichen: erstens ermöglicht eine räumliche Perspektive einen Fokus auf Grenzen (im Sinne von Zugangsbeschränkungen) in der Datensphäre. Zweitens erlaubt sie uns, die Interaktion des Datenraums mit der sozialen und der physischen Welt sowie deren wechselseitige Effekte herauszuarbeiten. Exemplarisch tue ich dies anhand der Implikationen, welche die Entwicklung der Datensphäre für politische Steuerung hat. Hier argumentiere ich, dass Daten eine Faktizität zugeschrieben wird, durch welche sie

unkritisch als Repräsentanten komplexer Sachverhalte konstruiert werden. Auf diese Weise informieren Daten politische Entscheidungsprozesse, wenn auch z.T. in irreführender Weise.

Datafizierung als Entstehung der Datensphäre

Daten sind Zeichen, also etwas Bezeichnendes, das auf ein Ding verweist. Datafizierung impliziert in diesem Sinne die Entstehung eines umfassenden Systems von Verweisen und Abbildungen des »Realen« bzw. der physischen Welt. Diese Daten sind aggregiert in Datensätze – lokale Anhäufungen von Daten, die teils miteinander vernetzt sind. Auch wenn die Vernetzung dieser Datenklumpen uneinheitlich ist, übernehme ich für ihre Totalität den Begriff der »Datensphäre«. Bergé, Grumbach und Zeno-Zencovich bezeichnen damit »a new space – a digital sphere – which constitutes a reflection of the physical world, containing both the objects we find in it (buildings, roads, plants, animals and landscapes) and the traces of the activity occurring in the physical world, such as our position at any given moment, our exchanges, the temperature of our homes, financial movements and movements of goods or road traffic« (2018, S. 145). Dieser Datenraum schafft Affordanzen für Neues, z.B. das Indexieren, Durchsuchen und Transformationen von Daten und Informationen aus der physischen Welt, sowie für die Digitalisierung von Aktivitäten (siehe insbesondere zu Googles Aktivitäten den Beitrag von Lars Pfeiffer in diesem Band).

Ich gehe hier von einem Raumkonzept aus, das von Theorien der kritischen Geografie und Raumsoziologie inspiriert ist (vgl. allgemein Agnew 1998, Massey 2005, Löw 2016). Ein Raum ist darin zunächst nicht mehr als eine Ausdehnung sowie eine Unterscheidung zwischen Innen und Außen (Malpas 2012). Dieser Raum kann in verschiedenen »Ontologien« gedacht werden, beispielsweise als Territorium, Ort, Landschaft oder Netzwerk, welche jeweils konkretere theoretische Annahmen machen (Lambach 2022a). Dieser Zugang ist für eine Analyse des bislang noch kaum ausformulierten Konzepts der »Datensphäre« in mehrfacher Hinsicht fruchtbar. Erstens ermöglicht er einen pragmatischen Umgang mit der Skalarität der Datensphäre, also der Beschaffenheit und des Eingebettetseins von Datenbeständen von der Mikro- bis zur Makroebene. Zweitens hebt sie die Bedeutung von Grenzen und Übergängen sowohl nach Außen als auch in ihrem Inneren her-

vor. Drittens richtet er unsere Aufmerksamkeit auf die soziale Konstruiertheit des Datenraums, der als »Neuland« und zu kolonisierende Heimat von Daten-Schätzen porträtiert wird. Damit werden auch die Spannungen zwischen der netzwerkartigen Architektur von Computersystemen und Datenbanken und einer territorialen Behandlung als »Parzellen« deutlich (Jessop u.a. 2008).

Eine räumliche Perspektive hilft auch als Korrektiv eines unter Netzwerkansätzen verbreiteten Fehlschlusses. Diese Ansätze postulieren eine »flache Ontologie« von Netzwerken, also die Annahme, dass es keine Prioritäten unter den Knotenpunkten eines Netzwerks gebe (Epstein 2018). Dies mag eine brauchbare Ausgangsheuristik sein, die einer analytischen Überprüfung standhalten muss, allerdings wird sie theoretisch wie praktisch oft als starke Annahme behandelt, wonach Netzwerke auch tatsächlich »flach« *sind*, beziehungsweise als normative Setzung, dass Netzwerke »flach« *sein sollten* (z.B. bei Mueller 2020). Daraus entsteht eine Prädisposition für das Horizontale und Emergente anstelle von Hierarchie und Struktur. Eine stärker räumliche Perspektive stellt diese flache Ontologie in Frage und hebt den Punkt hervor, dass nicht alle Teile eines Netzwerks gleich geschaffen sind (Mathew 2016, Schmidt 2014). Für die Datensphäre bedeutet dies, dass auch diese »uneben« ist. Manche Datenklumpen sind größer und schwerwiegender (»big data« im wörtlichen Sinne), manche sind stärker verknüpft als andere.

Die Datensphäre hat eine Geografie, die es ernstzunehmen gilt. Hier kann der Begriff der Datensphäre vorschnell die Illusion eines holistischen Ganzen erzeugen, nicht unähnlich des Konzepts der *electronic frontier*. Dieses Bild war in der Frühzeit des Internets in libertären Kreisen sehr beliebt, welche von einem autonomen »Grenzland« träumten, das nicht den althergebrachten Regeln des menschlichen Zusammenlebens unterworfen sei – eine schon damals zweifelhafte Behauptung (Saco 1999, Lambach 2020). Dies trifft auch nicht auf die Datensphäre zu. Daten sind nur teilweise miteinander verknüpft und die Hüter der Datenschätze sind sehr selektiv darin, wem sie welchen Zugang gewähren. Anders gesagt: Die Datensphäre hat nicht nur Außen- sondern auch Binnengrenzen. Nicht jeder Datensatz ist für jeden Zugriff und jede*n Nutzer*in zugänglich. Technisch kann dies auf unterschiedliche Weise implementiert werden, z.B. durch Authentifizierungsverfahren, Passwortschutz, Tokens, Cookies, IP-Einschränkungen etc.

Hüter von Daten können Programmierschnittstellen (*Application Programming Interface*, API) definieren, die anderen Systemen den Zugriff er-

möglichen. Die API definiert gewissermaßen das Protokoll des Austauschs und die Rechte der Zugreifenden. APIs erleichtern den Datenaustausch zwischen verschiedenen Systemen, z.B. innerhalb einer Verwaltung. Für Unternehmen erleichtern sie die Integration fremder Dienste in ihr System, um ihren Nutzer*innen ein besseres Angebot zu machen und sie damit fester an das eigene Ökosystem zu binden. In letzter Zeit zeichnet sich zudem eine zunehmend restriktive API-Politik großer Plattformen ab. Seitdem Daten nicht mehr nur als Grundlage für algorithmische Werbung sondern als zentraler Rohstoff für das Training künstlicher Intelligenzen angesehen werden, sitzen die Drachen immer eifersüchtiger auf ihren gehorteten Daten-Schätzen.

Kurz gesagt: Die Datensphäre existiert, aber sie ist uneben und voller Hürden, Mauern und Einlasskontrollen. Ihre genauere Kartierung wäre eine verdienstvolle Aufgabe, die aber nicht das Ziel dieses Artikels ist. Der Fokus hier liegt dagegen auf der Verschränkung der Datensphäre mit anderen Räumlichkeiten und dessen Implikationen, weshalb hier ein abstrakter Blick auf die Datensphäre ausreicht. Instruktiv sind hierfür Arbeiten über das *Entanglement* von Datensphäre und sozialer Welt, in der sich digital-physische Hybridwelten oder Overlays entwickeln (Zook/Graham 2007). Die für mich relevante Frage ist dabei: Was macht es mit unserer Welt und mit unserem Umgang damit, wenn wir große Teile davon datafizieren?

Die Datensphäre ist kein losgelöster Raum mit seinen eigenen Regeln. Vielmehr ist sie zweiseitig mit der realen Welt gekoppelt. Sie ist nicht das Spiegelbild des Physischen, sondern eine Abbildung mit Fehlern und Verzögerungen, die ihrerseits das Potenzial hat, die physische Welt zu beeinflussen. Sie existiert auch nicht »neben« der physischen Welt, sondern durchdringt sie. Je mehr Computer in smarten Geräten und Elektronik verpackt sind und je mehr Sensorik unsere Umgebung enthält, desto mehr Schnittstellen entstehen zwischen den Welten. Diese Logik der wechselseitigen Durchdringung, der Vernetzung und des Austauschs wird durch die Bezeichnung als »-sphäre« unterstrichen, die durch die Anthropozän-Literatur inspiriert ist. Die Erdsystemwissenschaften unterscheiden verschiedene Sphären des Planeten und heben deren enge Wechselwirkungen heraus. In den klassischen Geowissenschaften waren dies die Hydrosphäre, die Geosphäre, die Atmosphäre und die Biosphäre, die in jüngster Zeit durch die Anthroposphäre bzw. Technosphäre ergänzt wurden. Gemeint sind damit »our complex social structures together with the physical infrastructure and technological artefacts supporting energy, information

and material flows that enable the system to work« (Zalasiewicz u.a. 2017, S. 2–3). Die Datensphäre hebt in dieser Logik einen spezifischen Aspekt der Technosphäre heraus, um das Phänomen der Datafizierung in seiner Totalität sowie in seinem Wechselspiel mit anderen planetaren Sphären zu verstehen.

Eine datensphärische Perspektive hebt daher nicht nur das *Entanglement* des Datenraums mit der sozialen Welt hervor, sondern auch mit der natürlichen Welt. Um ein paar exemplarische Verflechtungen aufzuführen:

- Datenzentren, in denen die Datenschätze gesammelt werden, haben lokale ökologische Effekte. In den USA sind sie für fast 2 % des nationalen Stromverbrauchs verantwortlich. Darüber hinaus benötigen sie große Mengen an Kühlwasser und produzieren CO_2 (Siddik u.a. 2021).
- Datentransfer benötigt globale Infrastrukturen, die an verschiedenen Orten in lokale ökologische Zusammenhänge eingebunden sind. Für Satellitennetzwerke braucht es Startrampen und der Transport ins All hat klimarelevante Effekte (Ryan u.a. 2022, Shutler u.a. 2022). Unterwasserkabel verändern Tiefseeökosysteme und ihre Anlandestationen sind Teil lokaler Medienökologien (Pasek u.a. 2023).
- Daten werden vor allem über leicht zugängliche Teile der Welt produziert. Beispielsweise gibt es mittlerweile relativ gute Karten des Meeresbodens in den südlicheren Teilen des Nordpolarmeeres. Im zentralen arktischen Ozean, der immer noch von Eis bedeckt ist, ist Datenerhebung sehr viel schwieriger und deshalb seltener (Lambach 2022b).

Neben ihrer räumlichen Charakterisika hat die Datensphäre auch eine eigene Temporalität. Dies wird einerseits deutlich in ihrer ständigen Veränderung: Neue Daten werden in dramatisch zunehmendem Tempo gesammelt und erzeugt, was die Geografie der Datensphäre konstant verändert. Die Entstehung von *big data*-Klumpen bei großen Plattformen ist nur ein Beispiel hierfür, der rasante Zuwachs von industriellen Daten ein weiteres. Andererseits gibt es auch eine temporale Verzögerung in der Korrespondenz zwischen Daten und physischer Welt. Besonders drastisch wird dies durch Datenverluste deutlich, wenn Datenbestände durch schleichenden *bit rot* und veraltete Formate unlesbar werden. Aber auch noch zugängliche Datenbestände »altern«, wenn sie nicht kontinuierlich aktualisiert werden, und verlieren ihre Bezüge zu den Dingen, auf die sie verweisen sollen, z.B. wenn das Objekt einer Adressdatenbank seinen Wohnsitz wechselt. Die Dis-

kussion um »digitale Zwillinge« und »digitale Schatten« hat sehr deutlich gemacht, dass sich Zeichensysteme von ihren Referenzobjekten abkoppeln und ein Eigenleben entwickeln können.[3] Gleiches gilt für die Schatten nicht-menschlicher Objekte, von denen Daten auch nur unvollständige, fehlerhafte Abbilder zeichnen. Manchmal entsteht die Diskrepanz auch nicht durch die Daten, sondern die Algorithmen. So berichtet beispielsweise Helmreich von Google Oceans Problemen, in ihren Karten Inseln vom Meeresboden zu unterscheiden: »Some users report that recent upgrades of seafloor models have erased entire islands« (Helmreich 2011, S. 1230). Ein anderes Beispiel ist aus der Genomforschung bekannt, wo Wissenschaftler:innen erst nach Jahren bemerkten, dass die oft genutzte Software Microsoft Excel etablierte Namen von Genen nicht als Text-Strings, sondern als Datumsangaben verarbeitete. Um derartige Fehler künftig auszuschließen, entschloss sich die internationale Forschungsgemeinde, die entsprechende Gene umzubenennen, anstatt auf einen Patch der Software zu warten (Holland 2020).

Daten sollten daher nicht als neutrale Abbildung der physischen Welt verstanden werden. Daten sind unvollständig und nur lose mit ihrem Objekt gekoppelt. Durch ihre algorithmische Bearbeitung können weitere Fehler entstehen. Diese Distanz zwischen Repräsentation und Objekt wird in den Science and Technology Studies regelmäßig herausgearbeitet. Dort werden vermeintlich neutrale Abbildungen als »view from nowhere« oder als »God trick« bezeichnet, um auf die Unmöglichkeit eines neutralen Blickwinkels und die autoriale Agenda hinzuweisen, die jeder Repräsentation innewohnt (Haraway 1988, Helmreich 2011, Shim 2014).

More-than-human Data

Die Datensphäre in ihrer Gesamtheit besteht sowohl aus personenbezogenen Daten als auch aus solchen, die auf nicht-menschliche (*non-human* bzw. *more-than-human*) Gegenstände verweisen. Exemplarisch möchte ich hier auf Datensammlungen in den Bereichen Geographie, Umwelt, Bauwesen,

3 Siehe die Beiträge von Zaira Zihlmann und Malte Gruber sowie von Jasmin Brieske und Doris Schweitzer in diesem Band.

Industrie sowie durch smarte Geräte eingehen, um die Konturen dieser Aspekte der Datensphäre zu umreißen.

Geographische Daten sind über die gesamte Menschheitsgeschichte in unterschiedlichen Formen gesammelt worden. So ist die Kartografie nicht nur eine wichtige zivilisatorische Errungenschaft, sondern war auch eine zentrale politische Technologie der Staatsbildung (Branch 2014, Harley 1987) und ist auch heute noch Grundlage von Territorialansprüchen (Lambach 2022b). Artefakte aus der Jungsteinzeit (Stonehenge) oder der Bronzezeit (Himmelsscheibe von Nebra) zeigen, wie astronomische Daten über Sterne, Asteroiden oder die Jahreszeiten gesammelt und bewahrt wurden. Derartige Wissensbestände über die Erde und den Kosmos wurden in den letzten Jahrzehnten zunehmend digitalisiert, verfeinert und damit auch für neue Anwendungen (z.B. in der Routenplanung oder Raumplanung) nutzbar. Satellitengestützte Navigationssysteme zur Positionsbestimmung wie GPS, Galileo oder Beidou sind zu kritischen Infrastrukturen der Globalisierung geworden. Dies ist nicht nur ein Spielfeld staatlicher Agenturen, sondern auch ein Produkt kommerzieller Akteure, für die die Sammlung geografischer Daten, am besten in Echtzeit, ein Milliardengeschäft darstellt.

Von ähnlich großer Bedeutung sind *Umweltdaten*, z.B. zur Bestimmung von Temperaturen, Böden, Meeresströmungen, Wetter- und Klimaphänomenen, Luftverschmutzung oder dem Vorkommen von Tierbeständen (Gabrys 2016). Diese sind für alle Lebensbereiche relevant, von der Landwirtschaft über Bauvorhaben und Fischerei bis hin zu Fragen öffentlicher Gesundheit. Gesammelt werden derartige Daten bereits seit Jahrhunderten. Neuere wissenschaftliche Techniken, z.B. zur Bestimmung von Sedimenten in Bohrkernen, erzeugen historische Daten, die Jahrtausende in die Vergangenheit zurückreichen. Weltraumgestützte Infrastrukturen haben auch hier für Durchbrüche gesorgt. Selbst bei der Beobachtung von mit Minisendern ausgestatteten Tieren spielen Empfangsstationen im Weltall eine zentrale Rolle.[4] Auch weitere Techniken der Erdbeobachtung haben sich durch Satellitentechnologien massiv weiterentwickelt und generieren konstant neue Daten, die ein besseres Verständnis unseres Planeten und der durch den Klimawandel induzierten Veränderungen ermöglichen.

Weiterhin werden *Daten über die gebaute Umwelt* erzeugt. Dies betrifft zum einen das Katasterwesen, also das amtliche Verzeichnis über Grund-

4 Siehe das Icarus-Projekt des Max-Planck-Instituts für Verhaltensbiologie, https://www.icarus.mpg.de [21.5.2024].

stücksbesitz. Diese jahrhundertealte Herrschaftstechnologie wird nach und nach digitalisiert und dadurch zur Verknüpfung mit anderen Datenbeständen aufbereitet. Straßen werden mit automatischen Sensoren versehen, um das Verkehrsaufkommen zu zählen und Tempolimits anzupassen. Auch das Schienennetz wird zunehmend digitalisiert, um die Einstellung von Weichen und Signalen aus weit entfernten Leitstellen zu ermöglichen. Hinzu kommt die Digitalisierung von Baudenkmälern und des gebauten kulturellen Erbes. Diese Katalogisierung macht Denkmäler einerseits für Forschung zugänglich und eröffnet sie andererseits auch für kulturelle Zwecke, z.B. für einen virtuellen Besuch in einem 3D-Modell von Schloss Neuschwanstein. Moderne Smart Homes erzeugen die Daten gleich selbst und machen sie den Nutzer:innen sowie den Gerätehersteller:innen zugänglich.

Industrielle Daten stellen einen weiteren Ausschnitt von *more-than-human data* dar. Industrielle Kontrollsysteme erzeugen Daten im Betrieb, die für die Anlagensteuerung unerlässlich sind. Zusätzlich sollen durch die Datafizierung von Prozessen auch neue Möglichkeiten zur Wertschöpfung entstehen. Die Kommunikation von Geräten über einen Produktionsprozess oder eine ganze Lieferkette hinweg eröffnet hier ganz neue Horizonte in der »Industrie 4.0«. Datafizierung soll Produktion flexibler machen, modularen Fabrikaufbau ermöglichen, Logistik optimieren, Ressourcen sparen und den Kund:innen mehr Anpassungsmöglichkeiten für ihr Produkt einräumen. Kombiniert mit moderner Kommunikationstechnologie nach dem 5G-Standard soll sich das Volumen von Industriedaten in den kommenden Jahren um ein Vielfaches erhöhen.

Nicht zuletzt erzeugen *smarte Geräte* konstant Daten, Metadaten und Paradaten, die ausgelesen, gesammelt und ausgewertet werden können. Standort, Ladestand, verwendetes Betriebssystem, installierte Anwendungen – über alles stehen Daten zur Verfügung, die wiederum mit personenbezogenen Nutzer:innendaten verknüpft werden können. Geräte aus dem Internet der Dinge haben sich hier lange in einem unterregulierten Bereich bewegt und Hersteller beachten allzu oft Datenschutz- und Cybersicherheitsstandards nicht ausreichend.

Diese exemplarische Übersicht zeigt verschiedene Domänen der Datensphäre jenseits der Personendaten. In den verschiedenen Beispielen wird die Zentralität von Sensoren deutlich, die Daten zu physischen Dingen erzeugen, z.B. durch die Positionsbestimmung eines Gerätes mittels GPS oder die Erstellung eines 3D-Modells eines Baudenkmals durch eine Kombination von Fotos. Das GPS-Beispiel unterstreicht darüber hinaus, dass Senso-

ren ihrerseits in technologischen Netzwerken verknüpft sind. Kein Sensor funktioniert für sich allein, sondern ist mit anderen Sensoren, Computersystemen und anderen Technologien verbunden. Die Datensphäre ist somit ein untrennbarer Bestandteil der weiteren Technosphäre und die Geschichte der Datafizierung auch eine Geschichte der Sensorifizierung unserer Umgebung (Andrejevic/Burdon 2014).

Die Beziehung dieser Datensphärendimensionen zu ihren Objekten wirft politische, rechtliche und ethische Fragen auf. Diese sind nicht deckungsgleich mit den Fragen, die bei der Sammlung und Verarbeitung personenbezogener Daten entstehen, weisen aber gewisse Parallelen auf, z.B. in Grundfragen von Rechten, Autorität und Legitimität: Wer ist berechtigt, welche Daten zu sammeln und wer bekommt hinterher Zugang dazu? Ein klassisches Beispiel sind »genetische Ressourcen« von Pflanzen und Tieren. Wenn Forscher:innen eines Konzerns das Genom eines Lebewesens bestimmen, können sie dies als intellektuelles Eigentum schützen und die gewonnenen Daten und das Wissen damit vor dem Zugriff durch andere bewahren (Jensen/Murray 2005)? Haben menschliche Gemeinschaften, die diese Pflanzen und Tiere traditionell nutzen, bestimmte Vor- oder Einspruchsrechte gegen die Sammlung dieser Daten (Runge/Defrancesco 2006)? Hierzu hat sich ein internationaler Regimekomplex entwickelt (Raustiala/Victor 2004), der in jüngster Zeit auch durch ein Regelwerk zu marinen genetischen Ressourcen in Gebieten jenseits staatlicher Hoheitsgewässer erweitert wurde (Su 2021). Ein anderes Beispiel wäre, ob Staaten ein Einspruchsrecht gegen Satellitenaufnahmen ihres Territoriums haben, gewissermaßen ein Anrecht auf Privatsphäre (Emanuilov 2019).

Datensammler und Datenzugänge

Beteiligt an dieser massiven Datensammlung sind Akteure aus allen gesellschaftlichen Subsystemen. Forschungsinstitutionen haben eine lange Tradition im Sammeln von *more-than-human*-Daten mit dem Ziel der »Vermessung der Welt«, um einen bekannten Buchtitel zu zitieren. In der Forschung besteht ein Ethos des Datenteilens, der sich in jüngster Zeit vor allem in *open science*-Normen ausdrückte, die als Lösung für die sogenannte

Replikationskrise angesehen werden.[5] »Data sharing« ist der aktuelle Leitstern, auch wenn dessen Umsetzung nicht in allen Disziplinen, Ländern und Kontexten gleichermaßen konsequent ist (Tedersoo u.a. 2021). Dies gilt insbesondere für globale Kooperationsvorhaben, aktuell z.B. in der Genom- oder Teilchenforschung. Auch historische Beispiele gibt es genug, z.B. den internationalen Austausch von Beobachtungsdaten zum Venustransit vor der Sonne 1761 und 1769, die für die Vermessung des Sonnensystems von großer Bedeutung waren (Wulf 2012). War Datenzugang damals noch sehr aufwändig, gibt es heute Infrastrukturen, die die Transaktionskosten hierfür massiv senken, von der einfachen Email bis hin zu gut sortierten Datenrepositorien. Zwar gibt es in der Wissenschaftsgemeinde ein gewisses Verständnis für Forschende, die Daten zeitweise für sich behalten, um das Risiko eines *scoops* zu vermeiden, aber zumindest nominell folgt die Forschung klar der eingangs geschilderten Position, dass die von ihr gesammelten Daten Teil eines Gemeinschaftsguts sind, die möglichst ohne Schranken für alle zugänglich sein sollten.

Auch Regierungen, Verwaltungen und andere Akteure des öffentlichen Sektors sammeln und verwalten Daten. Jenseits von Personendaten beziehen sich diese z.B. auf Landnutzung, Raumplanung, Wirtschaftsstrukturen oder kritische Infrastrukturen wie Verkehr und Stromnetze, die für die effiziente Verwaltung moderner Gesellschaften unerlässlich sind. Regierungen sind aber auch an Forschungsdaten interessiert. Einerseits als Quelle von Prestige und Macht im internationalen Wettlauf (Yao 2021), andererseits ist in jüngerer Zeit »das Interesse von Staaten, Regierungen und der Zivilgesellschaft an qualitätsgesicherten Forschungsdaten im globalen Maßstab gewachsen. Forschungsdaten rücken zum einen als Evidenzbasis auch für außerwissenschaftliche Entscheidungsprozesse in den Fokus der allgemeinen Aufmerksamkeit« (RfII 2019, S. 8).

Anders als in der Forschung waren Daten für die Obrigkeit lange Zeit Teil ihres Herrschaftswissens, die teils unter expliziter Geheimhaltung vor neugierigen Augen geschützt werden mussten (Scott 1998). Hier kündigt sich seit geraumer Zeit ein kultureller Wandel hin zu mehr Transparenz an, auch wenn dies bislang nicht konsequent umgesetzt wird. Unter dem Stichwort »open government« werden Forderungen diskutiert, dass von staatlichen Stellen gesammelte Daten Bürger:innen und anderen Nutzergruppen frei zur Verfügung gestellt werden sollten (Attard u.a. 2015). Damit verspricht

5 Siehe den Text von Petra Gehring in diesem Band.

man sich bessere Teilhabemöglichkeiten für die Bürgerschaft und Zivilgesellschaft in einer zunehmend datengetriebenen Governance (Hansson u.a. 2014). In Deutschland stellen manche Kommunen Datenportale zur Verfügung, z.B. das Portal https://www.offenedaten.frankfurt.de/ der Stadt Frankfurt, wo z.B. Datensätze zu Stellplätzen, Starkregengefahren oder Toilettenstandorten abgerufen werden können.

In historischer Perspektive neu ist die starke Rolle von Privatunternehmen in der Sammlung und Verwaltung von nicht-menschlichen Daten. Große Internetunternehmen stechen hier heraus, die ihren Datenhunger nicht nur auf Personendaten beschränken. Hier ist an erster Stelle Google/Alphabet zu nennen, auch wenn andere Plattformen teils vergleichbare Aktivitäten unternehmen. Google hat bereits seit seiner Gründungsphase danach gestrebt, *more-than-human*-Daten zu sammeln und für eine breite Nutzerschaft aufzubereiten.[6] Am bekanntesten ist hier wahrscheinlich der Kartendienst Google Maps, aber auch Dienste wie Google Earth, Google Ocean oder Google Mars bieten geografische Daten für verschiedene Umgebungen. Google Dataset Search ist eine spezialisierte Suchmaschine für wissenschaftliche Datensätze. Für all diese Dienste sticht natürlich das Kommerzialisierungsmotiv hervor – wenn ein Unternehmen derartige Daten sammelt, dann mit Gewinnabsicht. Google ist berüchtigt dafür, unprofitable Applikationen schnell wieder abzuwickeln, selbst wenn sie noch in Gebrauch sind. Zwar ist der Zugriff teils kostenlos möglich, ist aber über Anmeldepflicht oder die Nutzung einer API und die damit einhergehende Unterwerfung unter die Vertragsbedingungen des Unternehmens geregelt. Der Mehrwert für das Unternehmen entsteht nicht zwingend durch den unmittelbaren Verkauf des Datenzugangs, sondern eventuell eher durch den Nutzen des Datenschatzes, um zusätzliche Nutzer:innen anzuziehen, das Gesamtökosystem attraktiver zu machen und somit Wechselkosten zu erhöhen.

Die Frage nach dem Zugang zu nicht-menschlichen Daten ist also maßgeblich eine Frage danach, wer sie gesammelt hat. Die obige Diskussion ist natürlich idealtypisch – es gibt Forscher:innen, die ihre Daten nicht teilen, und Unternehmen, die sie frei zugänglich ins Internet stellen. Ferner gibt es Kooperationen zwischen den verschiedenen Akteurstypen, die dann zwischen den verschiedenen Interessen bzgl. Datentransparenz ausgleichen müssen. Aber man erkennt hier *grosso modo* das Spannungsverhältnis

6 Siehe den Beitrag von Lars Pfeiffer in diesem Band.

zwischen einer Forderung, Datenbestände als *global commons* zu behandeln und größtmögliche Transparenz zu fordern (Shkabatur 2019), und einer Behandlung von Daten als Handelsware und Eigentum (Corson/MacDonald 2012). Wie eingangs angedeutet, wäre dafür noch weitere Differenzierung notwendig. Das *commons*-Argument ist sicherlich naheliegender, wenn es um Umweltdaten geht, insbesondere wenn diese Umwelten ihrerseits Global Commons sind, d.h. die Atmosphäre, die Hohe See, die Tiefsee, die Antarktis oder der Weltraum (Buck 1998, Lambach/Diehl 2021). Demgegenüber ist das Eigentumsargument überzeugender, wenn es um Daten geht, die von smarten Geräten erzeugt werden. Deren Hersteller sollte einen legitimen Anspruch auf diese Daten formulieren können.

Politische Steuerung in der neuen Datenwelt

Datafizierung verändert auch politische Steuerung. Auch hier lohnt sich eine historische Perspektive: Techniken wie Bevölkerungsstatistik, Kartografie und Registerwesen waren entscheidend für die Entwicklung moderner Verwaltungen und Staatswesen (Branch 2014). In den 1960er und 1970er Jahren wurden kybernetische Ansätze formuliert, die eine »datengetriebene«, rationale Steuerung des Staates propagierten. Waren diese Ansätze, wie z.B. das ambitionierte Cybersyn-Projekt der chilenischen Allende-Regierung, noch von Misserfolgen gekennzeichnet, hat die rasante Zunahme der Datensammel- und Datenverarbeitungskapazität seit der Jahrtausendwende die Grundlagen der Regierungstätigkeit merklich verändert (Greef 2023).

Dies ist eine grundsätzliche Tendenz: politische Steuerung im modernen Staatswesen ist zunehmend datengetrieben und technokratisch. »Forschungsdaten rücken […] als Evidenzbasis auch für außerwissenschaftliche Entscheidungsprozesse in den Fokus der allgemeinen Aufmerksamkeit« (RfII 2019, S. 8). Dies gilt auch für die politische Kommunikation – politische Entscheidungen, die sich nicht auf eine Datenbasis berufen können, werden skeptischer beurteilt und als »ideologisch« abgetan. Politische Akteure müssen Erzählungen anbieten, aber Zahlen sind ein wichtiger Bestandteil dieser Narrative. Was früher die monatliche Arbeitslosenstatistik war, waren gestern die Corona-Infektionszahlen. Auch Umfragedaten spielen eine zunehmend wichtige Debatte jenseits von Wahlkämpfen. Mit Zahlen werden Narrative geschaffen und Medienberichte lanciert. Da die

Erhebungstechniken immer einfacher werden und die Kosten sinken, gibt es schlicht auch immer mehr Umfragen und andere Formen der Gesellschaftsbeobachtung. Nicht zuletzt verfallen auch die Entscheidungsträger:innen selbst der Illusion der scheinbaren Faktizität von Daten. Ein Entwicklungsökonom sagte einmal in einem Hintergrundgespräch, sobald er im politischen Dialog Zahlen auf den Tisch lege, würden diese völlig unkritisch akzeptiert.

Diese Punkte lassen sich auch auf *more-than-human*-Daten anwenden. Theoretisch gesprochen: Technologien und Daten spielen eine wichtige vermittelnde Rolle zwischen menschlichen Akteur:innen und ihrer nichtmenschlichen Umgebung. Dies ist auch politisch bedeutsam, da die Steuerung dieser Umgebungen auf ihrer Abbildung in Daten beruht. Marine Raumplanung ist beispielsweise komplett von Karten abhängig, die eine Meeresumgebung nicht bloß abbilden, sondern mit erzeugen: »the map performs the territory instead of representing it, as inscriptions into the map will lead to proscriptions of behaviour« (Knol 2011, S. 982). Lehman bezeichnet den rasanten Zuwachs an Meeresdaten als »new world ocean: an ocean of data, a digital doppelganger for the wet and wild ocean out there, an ocean made informational« (Lehman 2016, S. 113). Gleiches gilt für die internationale Governance von Weltraumschrott, die auf der konstanten Radarüberwachung des Erdorbits und der detaillierten Verfolgung von derzeit über 33.000 Trümmerteilen beruht. Allerdings können diese Systeme aufgrund ihrer technischen Grenzen keine Objekte mit einer Kantenlänge von unter 10 cm erfassen. Kleinere Objekte werden also nicht direkt verfolgt, sondern lediglich an Computern modelliert, z.B. indem man Einschlagsmuster auf Raumfahrzeugen oder ausgedienten Satelliten untersucht. Derartige Modelle ergeben Schätzungen von 1 Mio Trümmerteilen > 1 cm und 130 Mio Teilen > 1 mm.[7] Die alarmierenden visuellen Darstellungen, die einen Orbit voller Müll zeigen und für die öffentliche Debatte prägend sind, arbeiten auch mit diesen Daten (Buchs 2021), sind aber weitgehend modellbasierte Fiktionen.

Daten sind das Medium, durch welches politische Steuerung von Umwelten organisiert wird. Die gewählten Beispiele stammen aus den Ozeanen und dem Weltraum, dieselbe Logik greift aber auch bei der Atmosphäre (Klimadaten, Verschmutzungsdaten, Wetterdaten) und an Land. Beispielsweise beruht die Governance der Landwirtschaft auf Daten über den Zustand der

7 https://www.esa.int/Space_Safety/Space_Debris/Space_debris_by_the_numbers [21.5.2024].

Böden, z.B. ihrer geologischen Beschaffenheit oder dem Grundwasserspiegel, die Erträge bestimmten Saatguts und die Produktivität der verwendeten Anbautechniken. Wirtschafts- und Finanzpolitik arbeiten mit volkswirtschaftlichen Daten, die Sozialpolitik mit Daten über Einkommen, Vermögen und Familien. Kurz: moderne politische Steuerung kommt nicht ohne aus Daten gewonnene Statistiken, Karten, Modelle, Prognosen oder Visualisierungen aus. Die Datensphäre ist eine Ressource, derer sich politische (und andere) Akteure bedienen, aber eben keine neutrale Abbildung, sondern eine geschaffene Repräsentation mit unterschiedlichen, teils konfligierenden Agenden.

Staat und Politik brauchen dafür Zugang zu den entsprechenden Daten sowie die Expertise, diese auch zu verstehen und damit zu arbeiten. Deshalb gibt es einen großen Sektor staatlicher Auftragsforschung sowie die einschlägigen staatlichen Agenturen wie das Bundeamt für Kartographie und Geodäsie, die Bundesanstalt für Geowissenschaften und Rohstoffe oder das Deutsche Luft- und Raumfahrtzentrum, die entsprechende Daten selber erheben, externe Forschung finanzieren sowie die nötige Expertise vorhalten. Auch Daten privater und kommerzieller Anbieter sind für öffentliche Stellen relevant. So benutzt das Umweltbundesamt für seine Luftqualitäts-App Kartendaten von Google Maps.[8] Hier kommt es manchmal zu Konflikten, wenn sich die Anbieter nicht an alle gesetzlichen Vorgaben halten, insbesondere aus der Datenschutzgrundverordnung, und ihre Daten deshalb nicht in staatlichen Angeboten eingebunden werden können. Es gibt auch Fälle, wo die Obrigkeit zur Ausübung ihrer hoheitlichen Aufgaben oder zur Strafverfolgung die Herausgabe bestimmter Daten verlangt, z.B. von Gerätedaten wie beispielsweise Positionsdaten eines Mobilfunkgeräts.

Triebkräfte der Datafizierung

Die Datafizierung der Umwelt wird aus politischen und wirtschaftlichen Gründen fortschreiten und die Suche nach immer detaillierteren Daten weiter vorantreiben. Auf politischer Ebene liegt dies an der Datensammel-

8 https://www.umweltbundesamt.de/datenschutzerklaerung-luftapp#i-name-und-anschrift-des-verantwortlichen [21.5.2024].

maschine Staat. Wie uns die Staatstheorie von James Scott (1998) aber auch technokratische Staatsideale, die Überwachungsforschung und verschiedene Bürokratietheorien lehren, ist der Staat eine Maschine zur Erzeugung und Verarbeitung von Informationen und der moderne Staat ganz besonders. Staaten sammeln Daten über Landeigentum, Einkommen, Familien, Staatsangehörigkeit, wirtschaftliche Aktivität, sowie allerlei öffentliche und private Aktivitäten ihrer Bürger:innen, die in Statistiken, Registern, Akten und Karten dargestellt werden. Für Scott ist der entscheidende Impetus, dass Staaten ihre Gesellschaften für sich »lesbar« machen wollen, um sie effektiver kontrollieren zu können. Dies geschieht einerseits durch die Herausbildung eines differenzierten Apparats zur Datenerhebung – Volkszählungen, Steuerprüfungen, Passwesen etc. –, andererseits dadurch dass die Gesellschaft an die Daten und die Notwendigkeiten der Datenerhebung angepasst wird, z.B. durch Umsiedlung, Praktiken der Namensgebung und Formalisierung von Ehe- und Arbeitsverhältnissen. Dies bezieht nicht nur die Gesellschaft mit ein, sondern auch die Natur. Wie Joanne Yao (2019) feststellt, war »control over nature« im 19. Jahrhundert ein wichtiger Indikator für den Grad der »Zivilisiertheit« eines Landes.

Auch in der Wirtschaft gibt es heute starke Triebkräfte für die weitere Datafizierung der Umwelt. Im weitesten Sinne sagen uns Theorien des Datenkapitalismus (Zuboff 2019), dass Daten zum zentralen Rohstoff der digitalen Wirtschaft geworden sind – »Daten sind das neue Öl«, wie es der Economist 2017 betitelte.[9] Dieser Satz ist zwar inhaltlich sinnlos, denn Öl ist eine begrenzte, geographisch lokalisierte Ressource, die mit viel Kapitalaufwand aus dem Gestein gepumpt werden muss, während Daten unbegrenzt, mobil und damit von physischer Geographie weitgehend losgelöst sind. Dennoch drückt dieser Slogan die Goldgräberstimmung aus, die in der Digitalwirtschaft verbreitet ist. Große Plattformen häufen *big data*-Schätze an, die das zentrale Mittel ihrer Wertschöpfung darstellen (Giblin/Doctorow 2022, Sadowski 2020). Dies ist nicht auf Personendaten beschränkt: Geographische Daten und akkurate Positionsbestimmung sind Schlüsseltechnologien für viele andere Anwendungen. Umweltdaten sind so gefragt, dass es inzwischen einen nennenswerten Sektor kommerzieller Erdbeobachtungssatelliten in der Umlaufbahn gibt. Daten über Gebäude und Verkehrsinfrastrukturen sind von großem Wert für die Immobilienwirtschaft und IoT-

9 https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data [21.5.2024].

Firmen. Industrielle Daten gelten als Goldgrube für das produzierende Gewerbe. Und Gerätedaten werden als Messgrößen für das Verhalten von Nutzer:innen verwendet. Nahezu jede Firma, die heutzutage irgendwelche elektronischen Komponenten verbaut, ist automatisch auch (oder vielleicht sogar vor allem) im Datengeschäft.

Fazit

Die Datensphäre ist ein nicht mehr wegzudenkender Teil des Erdsystems und der menschlichen Gesellschaft. Sie besteht aus Daten über alle möglichen Objekte, die in unterschiedlichster Weise miteinander verknüpft und in Beziehung gesetzt werden. Jenseits ihres Wachstums ist sie daher auch durch eine hohe Binnendynamik gekennzeichnet. Die Datensphäre hat keine flache Geographie und sie lässt sich nicht an einem einzelnen Ort lokalisieren. Dennoch ist sie nicht »ort-los« – sie existiert an den Schnittflächen zur physischen Welt (Sensoren) und an den Orten (physisch wie virtuell), wo die Datenklumpen auflaufen. Sie interagiert mit Geosphäre, Biosphäre, Atmosphäre oder Hydrosphäre durch ihren Stromverbrauch, ihren Kühlwasserbedarf, den Eingriff datensphärischer Infrastruktur in lokale Ökosysteme oder ihre klimaschädlichen Emissionen.

Die Bedeutung von *more-than-human data* in der Datensphäre ist dabei nicht zu unterschätzen, auch wenn sie in bisherigen Diskussionen noch etwas unterrepräsentiert waren. Daten über Industrien, Geräte, Tiere etc. sind von ebenso großer Relevanz für Wirtschaft und Politik wie personenbezogene Daten. Diese Daten sind das Medium, durch das sich Entscheidungsträger mit dem Gegenstand an sich befassen. Allerdings gibt es unterschiedliche Sichtweisen darauf, welche Daten wem zur Verfügung stehen sollten – welche *more-than-human*-Daten sollten Teil einer gemeinsamen Ressource der gesamten Menschheit sein, welche sollten privatisierbar und damit auch kommerzialisierbar sein? In der Auseinandersetzung zwischen diesen Positionen ergeben sich Binnengrenzen der Datensphäre. Zugangsbeschränkungen, Bezahlschranken und API-Richtlinien bestimmen, wer auf welche Datenschätze zugreifen und wofür er sie verwenden darf. Insofern muss man die Datensphäre als zerklüftete Landschaft verstehen.

Literatur

Agnew, John (1998): *Geopolitics: Re-visioning World Politics*, London.

Andrejevic, Mark/Burdon, Mark (2014): Defining the Sensor Society, in: *Television & New Media* 16, Heft 1, S. 19–36.

Attard, Judie/Orlandi, Fabrizio/Scerri, Simon/Auer, Sören (2015): A systematic review of open government data initiatives, in: *Government Information Quarterly* 32, Heft 4, S. 399–418.

Bergé, Jean-Sylvestre/Grumbach, Stéphane/Zeno-Zencovich, Vincenzo (2018): The ›Datasphere‹, Data Flows beyond Control, and the Challenges for Law and Governance, in: *European Journal of Comparative Law and Governance* 5, Heft 2, S. 144–178.

Branch, Jordan (2014): *The Cartographic State: Maps, Territory, and the Origins of Sovereignty*, Cambridge.

Buchs, Romain (2021): *Collision Risk from Space Debris: Current status, challenges and response strategies*, Lausanne.

Buck, Susan J. (1998): *The Global Commons: An Introduction*, Washington D.C.

Collis, Christy/Dodds, Klaus (2008): Assault on the unknown: the historical and political geographies of the International Geophysical Year (1957–8), in: *Journal of Historical Geography* 34, Heft 4, S. 555–573.

Corson, Catherine/MacDonald, Kenneth I. (2012): Enclosing the global commons: the convention on biological diversity and green grabbing, in: *The Journal of Peasant Studies* 39, Heft 2, S. 263–283.

Emanuilov, Ivo (2019): *From Space Big Data to Big Space Brother: do States have a right to privacy? (Part I)*, Blogpost, 23. Juli 2019, https://www.law.kuleuven.be/citip/blog/from-space-big-data-to-big-space-brother-do-states-have-a-right-to-privacy-part-i/ [21.5.2024].

Epstein, Brian (2018): Social Ontology, in: Edward N. Zalta (Hg.): *The Stanford Encyclopedia of Philosophy*, Summer 2018 Edition.

Gabrys, Jennifer (2016): *Program Earth: Environmental Sensing Technology and the Making of a Computational Planet*, Minneapolis.

Giblin, Rebecca/Doctorow, Cory (2022): *Chokepoint Capitalism*, Boston.

Greef, Samuel (2023): *Staat und Staatlichkeit im digitalen Zeitalter: Politische Steuerung im Wandel*, Bielefeld.

Hansson, Karin/Belkacem, Kheira/Ekenberg, Love (2014): Open Government and Democracy: A Research Review, in: *Social Science Computer Review* 33, Heft 5, S. 540–555.

Haraway, Donna (1988): Situated Knowledges: The Science Question in Feminism and the Privilege of Partial Perspective, in: *Feminist Studies* 14, Heft 3, S. 575–599.

Harley, J.B. (1987): The Map and the Development of the History of Cartography, in: Harley, Jonh B./ Woodward, David (Hg.): *The History of Cartography, Volume I: Cartography in Prehistoric, Ancient, and Medieval Europe and the Mediterranean*, Chicago, S. 1–42.

Helmreich, Stefan (2011): From Spaceship Earth to Google Ocean: Planetary Icons, Indexes, and Infrastructures, in: *Social Research* 78, Heft 4, S. 1211–1242.

Holland, Martin (2020): *Von Excel in Datumsangaben umgewandelt: Dutzende Gene umbenannt*, https://www.heise.de/news/Von-Excel-in-Datumsangaben-umgewandelt-Dutzende-Gene-umbenannt-4864993.html [21.5.2024].

Houben, Daniel/Prietl, Bianca (Hg.) (2018): *Datengesellschaft: Einsichten in die Datafizierung des Sozialen*, Bielefeld.

Jensen, Kyle/Murray, Fiona (2005): Intellectual Property Landscape of the Human Genome, in: *Science* 310, Heft 5746, S. 239–240.

Jessop, Bob/Brenner, Neil/Jones, Martin (2008): Theorizing Sociospatial Relations, in: *Environment and Planning D: Society and Space* 26, Heft 3, S. 389–401.

Knol, Maaike (2011): Mapping ocean governance: from ecological values to policy instrumentation, in: *Journal of Environmental Planning and Management* 54, Heft 7, S. 979–995.

Lambach, Daniel (2020): The Territorialization of Cyberspace, in: *International Studies Review* 22, Heft 3, S. 482–506.

Lambach, Daniel/Diehl, Carlo (2021): Die Territorialisierung der Global Commons, in: *Zeitschrift für Internationale Beziehungen* 28, Heft 2, S. 5–33.

Lambach, Daniel (2022a): Space, scale, and global politics: Towards a critical approach to space in international relations, in: *Review of International Studies* 48, Heft 2, S. 282–300.

Lambach, Daniel (2022b): Technology and the construction of oceanic space: Bathymetry and the Arctic continental shelf dispute, in: *Political Geography* 98.

Lehman, Jessica (2016): A sea of potential: The politics of global ocean observations, in: *Political Geography* 55, S. 113–123.

Löw, Martina (2016): *The Sociology of Space: Materiality, Social Structures and Action*, New York.

Malpas, Jeff (2012): Putting Space in Place: Philosophical Topography and Relational Geography, in: *Environment and Planning D: Society and Space* 30, Heft 2, S. 226–242.

Massey, Doreen (2005): *For Space*, London.

Mathew, Ashwin J. (2016): The Myth of the Decentralised Internet, in: *Internet Policy Review* 5, Heft 3.

Mayer-Schönberger, Viktor/Cukier, Kenneth (2013): *Big data: A revolution that will transform how we live, work, and think*, London.

Mueller, Milton (2020): Against Sovereignty in Cyberspace, in: *International Studies Review* 22, Heft 4, S. 779–801.

Pasek, Anne/Vaughan, Hunter/Starosielski, Nicole (2023): The world wide web of carbon: Toward a relational footprinting of information and communications technology's climate impacts, in: *Big Data & Society* 10, Heft 1.

Raustiala, Kal/Victor, David G. (2004): The Regime Complex for Plant Genetic Resources, in: *International Organization* 58, Heft 2, S. 277–309.

RfII [= Rat für Informationsinfrastrukturen] (2019): *Herausforderung Datenqualität – Empfehlungen zur Zukunftsfähigkeit von Forschung im digitalen Wandel*, Göttingen.

Runge, C. Ford/Defrancesco, Edi (2006): Exclusion, Inclusion, and Enclosure: Historical Commons and Modern Intellectual Property, in: *World Development* 34, Heft 10, S. 1713–1727.

Ryan, Barry J. (2015): Security spheres: A phenomenology of maritime spatial practices, in: *Security Dialogue* 46, Heft 6, S. 568–584.

Ryan, Robert G./Marais, Eloise A./Balhatchet, Chloe J./Eastham, Sebastian D. (2022): Impact of Rocket Launch and Space Debris Air Pollutant Emissions on Stratospheric Ozone and Global Climate, in: *Earth's Future* 10, Heft 6, e2021EF002612.

Saco, Diana (1999): Colonizing Cyberspace: ›National Security‹ and the Internet, in: Weldes, Jutta/ Laffey, Mark/ Gusterson, Hugh/ Duvall, Raymond (Hg.): *Cultures of Insecurity: States, Communities, and the Production of Danger*, Minneapolis, S. 261–292.

Sadowski, Jathan (2020): The Internet of Landlords: Digital Platforms and New Mechanisms of Rentier Capitalism, in: *Antipode* 52, Heft 2, S. 562–580.

Schmidt, Andreas (2014): Hierarchies in Networks: Emerging Hybrids of Networks and Hierarchies for Producing Internet Security, in: Kremer, Jan-Frederik/ Müller, Benedikt (Hg.): *Cyberspace and International Relations: Theory, Prospects and Challenges*, Berlin, S. 181–202.

Scott, James C. (1998): Seeing Like a State: *How Certain Schemes to Improve the Human Condition Have Failed*, New Haven.

Shim, David (2014): Remote sensing place: Satellite images as visual spatial imaginaries, in: *Geoforum* 51, S. 152–160.

Shkabatur, Jennifer (2019): The Global Commons of Data, in: *Stanford Technology Law Review* 22, S. 354–411.

Shutler, Jamie D./Yan, Xiaoyu/Cnossen, Ingrid/Schulz, Leonard/Watson, Andrew J./ Glaßmeier, Karl-Heinz/Hawkins, Naomi/Nasu, Hitoshi (2022): Atmospheric impacts of the space industry require oversight, in: *Nature Geoscience* 15, Heft 8, S. 598–600.

Siddik, Md Abu Bakar/Shehabi, Arman/Marston, Landon (2021): The environmental footprint of data centers in the United States, in: *Environmental Research Letters* 16, Heft 6, S. 064017.

Su, Jinyuan (2021): The Adjacency Doctrine in the Negotiation of BBNJ: Creeping Jurisdiction or Legitimate Claim?, in: *Ocean Development & International Law* 52, Heft 1, S. 41–63.

Tedersoo, Leho/Küngas, Rainer/Oras, Ester/Köster, Kajar/Eenmaa, Helen/Leijen, Äli/ Pedaste, Margus/Raju, Marju/Astapova, Anastasiya/Lukner, Heli/Kogermann, Karin/ Sepp, Tuul (2021): Data sharing practices and data availability upon request differ across scientific disciplines, in: *Scientific Data* 8, Heft 1, S. 192.

Wulf, Andrea (2012): *Chasing Venus: The Race to Measure the Heavens*, New York.

Yao, Joanne (2019): ›Conquest from barbarism‹: The Danube Commission, international order and the control of nature as a Standard of Civilization, in: *European Journal of International Relations* 25, Heft 2, S. 335–359.

Yao, Joanne (2021): An international hierarchy of science: conquest, cooperation, and the 1959 Antarctic Treaty System, in: *European Journal of International Relations* 27, Heft 4, S. 995–1019.

Zalasiewicz, Jan/Williams, Mark/Waters, Colin N/Barnosky, Anthony D/Palmesino, John/ Rönnskog, Ann-Sofi/Edgeworth, Matt/Neal, Cath/Cearreta, Alejandro/Ellis, Erle C/ Grinevald, Jacques/Haff, Peter/Ivar do Sul, Juliana A/Jeandel, Catherine/Leinfelder, Reinhold/McNeill, John R/Odada, Eric/Oreskes, Naomi/Price, Simon James/Revkin,

Andrew/Steffen, Will/Summerhayes, Colin/Vidas, Davor/Wing, Scott/Wolfe, Alexander P (2017): Scale and diversity of the physical technosphere: A geological perspective, in: *The Anthropocene Review* 4, Heft 1, S. 9–22.

Zook, Matthew A./Graham, Mark (2007): Mapping DigiPlace: Geocoded Internet Data and the Representation of Place, in: *Environment and Planning B: Planning and Design* 34, Heft 3, S. 466–482.

Zuboff, Shoshana (2019): *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, London.

Körperdaten und Datenkörper: Zugänge zum digitalen Zwilling

Malte-C. Gruber und Zaira Zihlmann

I. Von Mensch-Modellen und modellierten Menschen

Die Entwicklung des Datenrechts verläuft, verglichen mit bisherigen technikrechtlichen Erfahrungen, nun gleichsam in umgekehrter Richtung: War es ursprünglich die Abhängigkeit der Daten (und Software) von einem körperlichen Medium (Datenträger), die sich zunehmend aufgelöst hat,[1] so ist es jetzt die sich anbahnende Materialisierung eines aus Körperdaten konstituierten Datenkörpers mit seinen Rückwirkungen auf die menschliche Physis, die uns beschäftigen wird.

Dieser Datenkörper in der Gestalt des sogenannten digitalen Zwillings markiert den nächsten Entwicklungsschritt in der datengetriebenen Medizin. Das konzeptionelle Grundmodell des digitalen Zwillings besteht in einer virtuellen Repräsentation einer physischen Entität, die aus drei Hauptkomponenten besteht: dem physischen Objekt, seinem virtuellen Äquivalent sowie der Datenverbindung zwischen der physischen und der virtuellen Entität. Im Bereich der Medizin tritt der digitale Zwilling mit dem Versprechen an, einzelne Körperorgane, Körperfunktionen oder schließlich gar den gesamten Körper, einschließlich der Körpervorgänge, einer Person zu simulieren, um so etwa präzisere Diagnosen stellen zu können, Behandlungsempfehlungen zu geben sowie potenzielle Nebenwirkungen und Erfolgschancen von Behandlungen besser einzuschätzen.[2] Damit ermöglicht der digitale Zwilling eine Entwicklung hin zur sogenannten P4-

1 Siehe nur das Beispiel der Entwicklung im Produkthaftungsrecht: Die Produkteigenschaft von Software wird spätestens mit der neuen Produkthaftungsrichtlinie selbstverständlich anerkannt; der früher auf bewegliche (körperliche) Gegenstände und allenfalls auf Elektrizität verengte Produktbegriff ist somit endgültig Vergangenheit.

2 Tigard 2021, S. 407.

Medizin, wobei P4 für präzise, präventiv, personalisiert und partizipativ steht.[3] Es ist indes nicht nur dieses Anwendungspotential, das den digitalen Zwilling auszeichnet, vielmehr unterscheidet sich der digitale Zwilling von anderen Computermodellen durch die bidirektionale Datenverbindung, die zwischen dem Patienten und seinem digitalen Zwilling besteht. Eben diese Rückwirkung der virtuellen Entität auf die physische Entität ist nachfolgend denn auch von besonderem Interesse, zumal mit dieser Mensch-Maschine-Schnittstelle eine neue Qualität in der Beziehung zwischen Mensch und Maschine einhergeht, deren Ausgestaltung, insbesondere deren Grenzen, noch zu bestimmen sind.

Obschon sich die Technologie in der frühen Entwicklungsphase befindet und eher den Anschein von Science-Fiction hat,[4] ist es dennoch angezeigt, den digitalen Zwilling ins Blickfeld des Rechts zu rücken, unter anderem auch angesichts der Tatsache, dass die Europäische Kommission unlängst folgendes verlauten ließ:

»Im Bereich des öffentlichen Gesundheitswesens wird die Kommission die Entwicklung des europäischen virtuellen Zwillings des Menschen unterstützen, der dazu dient, den menschlichen Körper digital zu reproduzieren. Dazu müssen digitale Spitzentechnologien mit dem Zugang zum Hochleistungsrechnen und dem Zugang zu Forschungs- und Gesundheitsdaten über den europäischen Gesundheitsdatenraum verknüpft werden. Diese Leitinitiative zum virtuellen Zwilling des Menschen wird für klinische Entscheidungsunterstützungssysteme, für Instrumente zur persönlichen Gesundheitsprognose und für Konzepte der personalisierten Medizin von Nutzen sein.«[5]

Ferner hat die Kommission Ende Dezember 2023 die »European Virtual Human Twins Initiative« lanciert, welche die Entwicklung und Einführung von Lösungen für virtuelle menschliche Zwillinge im Bereich Gesundheit und Pflege unterstützen soll.[6]

Während mit Ausnahme von *Marina Teller*[7] der rechtswissenschaftliche Diskurs dem digitalen Zwilling bislang kaum Beachtung schenkt, hat die Bioethik den digitalen Zwilling bereits in den Blick genommen.[8] Im Beson-

3 Teller 2021, S. 2.

4 Sandra Wachter etwa sagt zum digitalen Zwilling: »[I]t is reminiscent of exciting science fiction novels, and at the moment that is the stage where it is at.« BBC News 2022.

5 Europäische Kommission 2023a, S. 14 f.

6 Europäische Kommission 2023b.

7 Teller 2021, S. 1 ff.

8 Bruynseels/Santoni de Sio/van den Hoven etwa haben bereits 2018 mannigfaltige ethische Aspekte des humanen digitalen Zwillings beleuchtet.

deren ist hier auf die Arbeit von *Jeffrey David Iqbal, Michael Krauthammer und Nikola Biller-Andorno* hinzuweisen, die mit vielen Fragen an den digitalen Zwilling herantreten und dazu aufrufen, die Gelegenheit zu nutzen, bereits jetzt über die mit dem digitalen Zwilling einhergehenden Herausforderungen nachzudenken, die sonst angesichts der rasanten technologischen Entwicklung über uns hereinbrechen könnten.[9] Der vorliegende Beitrag folgt insofern diesem Ruf und geht zugleich darüber hinaus, indem er versucht, den Fragenkatalog von *Iqbal, Krauthammer und Biller-Andorno* von rechtswissenschaftlicher Warte (nicht abschließend) zu erweitern, dabei aber überdies den digitalen Zwilling als Vehikel zu nutzen, um Fragen an das Daten(schutz)recht zu stellen, respektive dessen Konzepte zu hinterfragen.

Bevor dieser Schritt vollzogen werden kann, gilt es zunächst, den digitalen Zwilling vor dem Hintergrund der Entwicklung der datengetriebenen Medizin zu betrachten sowie dessen (technische) Ausgestaltung und die damit verbundenen Implikationen zu skizzieren.

II. Menschliche Gesundheitswesen – Deep Medicine und Digital Twins

Unter dem Titel »Deep Medicine: How Artificial Intelligence Can Make Healthcare Human Again« hat der US-amerikanische Mediziner *Eric Topol* seine damit verbundenen Hoffnungen zum Ausdruck gebracht: »Die Künstliche Intelligenz in der Heilkunde verspricht uns eine ganzheitliche Übersicht der medizinischen Daten einer Einzelperson, eine bessere Entscheidungsfindung, das Vermeiden von Fehldiagnosen und unnötigen Behandlungen, Hilfe beim Sortieren und Interpretieren geeigneter Untersuchungen und Behandlungsempfehlungen.«[10] Mit den Mitteln der Mustererkennung durch tiefe neuronale Netzwerke können etwa medizinische Bildaufzeichnungen wie Hirnscans, Pathologiebilder, Abbildungen von Hautläsionen, Netzhautaufnahmen, Elektrokardiogramme, Endoskopie-Aufnahmen oder Vitalparameter ausgewertet und interpretiert werden.[11] Gerade in Kombination mit bildgebenden Verfahren kann die Künstliche

9 Iqbal/Krauthammer/Biller-Andorno 2022, S. 594 f.
10 Topol 2020, S. 17.
11 Topol 2019, S. 44.

Intelligenz (KI) somit zu deutlichen Fortschritten in Diagnostik, Vorsorge und Therapie beitragen.[12]

Die Chancen des Einsatzes von KI liegen nicht etwa nur in einer besseren Kontrolle und Beschleunigung der ärztlichen Arbeitsabläufe, oder gar in einer Steigerung der Kosteneffizienz im Gesundheitssektor. Der Einsatz von KI in der »Deep Medicine« biete vielmehr die Gelegenheit, Ärztinnen und Ärzte von zeitaufwändigen Arbeitsroutinen des medizinischen Alltags zu entlasten und damit die nötige Freiheit zu schaffen, um die persönlichen Bindungen und das Vertrauen – »den menschlichen Kontakt« – in der Arzt-Patient-Beziehung »wiederzubeleben« und zu vertiefen.[13] Damit verbindet *Topol* die Erwartung, dass KI und Algorithmen mit fortschreitender Entwicklung zu »work partners«[14] des ärztlichen Arbeitsalltags werden.

In der »Deep Medicine« finden sich allerdings auch außerhalb der »ärztlich-künstlich intelligenten« Tätigkeit noch weitere Verbindungen zur KI. Das größte langfristige Potential der KI im Gesundheitswesen scheint *Topol* in deren Einsatz im Bereich des digital twin respektive digitalen Zwillings zu sehen.[15] Mit den weiteren Möglichkeiten der Text- und Sprachverarbeitung, der Nutzung datenverarbeitender Systeme wie Gesundheits-Apps, Wearables oder elektronischer Patientenakten sowie der Einrichtung einer »massive data infrastructure«[16] eröffnet sich die Perspektive auf eine personalisierte Medizin, die den individuellen Besonderheiten der Patientinnen und Patienten gerecht werden kann. Der digitale Zwilling soll den Leistungserbringern im Gesundheitswesen eine holistische Sicht auf den Patienten ermöglichen.[17] Er kann dabei in verschiedenen medizinischen Bereichen eingesetzt werden, und in allen Phasen des Krankheitsprozesses gibt es aktuel-

12 Dies etwa in den Bereichen Radiologie, Onkologie, Pathologie, Dermatologie, Ophthalmologie, Kardiologie, Gastroenterologie oder beispielsweise auch in der Psychiatrie, Neuropsychiatrie und Neurochirurgie. Vgl. Topol 2019, S. 44 ff.

13 Topol 2020, S. 26. Die Bezeichnung »Deep Medicine« bezieht sich ihrem Sinn gemäß auch nicht allein auf die neueren KI-Technologien des »Deep Learning« in künstlichen neuronalen Netzen, sondern auch auf die weiteren Aspekte des »Deep Phenotyping« mittels umfassender medizinischer Datenanalysen sowie der »Deep Empathy« als Bedingung einer tieferen »Mensch-Mensch-Beziehung« zwischen Ärzten und Patienten. Vgl. Topol 2020, S. 23.

14 Vgl. Topol 2020, S. 26. siehe dazu im Original ders., Deep Medicine: How Artificial Intelligence can make healthcare human again, New York 2019, S. 18: »Eventually, doctors will adopt AI and algorithms as their work partners.«

15 Topol 2019, S. 49; ebenso Cellina u.a. 2023, S. 3.

16 Topol 2019, S. 49.

17 Vallée 2023, S. 1.

le oder potenzielle Anwendungsbereiche für digitale Zwillinge: Prävention, Diagnose und Behandlung von Krankheiten sowie Nachsorge.[18]

Ein ganzkörperlicher digitaler Zwilling fehlt zwar bislang, jedoch haben einige Unternehmen und öffentliche Forschungsinstitute bereits digitale Zwillinge von Organen wie Herz, Lunge und Leber[19] sowie Körperteilen, genauer Fuß und Knöchel,[20] entwickelt. Während digitale Zwillinge für Teile des Körpers entwickelt wurden (oder werden), wird es wohl noch rund 15 Jahre dauern, bis ein digitaler Zwilling des gesamten menschlichen Körpers zur Verfügung steht.[21]

1. Vom Erscheinen des digitalen Zwillings

Während das Konzept eines digitalen Zwillings im medizinischen Bereich erst im Entstehen ist und entsprechend Unschärfen aufweist,[22] finden digitale Zwillinge in der Industrie 4.0 bereits Anwendung, indem sie etwa Maschinen simulieren und Produktionsprozesse abbilden. Dies geschieht, indem das physische Produkt mittels Datenaustausch mit seinem virtuellen Äquivalent verbunden wird, so dass das virtuelle Modell den Status des physischen Produkts dynamisch widerspiegelt.[23] Entsprechend wird der digitale Zwilling als Konvergenztechnologie charakterisiert.[24]

Indem digitale Zwillinge auch im Gesundheitswesen auf dynamischen digitalen Modellen genetischer, biochemischer, physiologischer und verhaltensbezogener Aspekte einzelner Personen basieren, folgen sie einem ingenieurwissenschaftlichen Paradigma und verkörpern einen datengetriebenen Ansatz in der Gesundheitsversorgung.[25] Da es beim digitalen Zwilling in der Medizin jedoch darüber hinaus zu einer Verschmelzung von Informationstechnologie mit Biotechnologie kommt, kann man diesen nicht nur als Konvergenz-, sondern vielmehr als Biokonvergenztechnologie charakterisieren.[26]

---

18 Iqbal/Krauthammer/Biller-Andorno 2022, S. 587.
19 Ebd., S. 588 f.
20 Geneux 2021.
21 Geneux 2021.
22 Braun 2021, S. 395; Cellina u.a. 2023, S. 3.
23 Bruynseels/Santoni de Sio/van den Hoven 2018, S. 1; Rubeis 2023, S. 196.
24 Bagaria u.a. 2020, S. 144.
25 Bruynseels/Santoni de Sio/van den Hoven 2018, S. 1, 3; Braun 2021, S. 395.
26 Braun 2021, S. 395; Amram u.a. 2023, S. 79.

Ähnlich der Industrie 4.0 besteht beim digitalen Zwilling im Gesundheitsbereich die Vision in der Abkehr von der Massenproduktion zur individuellen Fertigung. Anstelle einer massenhaften und reaktiven Gesundheitsversorgung richtet sich der Fokus auf ein personalisiertes und präventives Gesundheitswesen,[27] eine »Health 4.0«.[28]

2. Versprechungen des digitalen Zwillings

Der digitale Zwilling verspricht insofern ein »humaneres« Gesundheitswesen, als er den Eigenheiten des einzelnen Patienten Rechnung tragen, somit wirksamere Behandlungsmethoden für Krankheiten bestimmen und schließlich die Überlebensrate sowie die Lebensqualität des Patienten verbessern kann.[29] Dabei geht die Vision dahin, dass Individuen ihr Leben lang einen digitalen Zwilling haben werden, für den Daten von der Geburt an gesammelt werden, der mit dem Kind wächst und als lebenslange Gesundheitsakte oder medizinisches Untersuchungsobjekt dient.[30] *Hassani, Huang und MacFeely* etwa sprechen von einer *»life cycle healthcare«*[31] und schlagen drei Phasen der Gesundheitsfürsorge mittels digitalem Zwilling vor: vor der Geburt, während des gesamten Lebens sowie nach dem Tod.

Ganz grundsätzlich wird mit dem Einsatz des digitalen Zwillings vom derzeit im Gesundheitswesen[32] vorherrschenden *»one-size-fits-all«*-Ansatz abgerückt, indem die individuelle Variabilität stärkere Berücksichtigung findet.[33] Damit wird die personalisierte Medizin auf eine neue Stufe gehoben, deren Ziel es ist, die richtigen Behandlungen zur richtigen Zeit für die richtige Person bereitzustellen.[34] So werden mittels digitalen Zwillings die Gesundheitsdaten einer Person, bspw. deren genetische Informationen und Krankengeschichte, aber auch Lebensstilfaktoren erfasst und dazu verwen-

27 Bagaria u.a. 2020, S. 143 ff.
28 Ebd., S. 144.
29 Sun u.a. 2022, S. 5.
30 Sun/He/Li 2023, S. 10.
31 Hassani/Huang/MacFeely 2022, S. 7.
32 Eine weitere potenzielle Anwendung von digitalen Zwillingen im Gesundheitswesen ist die Optimierung von Krankenhausbetrieb und -management, indem diese die Kapazitätsplanung erleichtern und es den Gesundheitseinrichtungen ermöglichen sollen, unter anderem künftige Anforderungen zu antizipieren. Vgl. Vallée 2023, S. 3 f.
33 Cho/Martinez-Martin 2023, S. 44; Armeni u.a. 2022, S. 5 f.
34 Armeni u.a. 2022, S. 5 f.

det, personalisierte Behandlungspläne zu erstellen, die auf die Bedürfnisse jedes Einzelnen zugeschnitten sind.[35] Zudem soll es möglich sein, Frühdiagnosen zu stellen, indem Muster und Marker erkannt werden, die auf das Vorhandensein einer Krankheit hindeuten und es Ärzten beispielsweise erlauben, bei einer Person frühzeitig eine Krebserkrankung festzustellen.[36] Auch soll dank digitaler Zwillinge das Fortschreiten einer Krankheit präzise vorhergesagt sowie die Behandlung chronischer Krankheiten besser unterstützt werden können.[37]

Wie eine solche personalisierte und präzise Behandlung aussehen könnte, lässt sich am Beispiel der sogenannten »künstlichen Bauchspeicheldrüse« für Patienten mit Typ-1-Diabetes beobachten. Bei diesem Modell werden ein mathematisches Modell des menschlichen Glukosestoffwechsels und ein Regelungsalgorithmus, der die Insulinabgabe modelliert, sowie Daten von einem implantierten Glukosesensor zu einem patientenspezifischen digitalen Zwilling zusammengefügt. Dieser berechnet kontinuierlich den Insulinbedarf und steuert eine implantierte Insulinpumpe an, die die Insulinkonzentration im Blut des Patienten anpasst.[38]

Bei alledem wird erwartet, dass der digitale Zwilling auch die Möglichkeit der Fernüberwachung – wohl in Echtzeit[39] – von Patienten eröffnet, wodurch etwa Ärztinnen Vitalparameter, Symptome und die Einhaltung von Behandlungsvorschriften aus der Ferne verfolgen können und die Möglichkeiten der Telemedizin verbessert wird.[40] Chirurgen sollen sich dank des digitalen Zwillings auch besser auf Operationen vorbereiten können, indem dieser bei der Erstellung eines chirurgischen Operationsplans beigezogen wird und der Operationsplan am virtuellen menschlichen Körper getestet werden kann.[41]

Auch bei medikamentösen Behandlungen versprechen digitale Zwillinge mehr Präzision, indem der Datenkörper des Patienten kopiert wird. Die Kopien werden rechnerisch mit tausenden von Arzneimitteln behandelt, um so

35 Cellina u.a. 2023, S. 13.
36 Ebd., S. 13; Geneux 2021.
37 Cellina u.a. 2023, S. 13; Sun/He/Li 2023, S. 9.
38 Laubenbacher/Sluka/Glazier 2021, S. 1105.
39 Sun u.a. 2022, S. 5.
40 Cellina u.a. 2023, S. 13; Sun/He/Li 2023, S. 10.
41 Sun/He/Li 2023, S. 10.

das am besten wirksame Arzneimittel zu ermitteln und schließlich den tatsächlichen Patienten mit diesem Mittel zu behandeln.[42]

Neben ihrer Anwendung zur Behandlung im Gesundheitswesen könnten Datenkörper auch bei der Durchführung klinischer Studien nützlich sein, indem Kopien von digitalen Zwillingen zur Erprobung von Arzneimitteln im Frühstadium verwendet werden.[43] Damit ließe sich wohl auch die Anzahl von Tierversuchen verringern.[44]

Digitale Zwillinge sollen aber nicht nur eine präzise und effiziente Behandlung von Krankheiten ermöglichen, sie sollen auch für die Prävention eingesetzt werden.[45] Eine Idee richtet sich zum Beispiel darauf, mit digitalen Zwillingen einen gesunden Lebensstil zu fördern und etwa Herzkrankheiten vorzubeugen, indem der digitale Zwilling bei seinem analogen Gegenüber Daten sammelt, bspw. mittels Smartwatch, welche die Herzfrequenz misst, diese Daten mithilfe von maschinellem Lernen analysiert und auf Grundlage dieser Analyse dem analogen Zwilling Empfehlungen für verschiedene Aktivitäten macht, passend zu dessen Vorlieben und körperlicher Verfassung. Der Datenkörper kann auch aufgrund von Gewicht, Kalorienverbrauch, klinischen Daten und/oder biologischen Signalen, die mittels verschiedener Sensoren gewonnen werden, Risikofaktoren wie Fettleibigkeit, Alkohol- oder Tabakkonsum analysieren und dem realen Zwilling helfen, diese je nach persönlichem Bedarf zu reduzieren.[46]

Es scheint also, dass es aufgrund von Informationen des digitalen Zwillings beim Patienten eben nicht nur zu Interventionen durch Ärzte kommt, sondern der digitale Zwilling selbst mit seinem analogen Zwilling kommunizieren kann. Was das für Auswirkungen auf das Gegenüber haben könnte, wird unter III. kritisch beleuchtet.

3. Formierung(en) des digitalen Zwillings

Die Idee, Menschen zu replizieren, ist freilich nicht neu. Dementsprechend wird der Diskurs von vielen zwillingsartigen Geschöpfen und Mensch-Maschinen-Visionen, wie etwa »Doppelgängern«, »Automaten«, »Robo-

42 Björnsson u.a. 2019, S. 1 f.
43 Armeni u.a. 2022, S. 8 f.
44 Geneux 2021.
45 Bagaria u.a.2020, S. 143 ff.
46 Bagaria u.a.2020, S. 150.

tern«, »Simulationen« und »Phantomen« bevölkert.[47] Während es bei der Schöpfung solcher Kreaturen wohl noch um die Schaffung von neuen »menschenartigen« Wesen, als Nachbildungen des Gattungswesens geht, dient der digitale Zwilling dazu, ein menschliches Individuum nachzubilden, eben zu verdoppeln oder zu spiegeln und darüber hinaus gewissermaßen selbst zum Leben zu erwecken. So ist denn oftmals auch die Rede vom »Human Digital Twin«[48] oder vom »Digital Human Twin«[49], der zu einer »live or near-live«[50] Repräsentation einer Patientin oder eines Patienten wird. Die Idee der exakten Verdoppelung des Individuums wird dabei durch den Begriff des »Zwillings« hervorgehoben, denn wie *Deborah Lupton* feststellt, wird damit eine sehr starke Ähnlichkeit suggeriert, vor allem, wenn man dabei eher an eineiige als an zweieiige menschliche Zwillinge denkt.[51]

Den Aspekt des »Lebendigen« gilt es hervorzuheben, denn, und insofern vorgreifend, der digitale Zwilling bildet nicht einfach nur den (lebenden) Menschen ab,[52] vielmehr unterhält der digitale Zwilling eine dynamische, bidirektionale Echtzeit-Datenverbindung mit seinem menschlichen Gegenüber.[53] Oder um es in den Worten von *Liu, Meyendorf und Mrad* auszudrücken: »The digital twin is actually a *living model* of the physical asset or system, which continually adapts to operational changes based on the collected online data and information, and can forecast the future of the corresponding physical counterpart.«[54]

Um den Aspekt des Lebendigen zu betonen, verwendet der vorliegende Beitrag nebst dem Begriff des digitalen Zwillings auch den Begriff des »Datenkörpers«, angelehnt an *Konrad Becker*. Gemäß *Becker* hat der reale physische Körper im Cyberspace ein virtuelles Gegenstück, den Datenkörper, ent-

47 Vgl. Popa u.a. 2021, S. 1.

48 So etwa Armeni u.a. 2022, S. 4; Iqbal/Krauthammer/Biller-Andorno 2022, S. 588; Miller/Spatz 2022, S. 23; Kamel/Maged/Zhang 2021, S. 3; Shengli 2021, S. 1.

49 So bei Cellina u.a. 2023, S. 2.

50 Iqbal/Krauthammer/Biller-Andorno 2022, S. 584.

51 Lupton 2021, S. 409.

52 Popa u.a. 2021, S. 1.

53 Kamel/Maged/Zhang 2021, S. 3; Hassani/Huang/MacFeely 2022, S. 4.

54 Liu/Meyendorf/Mrad 2018, S. 020023–1 [Hervorhebungen hinzugefügt]. Sun/He/Li 2023 scheinen noch weiter zu gehen: »However, the [digital twin] is more than just a digital model that is connected with a real-life twin through various emerging technologies. It is a *living, intelligent* and evolving model which can optimise the processes and continuously predicts future statuses (e.g. defects, damages and failures) through the closed-loop optimisation between DT and surrounding environment.« S. 2 [Hervorhebungen hinzugefügt].

wickelt. »Dieser Datenkörper besteht nicht aus Fleisch und Blut, sondern aus der Gesamtheit aller Daten, die mit einer Person verknüpft sind […]. Wie der physische Körper im realen Raum, so ist es in der Info-Sphäre dieser Datenkörper, der die soziale Präsenz einer Person vermittelt.«[55] *Becker* hat bei dieser Beobachtung indes nicht den digitalen Zwilling vor Augen, dennoch erweist sich der Begriff vorliegend als produktiv, denn er ruft in Erinnerung, dass diese Entität auf Daten angewiesen ist, quasi durch (Körper-)Daten »mit Leben gefüllt« und mit Lebendigem verknüpft wird.

Darüber hinaus weist er darauf hin, dass Daten gespeichert werden können. Der Datenkörper kann damit quasi in »Speicherhaft«[56] genommen werden. Gleichzeitig, und insoweit paradox, bedeutet die Anwesenheit des Datenkörpers in der Info-Sphäre, dass er zeit- und ortsunabhängig ist – er ist »ubipräsent«[57]. Es scheint also, als hätten wir es beim *human digital twin* mit einer Entität zu tun, die das Humane nicht nur abbildet, sondern darüber hinaus zu überschreiten vermag. Bevor auf diese und weitere Problemstellungen eingegangen werden kann, gilt es zunächst, das eingangs gegebene Versprechen einzulösen und zu skizzieren, wie sich ein solcher Datenkörper technisch formiert und von anderen Computermodellen abgrenzt.

In seinem Grundmodell besteht der digitale Zwilling aus drei Hauptkomponenten: (1) einem realen Objekt, (2) dessen virtuellem Äquivalent und (3) der Datenverbindung zwischen der physischen und der virtuellen Entität.[58]

Beim realen Objekt kann es sich um eine einzelne Einheit auf zellulärer Ebene bis hin zu einem System oder Prozess handeln. Obschon die Bandbreite und der Umfang der physischen Objekte, auf das sich das virtuelle Äquivalent beziehen kann, weit sind, geht es jeweils um die Repräsentation einer bestimmten einzelnen physischen Entität. Soll ein digitaler Zwilling für eine Gruppe ähnlicher Entitäten entwickelt werden, so scheint der übliche Ansatz darin zu bestehen, einen Prototyp für die Gruppe zu entwickeln und dann jeder einzelnen Einheit einen individualisierten digitalen Zwilling zuzuweisen.[59]

Die virtuelle Entität stellt dabei den eigentlichen digitalen Zwilling dar. Dieser basiert typischerweise auf einem mechanistischen sowie einem Machine-Learning-Modell. Durch die Kombination dieser Modellkompo-

55 Becker 2003, S. 195.
56 Lobe 2019, S. 140.
57 Vgl. Noller 2022, S. 45.
58 Cellina u.a. 2023, S. 1 f.; Korenhof/Blok/Kloppenburg 2021, S. 1754.
59 Korenhof/Blok/Kloppenburg 2021, S. 1754.

nenten, die sich auf mehrere Datenquellen stützen, ergibt sich ein für den jeweiligen Patienten spezifischer Personalisierungsgrad.[60] Es kommt also zu einer Verschmelzung von Bio- und Informationstechnologie.[61] Dabei greifen die Modelle sowohl auf Datensätze[62] als auch auf personenbezogene Daten zurück, wobei diese aus dem Spektrum traditioneller medizinischer Daten (bspw. genetische Daten, Daten aus bildgebenden Verfahren) und nicht-medizinischer Daten (bspw. Daten aus den sozialen Medien) sowie aus den Schattierungen dazwischen (bspw. Anzahl der zurückgelegten Schritte) stammen.[63] Dabei ist es zentral, dass die Daten hochwertig, korrekt und vollständig sind, da dies die Qualität des virtuellen Bildes des digitalen Zwillings sicherstellt.[64] Dies betrifft nicht nur die personenbezogenen Daten, sondern auch die Datensätze, mit denen die Daten des Patienten verglichen werden, wobei sich hier die besondere Problematik der Verzerrungen solcher Daten und des damit verbundenen Diskriminierungspotentials aktualisiert.[65]

Es bleibt indes nicht bei den eingangs erfassten Daten, vielmehr besteht die Vision darin, dass dem digitalen Zwilling kontinuierlich weitere Daten übertragen werden, dies durch einen Strom von (fast) Live-Daten, die den gegenwärtigen Zustand des physischen Zwillings abbilden.[66] Diese Daten sollen dabei unter anderem von den Patienten auf dem Weg der Selbstvermessung gesammelt und eingespeist werden.[67] Die Daten sind folglich nicht nur *real-time*, sondern auch *real-world*.[68] Der digitale Zwilling eröffnet damit die Möglichkeit einer dynamischen – im Sinne einer sich fortwährend aktualisierenden – Nachbildung des menschlichen Körpers.[69]

Dabei verläuft der Datenstrom nicht einseitig. Vielmehr besteht die Vorstellung darin, dass die virtuelle Entität aufgrund der eingespeisten Daten Schlussfolgerungen zieht und Handlungsempfehlungen ableitet.[70] Dies passiert, indem der digitale Zwilling unter anderem mittels künstlicher Intel-

60 Iqbal/Krauthammer/Biller-Andorno 2022, S. 584.
61 Vgl. Braun 2021, S. 395.
62 Schwartz u.a. 2020, S. 14; Acosta u.a. 2022, S. 1776.
63 Iqbal/Krauthammer/Biller-Andorno 2022, S. 584; Cellina u.a. 2023, S. 4.
64 Cellina u.a. 2023, S. 4; Teller 2021, S. 4.
65 Schwartz u.a. 2020, S. 14; Teller 2021, S. 4.
66 Iqbal/Krauthammer/Biller-Andorno 2022, S. 584.
67 Boer 2020, S. 408.
68 Kamel/Maged/Zhang 2021, S. 2.
69 Bruynseels/Santoni de Sio/van den Hoven 2018, S. 1 f.
70 Iqbal/Krauthammer/Biller-Andorno 2022, S. 586.

ligenz eine Person simuliert, um deren zukünftige (gesundheitliche) Entwicklungen vorherzusagen und auf Grundlage dieser prädiktiven Simulationen via Informationsfeedback zu warnen oder geeignete Behandlungen respektive Änderungen der Lebensweise zu empfehlen.[71] Dabei scheint der digitale Zwilling einen sogenannten »data-first«-Ansatz zu verfolgen. Dies meint, dass es keiner vorgängigen Hypothesen oder sogar einer Vorspezifizierung von Variablen bedarf, um Assoziationen und Muster in Daten zu erkennen, so dass von der KI »Antworten« geliefert werden, obschon keine spezifische Frage gestellt wurde.[72] Die ausgefeiltesten digitalen Zwillinge verbessern sich zudem auch selbst – sie überwachen kontinuierlich die Abweichungen zwischen ihren Vorhersagen und Beobachtungen und nutzen diese Abweichungen, um ihre eigene Genauigkeit zu verbessern.[73]

Die Handlungsempfehlungen der virtuellen Entität sollen direkt an die Patienten kommuniziert werden, bspw. via Avatar.[74] Die Datenverbindung ist somit bidirektional, d.h. die physische Entität speist die virtuelle Entität mit Daten, während diese wiederum Informationen an die physische Entität zurückgibt; es kommt zu einer Feedback-Schleife.[75] Diese Informationen und damit verbundene Interventionen erzeugen dann neue Daten, die in das virtuelle Modell eingespeist werden, wodurch die Schleife von neuem beginnt.[76] Es kommt zu einer (permanenten) Interaktion und Kommunikation zwischen Mensch und Maschine.[77]

Inwiefern es dabei bleiben wird, dass die virtuelle Entität Informationen an ihr Gegenüber gibt, oder ob es nicht so weit gehen wird, dass die virtuelle Entität direkt auf die Physis des Menschen einwirkt, lässt sich momentan nicht abschließend beurteilen. Es ist indes denkbar, dass dies passieren könnte, ruft man sich das Beispiel der künstlichen Bauchspeicheldrüse in Erinnerung, bei der direkt die implantierte Pumpe angesteuert wird.

Es ist die dynamische und bidirektionale Echtzeit-Datenverbindung, die das Alleinstellungsmerkmal des digitalen Zwillings bildet und diesen von anderen Computermodellen abgrenzt.[78] Digitale Zwillinge sind keine unidi-

71 Cellina u.a. 2023, S. 3; Braun 2022, S. 210; Kamel/Maged/Zhang 2021, S. 3.
72 Cho/Martinez-Martin 2023, S. 45.
73 Laubenbacher/Sluka/Glazier 2021, S. 1105.
74 Braun 2022, S. 210.
75 Kamel/Maged/Zhang 2021, S. 2; Hassani/Huang/MacFeely 2022, S. 3; Rubeis 2023, S. 203.
76 Rubeis 2023, S. 203.
77 Vgl. Braun 2022, S. 210; vgl. Rubeis 2023, S. 197.
78 Hassani/Huang/MacFeely 2022, S. 4; umfassend dazu Korenhof/Blok/Kloppenburg 2021, S. 1755.

rektionale Repräsentation, keine digitalen Klone[79], kein digitaler Schatten, kein Simulationsmodell einer physischen realen Einheit im virtuellen Bereich;[80] vielmehr erlaubt es die Datenverbindung der virtuellen Entität von seinem realen Gegenstück zu lernen sowie zu dessen Verbesserung beizutragen[81] und zudem kontinuierlich mit der von ihm repräsentierten physischen Entität zu kommunizieren.[82] Die Repräsentation ist damit hochdynamisch, folgt der physischen Einheit und greift in sie ein.[83]

Das Konzept des digitalen Zwillings ist damit auch der Versuch, digitale Repräsentationen zu schaffen, die über die bloße Abstraktion hinausgehen, indem sie die zeitliche und räumliche Distanz zwischen der Repräsentation und dem Repräsentierten minimieren.[84]

Dabei ist es ist die oben bereits zur Sprache gekommene Verfügbarkeit von Smart Wearables und Internet of Things-Anwendungen, die permanent und allgegenwärtig beim Patienten und/oder dessen Umgebung Daten sammeln und speichern, sowie KI, Anwendungen des maschinellen Lernens und eine ausreichende Rechenleistung, welche aus den großen Datenmengen aussagekräftige Informationen extrahieren können, die es erst ermöglichen, digitale Zwillinge mit den soeben aufgezeigten Potentialen zu erschaffen.[85] Folglich benötigt die Entwicklung eines digitalen Zwillings ein breites Spektrum an Kompetenzen, und es bedarf eines erheblichen finanziellen Aufwands. Entsprechend erstaunt es nicht, dass ein Großteil der Entwicklungsarbeit im privaten Sektor geleistet (werden) wird,[86] da dieser das Knowhow und die technologischen Mittel für das Sammeln, Speichern und Analysieren großer und heterogener Datenmengen hat.[87] Mit anderen Worten sind es die großen Technologieunternehmen des pri-

79 Wie bereits erläutert, bildet der Datenkörper als virtuelle Entität den analogen Körper ab. Angesichts dessen, dass dabei die verschiedenen biologischen Aspekte des analogen Körpers möglichst präzise nachgebildet werden sollen, respektive der Datenkörper ein möglichst realitätsnahes Abbild des analogen Körpers bilden soll, wird von einigen Autoren der digitale Zwilling als »digital clone« bezeichnet (bspw. Amram u.a. 2023, S. 79). Diese Bezeichnung greift indes zu kurz. Vgl. dazu Braun 2021, S. 394.

80 Kamel/Maged/Zhang 2021, S. 3.

81 Miller/Spatz 2022, S. 26; vgl. Rubeis 2023, S. 193.

82 Haleem u.a. 2023, S. 29.

83 Korenhof/Blok/Kloppenburg 2021, S. 1755 ff.

84 Ebd.

85 Bruynseels/Santoni de Sio/van den Hoven 2018, S. 2; Armeni u.a. 2022, S. 4 f.; Rubeis 2023, S. 198.

86 Vgl. Geneux 2021.

87 Vgl. Sharon 2018. S. 1.

vaten Wirtschaftssektors, die digitale Zwillinge entwickeln,[88] wobei es zu Verbindungen zwischen Big-Data-Unternehmen, die über die Rechen- und Speicherressourcen verfügen, Gesundheitsunternehmen, die die Daten bereitstellen, und biomedizinischen Forschungszentren, die die Analyse und Interpretation der Modelle leiten, kommt.[89]

Es treten damit neue Akteure mit ganz unterschiedlichen soziotechnischen Funktionen auf und – wie *Iqbal und Biller-Andorno* beschreiben – bringen einen neuen Typ von »hybriden Akteuren«[90] hervor.[91] Solche sogenannten »payer-providers« heben die im Gesundheitswesen übliche Trennung von privater Dienstleistung und Behandlungskostenerstattung auf und führen diese – wie etwa im Fall von »Amazon Care« – in Gestalt eines umfassenden technikgestützten Angebots von Telemedizin, Krankenversicherung, Medikamentenversorgung und weiteren medizinischen Dienstleistungen zusammen. Aber auch intermediäre Unternehmen wie »Amazon Care« bilden freilich nur eine Spitze des Eisbergs, der sich aus einer Vielzahl einzelner neuer Akteure im Gesundheitswesen formiert hat, die traditionell nicht unbedingt zum Anwendungsbereich medizinischer Dienstleistungen gehört haben. Zu diesen gehören insbesondere auch Anbieter digitaler Konsumgüter (wie Wearables), Vertriebsplattformen für digitale Gesundheitsanwendungen oder auch Provider für elektronische Krankenakten oder Krankenhaus-Managementsysteme.

In Anbetracht der Tatsache, dass es bereits jetzt verschiedene Initiativen und potentielle Anbieter gibt, die die Entwicklung und den Einsatz der *digital twin* Technologie vorantreiben[92], stellt sich ferner die Frage, ob der einzelne Patient mehrere digitale Zwillinge haben wird – ähnlich wie dies bei den sogenannten »digital shadows« der Fall ist, bei denen verschiedene Unternehmen unabhängig voneinander virtuelle Repräsentationen von Konsumenten erstellen.[93]

88 Vgl. Braun 2021, S. 399.

89 Cellina u.a. 2023, S. 4 f.

90 Iqbal/Biller-Andorno 2022, S. 2.

91 In der Folienabbildung von Iqbal/Krauthammer/Biller-Andorno 2022, S. 586 wird zudem eine Abhängigkeit von drei unterschiedlichen »user groups« nahegelegt: »Healthcare Providers, MedTech and Pharma Industry and Individuals«.

92 Bruynseels/Santoni de Sio/van den Hoven 2018, S. 3. Eine Liste von Gesundheits- und Pharmaunternehmen, die Technologie für eine intelligente, personalisierte Gesundheitsversorgung einsetzen, respektive entwickeln, findet sich bei Sahal/Alsamhi/Brown 2022, S. 16.

93 Vgl. Mocanu/Sibony 2023, S. 234.

III. Digitalität des Datenkörpers – Der digitale Zwilling und sein Gegenüber

Der digitale Zwilling gehört zu den Innovationen einer datengetriebenen Hochleistungsmedizin, die »uns irgendwann weit über die Summe der Teile menschlicher und maschineller Intelligenz hinausführen wird«.[94] Damit bekommen wir es in der »Deep Medicine« also mit doppelten Mensch-Maschine-Assoziationen zu tun, in denen menschliche und künstliche Intelligenz konvergieren und sich *Topol* zufolge auf die drei Ebenen der ärztlichen Tätigkeit, der Gesundheitssysteme und der beteiligten Patienten auswirkt.[95]

Wie diese Wirkung aussehen könnte, soll nachfolgend spekulativ antizipiert werden. Dabei gilt es darauf hinzuweisen, dass den folgenden Ausführungen eine Vorstellung von digitalen Zwillingen zugrunde liegt, die Zukunftsszenarien abbilden. Wie fern oder nahe diese Zukunft ist, muss indes offen bleiben, zumal sich die Einschätzungen in der Debatte stark unterscheiden.[96]

1. Mensch-Maschinen-Schnittstellen

Indem der digitale Zwilling zur »live or near-live«[97] Repräsentation eines Patienten wird, bildet sich auf Seiten des Patienten eine eigene Mensch-Maschinen-Beziehung heraus.[98] Kommt der digitale Zwilling im Rahmen der ärztlichen Behandlung zum Einsatz, findet sich wohl auch zwischen Arzt und digitalem Zwilling eine Mensch-Maschine-Schnittstelle, ähnlich jener bei anderen »Deep Medicine«-Anwendungen.[99] Darüber hinaus kommt es

94 Topol 2019, S. 52: »[…] and will eventually take us well beyond the sum of the parts of human and machine intelligence«.

95 Ebd., S. 44.

96 Die Fallstudien des DSI Strategy Lab 2022 zu den Bereichen »Diagnose«, »Therapie«, »Prävention« und »Mittelallokation« zeigen mögliche Entwicklungen der Künstlichen Intelligenz in der Medizin auf, wobei diese im »Jetzt« beginnt, über eine »nahe Zukunft« hin zu einem »Ferne-Zukunft-Szenario« geht. In letzterem wird durchgespielt, wie eine KI als »digitaler Zwilling« relevante Entscheidungen weitgehend autonom trifft. Coveney/Highfield 2023 scheinen dagegen den digitalen Zwilling in einer weniger fernen Zukunft zu verorten.

97 Iqbal/Krauthammer/Biller-Andorno 2022, S. 584.

98 Vgl. van der Valk u.a. 2020, S. 7.

99 Vgl. hierzu Gruber 2023, S. 277 ff.

zu einer Maschine-Maschine-Schnittstelle, indem der digitale Zwilling über den Datenstrom ständig Aktualisierungen erhält und sowohl Rohdaten als auch vorverarbeitete Daten verarbeitet.[100] Wie vielfach aufgezeigt, handelt es sich bei der Datenverbindung um eine bidirektionale Verbindung. Solange der Datenkörper über diese Verbindung seinem analogen Gegenüber Informationen übermittelt, bspw. mitteilt, dass die Insulinkonzentration im Blut des Patienten zu gering ist, kann diese Verbindung wohl noch als Mensch-Maschine-Schnittstelle qualifiziert werden. Vergegenwärtigt man sich indes das Beispiel der künstlichen Bauchspeicheldrüse, bei der die virtuelle Entität eine implantierte Pumpe ansteuert, welche die Insulinkonzentration im Blut anpasst, scheinen wir es mit einer weiteren Maschine-Maschine-Schnittstelle zu tun zu haben. Die Kopplung des analogen Körpers mit dem Datenkörper führt somit zu neuen Mensch-Maschinen-Schnittstellen.[101]

Die Konzeptualisierung des digitalen Zwillings als möglichst realitätsnahes Abbild des analogen Körpers respektive der physischen Entität legt zunächst nahe, dass eine Abhängigkeit des Datenkörpers von der physischen Entität besteht, indem der digitale Zwilling seinen »Zustand« von der physischen Entität übernimmt[102] und dieser mit einer Art Unterwürfigkeit begegnet.[103] Die Vorstellung einer solchen sekundären Positionierung des digitalen Zwillings gegenüber der physischen Entität greift jedoch zu kurz, zumal das Verhältnis der beiden eben gerade nicht unidirektional, sondern bidirektional ist. Indem Informationen vom digitalen Zwilling zurück an sein physisches Gegenüber fließen, werden dessen Verhalten sowie Zustand beeinflusst, was zur Konsequenz hat, dass die Unterscheidung zwischen Vorbild und Abbild verschwimmt und damit auch das Machtverhältnis, wer wen kontrolliert (oder was wen kontrolliert).[104] *Simona Chiodo* geht dabei so weit zu behaupten, dass »the constantly mutual relationship between the physical object and the digital object, i.e. its digital twin, means not only that the latter changes if the former changes but also, and especially, that the former changes if the latter changes – which gives human digital twins a kind of power over humans […]«.[105]

100 Vgl. van der Valk u.a. 2020, S. 7.
101 Vgl. Wiedemann 2022, S. 78.
102 Iqbal/Krauthammer/Biller-Andorno 2022, S. 593.
103 Korenhof/Blok/Kloppenburg 2021, S. 1757 f.
104 Iqbal/Krauthammer/Biller-Andorno 2022, S. 593.
105 Chiodo 2023, S. 159.

Das »wechselseitige Aufeinander-Bezogen-Sein und In-Beziehung-Stehen«[106] von analogen und digitalen Körpern ist vorliegend von besonderem Interesse, denn, wie bereits festgestellt, wird der digitale Zwilling quasi durch Daten mit Leben gefüllt und mit Lebendigem verknüpft. Eine ähnliche Beobachtung – jedoch nicht primär auf den digitalen Zwilling bezogen – macht auch *Wiedemann*: »[N]nur die Bezugnahme auf oder die praktische Auseinandersetzung mit den in Geräten gespeicherten Daten lässt den digitalen Körper ›lebendig‹ und im Sinne Bruno Latours zu einem *sozialen Akteur* werden, das heißt zu einem ›Ding, das eine gegebene Situation verändert, indem es einen Unterschied macht‹.«[107]

Die vorliegende Mensch-Maschine-Verbindung im Sinne der Patient-Maschine-Beziehung ist also von einer doppelten Körpergestaltung geprägt, indem der digitale Zwilling eine bidirektionale Interaktionsbeziehung mit seinem physischen Gegenüber entfaltet und damit dessen Körperverfassung fortdauernd modelliert, wie er auch selbst modelliert wird. Damit wird die Unterscheidung zwischen dem Kontrollierten und dem Kontrollierenden unscharf.[108]

2. Responsibilisierung, Modellierung, Disziplinierung und Subsituierung

Indem es dem einzelnen Patienten mittels digitalem Zwilling ermöglicht wird, eine größere Rolle bei der Pflege seiner eigenen Gesundheit zu spielen, verspricht dies mehr persönliche Freiheit im Umgang mit den eigenen biologischen Gegebenheiten.[109] Damit einher geht aber eine Responsibilisierung des Patienten, denn es kommt zu einer Verlagerung des Gesundheitsmanagements weg vom Staat auf die Schultern des einzelnen Patienten.[110] In diesem Kontext wird auch befürchtet, dass mit der zunehmenden Forderung, die Medizin zu einer Präventivmedizin zu machen, die Bürger dazu gedrängt werden, einen digitalen Zwilling zu nutzen[111] oder etwa Versiche-

106 Wiedemann 2022, S. 82.
107 Ebd., mit Zitat aus Latour 2007, S. 123 [Hervorhebungen hinzugefügt].
108 Vgl. Iqbal/Krauthammer/Biller-Andorno 2022, S. 593.
109 Ebd., S. 583; Popa u.a. 2021, S. 12.
110 Vgl. Sharon 2017, S. 101; vgl. auch Krutzinna 2021, S. 403.
111 Vgl. Boer 2020, S. 406; vgl. Wieser 2019, S. 438.

rungen ihren Versicherten Prämienverbilligungen verweigern, wenn diese keinen digitalen Zwilling nutzen wollen.[112]

Was als »gesund« gilt, könnte dabei von den bei der Konstruktion eines digitalen Zwillings verwendeten Datensätzen definiert werden, indem diese die Konstrukte von Normalität und Gesundheit formieren.[113] Sind diese Daten verzerrt, etwa indem ethnische Minderheiten zu wenig berücksichtigt werden oder geschlechterspezifische Verzerrungen vorliegen, kann dies zu ungenauen Ergebnissen für jeden Patienten führen, der nicht dem typischen Profil des verwendeten Datensatzes entspricht.[114] Es droht das Szenario, das bereits im Rahmen der Selbstvermessungstechnologien diskutiert wird: Die Schaffung von neuen ungleichheitsproduzierenden Ordnungen, indem jene exkludiert werden, die mit anderen »gesunden« oder »normalen« Datenkörpern nicht mithalten können.[115] Damit weitet sich das Beziehungsnetz des Datenkörpers aus, denn dieser steht nun nicht nur in Relation zum analogen Körper, sondern auch zu anderen Datenkörpern.[116] Dieses Netz könnte sich sogar noch weiterspinnen, indem der digitale Zwilling nicht nur bei seinem analogen Zwilling Implikationen zeitigt, sondern auch bei (analogen) Dritten, denn die Analyse der Krankheitsgeschichte oder der genetischen Daten des Patienten können Hinweise auf die Familienangehörigen und genetisch Verwandten eines Patienten geben.[117] Die »Phänomenologie des Digital Twin« ist entsprechend geprägt von dezentralen, distribuierten, bidirektionalen (multiplen) Mensch-Maschine-Assoziationen.

Es gibt indes auch Stimmen, die argumentieren, dass der Ansatz des digitalen Zwillings im Gegensatz steht zu den erwähnten Konzepten, die einen normalen oder gesunden Zustand auf der Grundlage von Statistiken definieren, die aus großen Kohortenstudien abgeleitet werden. Vielmehr biete der digitale Zwilling die Möglichkeit, den Normalzustand auf der Grundlage der detaillierten Krankengeschichte einer Person zu definieren und natürliche Variationen zwischen Individuen, die es ansonsten schwierig machen, genau zu bestimmen, was normal ist, abzubilden, etwa indem Faktoren wie

112 Popa u.a. 2021, S. 14.
113 Vgl. Iqbal/Krauthammer/Biller-Andorno 2022, S. 590; vgl. Cho/Martinez-Martin 2023, S. 47.
114 Armeni u.a. 2022, S. 10.
115 Wiedemann 2022, S. 84.
116 Vgl. Wiedemann 2022, S. 84.
117 Vgl. Geneux 2021.

Alter, Lebensstil und genetischer Hintergrund berücksichtigt werden.[118] Mit andern Worten: Das Normale wird individualisiert.[119]

Nichtsdestotrotz hat der digitale Zwilling das Potential, nicht nur Schwachstellen des physischen Gegenübers aufzuzeigen, sondern auch Empfehlungen zu dessen Optimierung zu geben. Ein digitaler Zwilling bildet also nicht nur die physische Einheit ab, sondern beschreibt auch, wie die physische Einheit idealerweise funktionieren sollte.[120] Entsprechend wohnt dem digitalen Zwilling eine formende Rolle gegenüber der physischen Entität inne. Mit anderen Worten: Der digitale Zwilling ist nicht rein deskriptiv (nachahmend), sondern vielmehr auch präskriptiv (lenkend).[121]

Die bidirektionale Verbindung, die mittels Information und Feedback-Schleife den analogen Körper in Richtung optimaler Zustände zu lenken vermag, weist gemäß *Paulan Korenhof, Vincent Blok und Sanneke Kloppenburg* eine auffällige Ähnlichkeit mit der Kybernetik auf.[122] Unter Bezugnahme auf *Habermas* kommen sie zu dem Schluss, dass der digitale Zwilling als Steuerungstechnik verstanden werden kann.[123] Angesichts dessen geben sie zu bedenken, dass dies Fragen aufwirft, was dessen Ziele sind, wie diese erreicht werden und wer darüber entscheidet.[124]

Ebenfalls problematisch ist der Umstand, dass es, indem digitale Zwillinge zur Prävention genutzt werden, zu einer umfassenden, kontinuierlichen datengestützten Überwachung des Körpers kommt. Dies macht es zwar möglich, zu erfassen, was zwischen den Arztbesuchen passiert und so longitudinale Datensätze zu erstellen, wodurch Patientinnen, wie soeben erwähnt, zu ihren eigenen Kontrollgruppen werden können.[125] Gleichzeitig ist mit solch einer Überwachung des Körpers der Wille zur Kontrolle und Bewertung verbunden – ein Charakteristikum der gegenwärtigen Überwachungs- und Kontrollgesellschaft.[126]

Doch während Überwachung traditionell als etwas von außen Kommendes konzeptualisiert wird, scheint auch für den digitalen Zwilling das zu gelten, was bereits im Rahmen des Self-Trackings festgesellt wurde: Hier

118 Bruynseels/Santoni de Sio/van den Hoven 2018, S. 4; Cho/Martinez-Martin 2023, S. 49.
119 Bruynseels/Santoni de Sio/van den Hoven 2018, S. 4.
120 Korenhof/Blok/Kloppenburg 2021, S. 1755 ff.
121 Ebd., S. 1757 f.
122 Ebd., S. 1764.
123 Korenhof/Blok/Kloppenburg 2021, S. 1765.
124 Ebd.
125 Vgl. Winkler und Prainsack 2021, S. 376.
126 Wiedemann 2022, S. 83; vgl. Sharon 2017, S. 98.

wird der Nutzer dazu ermutigt, den medizinischen Blick in Form einer Selbstüberwachung auf sich selbst zu richten.[127] Dabei kennt der digitale Zwilling sein Gegenüber ausgesprochen gut. Gestützt auf dessen Kalorienverbrauch, Gewicht, klinische Daten und/oder biologische Signale, die von verschiedenen Sensoren gewonnen werden, kann der digitale Zwilling etwa Situationen erkennen, die mit Fettleibigkeit, Alkohol- oder Tabakkonsum zusammenhängen.[128] Durch die bidirektionale Ausgestaltung des digitalen Zwillings ist es möglich, dass dieser seinen Nutzer auf ungesunde Essgewohnheiten aufmerksam macht und ihn ermutigt, diese zu ändern. Dies mag zwar der Gesundheit des analogen Zwillings zuträglich sein, es birgt aber auch die Gefahr, dass die Kommentierung des Essverhaltens und die Vorhersage, wie sich dieses auf die Gesundheit auswirkt, dazu führt, dass der Nutzer sich von seiner Wahrnehmung von sich selbst und der Welt entfremdet, etwa indem Essen nur noch von einer quantifizierenden Perspektive her betrachtet wird.[129] Zudem stellt sich angesichts der engen Verbindung zwischen der Patientin und ihrem digitalen Zwilling die Frage, inwieweit es der Patientin möglich sein wird, selbständig zu entscheiden, was gut oder schlecht für sie ist respektive inwieweit sie vom digitalen Zwilling bevormundet wird.[130] Schließlich ist auch zu fragen, inwiefern es den Anbietern von digitalen Zwillingen möglich wäre, die Patienten mithilfe des digitalen Zwillings zu überwachen oder gar paternalistisch zu bevormunden. Möglicherweise könnten Akteure des Gesundheitswesens zudem gesellschaftlichen Druck auf Patienten ausüben, einen solchen digitalen Zwilling zu haben und bereitzustellen.

Das Versprechen an den einzelnen Patienten, dank des digitalen Zwillings mehr persönliche Freiheit im Umgang mit den eigenen biologischen Gegebenheiten zu erlangen, erscheint damit in Teilen trügerisch angesichts eines digitalen Zwillings, der infolge seiner Vorhersagekraft und seiner bidirektionalen Ausgestaltung zwischen der Ermöglichung neuer Freiheiten und der Beeinträchtigung von Freiheit oszilliert.[131] Vor diesem Hintergrund ist es zentral, dass die Patienten ein angemessenes Verhältnis zu ihrem digitalen Zwilling unterhalten und die Fähigkeit entwickeln, angesichts star-

127 Sharon 2017, S. 98.
128 Bagaria u.a. 2020, S. 150.
129 Tretter 2021, S. 410.
130 Bruynseels/Santoni de Sio/van den Hoven 2018, S. 9.
131 Vgl. Braun 2022, S. 217.

ker datengesteuerter personalisierter Modelle fundierte Entscheidungen zu treffen.[132]

Mittels Datenkörper wird also Gesundheit zur quantifizierbaren Zielvorgabe und damit Gesundheitsverhalten zur Optimierungspraxis.[133] Denn: »Ist das menschliche Leben erst einmal in Zahlen übersetzt, lässt es sich auch durchoptimieren.«[134] Zudem wird der analoge Körper durch den Datenkörper anfälliger für den »regulierenden Blick von außen«[135] und damit potentiell zu einem operativen Werkzeug des Kontroll- und Überwachungsgefüges.[136]

Es könnte indes noch weiter gehen: Der soeben als Instrument des Kontroll- und Überwachungsgefüges beschriebene Datenkörper könnte selbst zum Gegenstand eben dieses Gefüges werden. Denn die Zerlegung des analogen Körpers in einzelne Datenpunkte, die dann wiederum zum Datenkörper zusammengefügt werden, bedeutet nicht nur die Auflösung der äußerlichen Schutzhülle des physischen Körpers,[137] vielmehr wird dieser entkörperlichte Körper zu einer eigentlichen »surveillant assemblage«.[138] In den Worten *Beckers*: »Es gibt irgendwann keine Möglichkeit mehr, außerhalb seiner digitalen Repräsentationen zu leben. Man ist gefangen in seinem Datenkörper. In der Disziplinargesellschaft war der unterworfene Körper immer noch eine Trutzburg, aus der intime Informationen (etwa Gedanken oder Krankheiten) nicht ohne Weiteres nach außen drangen.«[139]

Kurzum: Nicht nur der physische Körper lässt sich durch den Datenkörper disziplinieren, vielmehr lässt sich auch der Datenkörper selbst steuern. »Der Datenkörper lässt sich als numerische Repräsentation des physischen Körpers formatieren, archivieren, arretieren, traktieren und kontrollieren […].«[140] Die »Daseinsform« des Datenkörpers als reine Virtualität bedeutet zudem, dass ein Zugriff potenziell anlasslos, ohne Vorwarnung und ohne Berührung passieren kann.[141] *Becker* stellt fest: »Macht kann direkt, unter Ausschaltung demokratischer Entscheidungsverfahren, ausgeübt werden,

132 Bruynseels/Santoni de Sio/van den Hoven 2018, S. 9.
133 Wieser 2019, S. 444.
134 Ebd.
135 Wiedemann 2022, S. 84.
136 Vgl. Wiedemann 2022, S. 83.
137 Lobe, S. 137.
138 Vgl. Haggert/Ericson 2000, S. 611 f.
139 Lobe, S. 103 f.
140 Ebd., S. 137.
141 Ebd.

indem man sich Datenkörper aneignet. Dieses totalitäre Potenzial, das der Datenkörper möglichen Nutzern in die Hand legt, macht ihn zu einem problematischen Phänomen, das ein anderes Verständnis von Daten erforderlich macht: nämlich als soziale Konstruktion und nicht als Abbild einer objektiven Realität. Wie Datenkörper angelegt werden, was mit ihnen geschieht und wer sie kontrolliert ist daher eine brisante politische Frage.«[142]

Obwohl diese Aspekte schon brisant sind, könnte sich die Problematik noch zuspitzen: Im Rahmen der Diskussion der Beziehung von digitalem und analogem Zwilling wird insbesondere der Aspekt diskutiert, inwiefern und inwieweit der digitale Zwilling zum Stellvertreter seines analogen Gegenübers wird.[143] Während manche Autoren danach fragen, wie genau, wenn überhaupt, digitale Zwillinge im Namen von Patienten »handeln« können und ob wirklich das Risiko besteht, dass Patienten durch ihren Zwilling ersetzt werden,[144] interessiert andere, welche problematischen Aspekte mit einer Stellvertretung durch den digitalen Zwilling einhergehen könnten.[145] Dabei gilt es zunächst festzustellen, dass die Stellvertretung i.S. der Substitution im medizinischen Kontext nicht unbekannt ist.[146] Der Grundgedanke ist, dass die vertretende Person als eine Art Surrogat im Namen der vertretenen Person handelt. Während es in diesem bekannten Kontext bereits zu einer Dynamik kommen kann, die im Endeffekt bedeutet, dass die Substitution keine Repräsentation mehr ist,[147] verschärft sich diese beim digitalen Zwilling: Indem der digitale Zwilling die physische Einheit repräsentiert, verleiht er dieser eine gewisse Präsenz im digitalen Raum, wo die physische Einheit selbst zwangsläufig nicht existiert.[148] Der digitale Zwilling fungiert also als Substitut. Der Datenkörper gibt sich als die physische Entität aus und wird als solche behandelt. D.h. ein technisches Artefakt wird als die Realität einer physischen Entität behandelt, und die Materialität des menschlichen Körpers als Grundlage der medizinischen Entscheidung wird verdrängt.[149] Mit anderen Worten bedeutet das, dass körperliche und nicht-körperliche Vorgänge als gegeneinander austauschbare kommunika-

142 Becker 2003, S. 197.
143 Braun 2021, S. 396.
144 Tigard 2021, S. 407.
145 Braun 2022, S. 217; Korenhof/Blok/Kloppenburg 2021, S. 1763 f.
146 Braun 2022, S. 217.
147 Ebd.
148 Korenhof/Blok/Kloppenburg 2021, S. 1763 f.
149 Haidar u.a. 2023, S. 82.

tive Prozesse betrachtet werden.[150] Gleichzeitig ist die physische Entität von ihrem digitalen Substitut abhängig, denn dieses ist die Repräsentation, auf der die Entscheidungen zur Steuerung der physischen Entität beruhen.[151]

Indem der digitale Zwilling die Patientin in bestimmten Kontexten und Praktiken ersetzt, dürfte er die Beziehung zwischen verschiedenen Akteuren des Gesundheitswesens und der Patientin beeinflussen: Wie bereits festgestellt, ermöglicht die Daseinsform des Datenkörpers einen jederzeitigen und ortsunabhängigen Zugriff auf diesen, um so Aspekte der physischen Entität zu überwachen, zu diagnostizieren und vorherzusagen. Diese Interaktion wird immer mit dem Datenkörper und nicht mit der realen Patientin stattfinden. Je mehr ein digitaler Zwilling zum primären Fokus der Akteure wird, desto mehr kann die Aufmerksamkeit der Akteure für die Patientin abnehmen oder zeitlich eingeschränkt werden.[152] Dies könnte zu einem Rollenwechsel führen, bei dem das Substitut zum Hauptobjekt des Interesses der Akteure wird, während die physische Entität funktionell zu einer Ergänzung des Substituts wird.[153] Allenfalls könnte es so weit gehen, dass der digitale Zwilling als zuverlässigste Quelle bezüglich des Gesundheitszustands der Patientin betrachtet wird.[154] Ob dieser Umstand dem Bild eines menschlichen Gesundheitswesens, wie es *Topol* vor Augen hat, (noch) entspricht, erscheint fraglich.

Bevor auf die möglichen rechtlichen Konsequenzen angesichts dieser Umstände einzugehen ist, ist zunächst noch eine weitere Beobachtung einzubeziehen, die die ohnehin schon brisante Mensch-Maschine-Beziehung noch prekärer erscheinen lässt.

3. Überschreitung des Humanen – Der digitale Zwilling ist mehr als ein Zwilling

Der Begriff »Zwilling« suggeriert eine Gleichheit zwischen der physischen und der virtuellen Entität dahingehend, dass die digitale dieselben Eigenschaften wie die physische Entität aufweist und sich zur physischen Entität

150 Gruber 2015, S. 22.
151 Korenhof/Blok/Kloppenburg 2021, S. 1761 f.
152 Haidar u.a. 2023, S. 82.
153 Korenhof/Blok/Kloppenburg 2021, S. 1762 f.
154 Chiodo 2023, S. 171 f.

geradezu wie ein Äquivalent verhält.[155] Aber haben wir es tatsächlich mit einem solchen Zwilling zu tun?

Zunächst ist zu bedenken, dass der digitale Zwilling die Fähigkeit zur Vorhersage über zukünftige Gesundheits- oder Krankheitszustände hat, also ständig mögliche zukünftige Zustände des analogen Gegenübers entwirft. Sieht sich der analoge Patient dann nicht vielmehr mit seinem »zukünftigen Ich« konfrontiert? Einem ihm vorauseilenden Datenkörper?[156]

Des Weiteren befindet sich der Datenkörper im virtuellen Raum; er hat keinen wirklichen Aufenthaltsort und ist zeitunabhängig. In den Worten von *Matthias Braun*: »In dem Moment und an dem Ort, an dem ein digitaler Zwilling für die Person (oder besser: ihren Körper) einspringt und damit ihren Platz einnimmt, ist der digitale Zwilling nicht nur dort, wo die andere Person war oder in der Zukunft sein wird, sondern zugleich an der Stelle, wo sich der simulierte physische Körper gerade befindet.«[157] Damit ist er weniger Einschränkungen unterworfen als sein menschliches Gegenüber.[158] Dies ermöglicht es ihm auch, sich mit anderen virtuellen Entitäten zu verknüpfen, etwa mit ihnen ein »Internet of Digital Twins« zu bilden.[159] Wie aufgezeigt, lassen sich Datenkörper zudem kopieren, etwa um Arzneimittel auf ihre Wirksamkeit hin zu überprüfen, ohne dabei Gefahr zu laufen, damit die Testperson zu erschöpfen.[160]

Ferner – insoweit aber wieder näher am analogen Gegenüber – bietet der digitale Zwilling seinem Gegenüber die Möglichkeit der Externalisierung seiner kognitiven Fähigkeiten, etwa dadurch, dass dieser Speicherkapazitäten zur Verfügung stellt, quasi ein externes Gedächtnis, welches die Möglichkeiten des menschlichen übersteigt.[161] Der digitale Zwilling vermag insoweit als funktionaler Bestandteil des menschlichen Körpers und Geistes zu wirken und diese über die physischen Hautgrenzen hinaus zu erweitern.[162]

Schließlich gilt es zu bedenken, dass der Datenkörper in seiner kommunikativen Dimension als semantisches Artefakt im Gegensatz zu seinem

155 Korenhof/Blok/Kloppenburg 2021, S. 1768; vgl. Lupton 2021, S. 409.
156 Vgl. Stalder 2002, S. 120.
157 Braun 2022, S. 217.
158 Vgl. Becker 2003, S. 196.
159 Von einem Internet of Digital Twins sprechen Wang u.a. 2023, S. 1.
160 Kamel/Maged/Zhang 2021, S. 3.
161 Wiedemann 2022, S. 84.
162 Kerckhove 2021, S. 7.

analogen Gegenüber unsterblich ist.[163] Die Unsterblichkeit des digitalen Zwillings wird von *Sahal, Alsamhi und Brown* als positiver Aspekt hervorgehoben, denn aus ihrer Sicht könnten digitale Zwillinge dazu dienen, die Daten i.S. eines digitalen Nachlasses eines Verstorbenen zu bewahren und darüber hinaus (in Kombination mit Natural Language Processing Technologien) als Quelle für Erzählungen über den Verstorbenen fungieren.[164] Sie sehen im digitalen Zwilling einen Datenspeicher für die »menschliche Ewigkeit durch Daten«.[165] Für Lobe markiert die Unsterblichkeit des Datenkörpers indes die Geburt einer neuen Biopolitik, die nicht mehr Körper, sondern Datenkörper – respektive Körperdaten – regiert.[166]

Digitale Zwillinge überschreiten ihre Repräsentationsfunktion allerdings nicht nur, indem sie »mehr«, sondern auch anders als die analogen Körper sind: Damit es zu einer virtuellen Verdoppelung des analogen Körpers kommen kann, muss dieser Körper wohl zunächst datafiziert werden, d.h. er muss zunächst technisch verfügbar gemacht und funktionalisiert werden. Angesichts dessen, dass Quantifizierung und Digitalisierung in sich selbst reduktionistische Prozesse sind[167] und insbesondere Lebewesen und Systeme kaum vollständig zu modellieren sind,[168] fehlt es dem digitalen Zwilling an Ganzheit. Mit anderen Worten: Der digitale Zwilling wäre demzufolge gar kein Zwilling.[169] Aber was wäre er dann? Ein anderes Ich? Ein besseres Ich? Ein zukünftiges Ich?[170] Haben wir es hier mit einer Form von Transhumanismus zu tun, oder beschreiten wir mit dem digitalen Zwilling ein Zeitalter des »Exo-Humanismus«?[171]

Rubeis bedient sich des Begriffs »Simulacra«, um den digitalen Zwilling zu beschreiben, dies mit dem Argument, dass die Bidirektionalität der digitalen Zwillinge dem von *Baudrillard* beschriebenen operativen Charakter der Simulacra entspräche.[172] Digitale Zwillinge seien hyperreal, da sie das

163 Vgl. Krüger 2019. S. 70: »Das Vergleichsmoment zwischen dem Menschen und der virtuellen Simulation des Menschen ist zunächst seine Sterblichkeit und die vermeintliche Unsterblichkeit seiner medialen Simulation.«
164 Sahal/Alsamhi/Brown 2022, S. 13.
165 Ebd.: »Therefore, the PDTs will be the data lake for human eternity through data.«
166 Lobe, S. 140.
167 Vgl. Sharon 2017, S. 105; vgl. Haidar u.a. 2023, S. 83.
168 Korenhof/Blok/Kloppenburg 2021, S. 1760.
169 Ebd., S. 1768.
170 Teller 2021, S. 2.
171 Ebd.
172 Rubeis 2023, S. 203.

Reale nicht nur abbilden, sondern transformieren. Die operative Logik der Simulation bestimme das Simulakrum. Nach *Rubeis* repräsentiert ein Simulakrum nicht nur das physische Objekt, sondern ist in gewisser Weise realer als dieses Objekt.[173] Aber dennoch könne es die notwendige Referenz auf den Bereich des Physischen nicht ersetzen.

Als produktiver könnten sich die – indes nicht auf den digitalen Zwilling per se bezogenen – Überlegungen von *Deborah Lupton* erweisen, wonach wir damit beginnen könnten, unsere »digital data assemblages« als Begleiter zu betrachten, die ein Eigenleben führen, das sich unserer vollständigen Kontrolle entzieht.[174] »Digital data assemblages« sind dabei gemäß *Lupton* in mehrfacher Hinsicht lebendig: Sie handeln vom (menschlichen) Leben selbst; sie scheinen einem steten Wandel zu unterliegen, zumal sie ständig generiert und regeneriert sowie zweckgebunden und umgewidmet werden; sie haben potenzielle Auswirkungen auf das Leben von Menschen und schließlich trägt ihr kommerzieller und wissenschaftlicher Wert zum Lebensunterhalt bei.[175] In diesem Sinne stellt *Teller* fest: »Indeed, the digital twin refers as much to the idea of person as to the idea of possession: this twin is as much a replication of the person as it is a ›putting into data of the person‹ with a patrimonial dimension. *The twin is the person but the person has his twin*«.[176]

Dies führt zur Frage, an welcher Stelle die Person endet und wo die virtuelle Entität beginnt. Oder haben wir es mit einer Art digitalem Unbewusstem auf halbem Weg zwischen der Person und dem Ding zu tun,[177] einem Mischwesen, das sich nicht mehr trennscharf in menschliches Subjekt und technisches Objekt aufgliedern lässt?[178] Einem Quasi-Objekt?[179] Wird die traditionelle Subjekt-Objekt-Dichotomie dieser Existenzform noch gerecht oder muss das Verhältnis von Subjekt und Objekt neu gedacht werden?

---

173 Ebd.; Auch Haidar u.a. 2023 setzen sich mit dem Begriff auseinander bzw. benutzen ihn, um sich der Problematik des digitalen Zwillings zu nähern. »Baudrillard's concepts of simulacrum and integral reality provide a valuable framework for anticipating the implications of ongoing digitization in biomedical research. Integral reality arises when the ›reality‹ of the sign becomes independent and equally significant as the signified.« S. 83.

174 Lupton 2016, S. 3.

175 Ebd., S. 2.

176 Teller 2021, S. 2 [Hervorhebungen hinzugefügt].

177 Ebd., S. 5.

178 Wieser 2019, S. 445.

179 Gruber 2015, S. 232.

Angesichts dessen, dass ein digitaler Zwilling eine bidirektionale Interaktionsbeziehung mit seinem physischen Gegenüber entfaltet und damit dessen Körperverfassung fortdauernd modelliert, wie er auch selbst modelliert wird, wirkt sich das womöglich auf seinen rechtlichen Status aus. Seine aktive, »körpergestaltende« Rolle lässt ihn insoweit nämlich als Datenkörper mit einer eigenen Wirkmacht, in diesem Sinne mit eigener »agency« erscheinen. Auf diese Weise bilden sich in diesem ohnehin schon komplexen Zusammenhang neuartige semantische Artefakte heraus, die über das Potential neuartiger Datensubjekte verfügen.

Der digitale Zwilling als Datenkörper zeitigt damit nicht nur Implikationen für sein menschliches Gegenüber. Vielmehr erwachsen aus dem »wechselseitigen Aufeinander-Bezogen-Sein und In-Beziehung-Stehen«[180] ganz grundsätzliche Fragen danach, was unter einer Person zu verstehen ist.

4. Zur Notwendigkeit der Humanisierung durch (Daten-)Recht

Die vorhergehenden Ausführungen haben gezeigt, dass der digitale Zwilling das Potential hat, das Gesundheitswesen nicht humaner zu machen – entgegen seinen ursprünglichen Versprechungen. Umso wichtiger erscheint es daher, den möglichen Beitrag des Rechts zu einer »humanen« Implementierung von KI in der Medizin herauszuarbeiten, um befürchtete Fehlentwicklungen einer datengetriebenen Gesundheitswirtschaft zu hemmen.

In Anbetracht der Beobachtung, dass es sich beim digitalen Zwilling um eine biopolitische Steuerungstechnik handelt, deren Interventionen allenfalls sogar direkt durch die Haut-Grenzen hindurch, jedenfalls aber indirekt durch darauf basierende Entscheidungen zu (medizinischen) Eingriffen auf die menschliche Physis wirken, ist es zentral, die Modalitäten des Einsatzes des digitalen Zwillings zu regulieren respektive die Ausgestaltung der Beziehung zwischen Mensch und Maschine, insbesondere deren Grenzen, zu bestimmen.

Unter anderem sind etwa folgende Fragen zu beantworten: Wo »befindet« sich der digitale Zwilling? Wem »gehört« er? Wer hat Kontrolle über ihn? Wer kann auf ihn zugreifen? Was sind geeignete Mechanismen zur Erteilung der dafür notwendigen Zustimmung? Wer ist verantwortlich für Entschei-

180 Wiedemann 2022, S. 82.

dungen, die auf der Grundlage des digitalen Zwillings getroffen werden? Hat der Mensch, auf dem ein digitaler Zwilling basiert, das Recht, die Verarbeitung bestimmter Daten oder die Erstellung von Prognosen zu verweigern? Kann ein Patient die von seinem digitalen Zwilling getroffenen Entscheidungen ignorieren, übersteuern oder ändern?[181] Was passiert mit dem digitalen Zwilling, wenn der Patient stirbt? Auch Aspekte der Transparenz, der Datengenauigkeit, möglicher Verzerrungen sowie die Frage nach Vertrauen sind angesichts des (Macht-)Verhältnisses zwischen Mensch und Maschine relevant.[182]

Der digitale Zwilling bewegt sich indes nicht in einem rechtsfreien Raum und es kann durchaus argumentiert werden, dass das bestehende Rechtssystem, insbesondere das europäische Datenrecht, bereits über Mechanismen verfügt, um dem problematischen Potential des digitalen Zwillings zu begegnen.[183] Indes – und wie sich nachfolgend in Grundzügen zeigen wird – scheinen bislang viele Aspekte ungeklärt.[184] Angesichts der Skalierbarkeit des digitalen Zwillings potenzieren sich zudem die bisherigen mit Selbstvermessungstechniken verbundenen Herausforderungen.[185] Gleichzeitig und erschwerend kommt hinzu, dass der digitale Zwilling das Potential hat, zahlreiche strukturierende Begriffe des Rechts – allen voran die Konzepte der Rechtssubjekts, des Rechtsobjekts und der personalen Verantwortungszurechnung – in Frage zu stellen.[186]

Ähnlich seiner Aufgabe in der Medizin kann der digitale Zwilling damit auch dem Recht als Untersuchungsgegenstand dienen, um zu fragen, ob es angesichts der Eigenheiten des digitalen Zwillings vielleicht an der Zeit ist, bestimmte Rechte oder Rechtskonzepte zu aktualisieren oder zu überdenken.[187] Der digitale Zwilling wirft also nicht nur rechtliche Fragen auf, sondern er stellt auch das Recht selbst in Frage.[188]

181 Maeyer/Markopoulos 2020, S. 9; Cho/Martinez-Martin 2023, S. 48; Haidar u.a. 2023, S. 83.
182 Korenhof/Blok/Kloppenburg 2021, S. 1766 f.
183 Teller 2021, S. 6.
184 Vgl. Cho/Martinez-Martin 2023, S. 48.
185 Vgl. Haidar u.a. 2023, S. 83.
186 Teller 2021, S. 1.
187 Ebd., S. 2.
188 So auch Teller 2021, S. 2.

IV. Datenkörper und Datenrecht

Die Herausforderung des Rechts besteht also darin, mit den neuen Gemengen und Gemischen von technisierten Körpern, verkörperter Technik und anderen Quasi-Objekten rechtlich umzugehen.[189] In dieser Hinsicht hat das Recht – selbst beobachtbar als eine Technik der (Re-)Humanisierung von Technik – seine Schutzwirkungen auf menschliche Individuen anzupassen und angesichts der neuen Herausforderungen über die individualistische Orientierung an engagiertem Bewusstsein und kommunikativer Kompetenz hinauszugehen.[190]

Diesbezüglich ist also zu fragen, ob es nicht angezeigt wäre, den digitalen Zwilling als Datenperson oder Datensubjekt zu behandeln, zumal ein zweiter Datenkörper zur spät- oder nachmodernen Natur des Menschen werden könnte[191] und damit Datenschutz tatsächlich »Personenschutz« bedeutet.[192]

Die Frage nach einer möglichen Subjektqualität des digitalen Zwillings bedarf dabei einer Verständigung darüber, wann sich diese Frage überhaupt stellt. Wie nachfolgend zu zeigen sein wird, geht der vorliegende Beitrag davon aus, dass dies unter anderem abhängig davon ist, inwieweit (ab welchem Zeitpunkt und unter welchen Voraussetzungen) der digitale Zwilling von seiner physischen »Trägerperson« ablösbar ist und einen eigenständigen, in diesem Sinne doch autonomen Existenzmodus eines digitalen Subjekts entwickelt. Eine wichtige Rolle wird dabei freilich die zeitliche Komponente spielen, vor allem die Frage, ob der physische Datengeber zum Zeitpunkt der Datenverarbeitung noch lebt oder allenfalls noch im Rahmen einer persönlichkeitsrechtlichen Nachwirkung »postmortal« schutzwürdig erscheint.

Bevor auf diese Frage noch einzugehen ist, soll zunächst eruiert werden, wie der digitale Zwilling gegenwärtig reguliert wird. Vor dem Hintergrund, und insofern vorgreifend, dass Daten quasi das »Lebenselixier« des digitalen Zwillings bilden, liegt der Fokus der nachfolgenden Ausführungen auf dem Datenschutzrecht. Dies scheint naheliegend, ist insofern aber allenfalls nachteilig, berücksichtigt man die Beobachtung von *Irma van der Ploeg*: »In the case of the body-as-information, the problem is that we have very differ-

189 Gruber 2015, S. 108.
190 Vgl. Gruber 2015, S. 7.
191 Wiedemann 2022, S. 80, mit weiterem Verweis auf Borck 2016, S. 121.
192 Vgl. Becker 2003, S. 195.

ent regimes for protecting bodies and for protecting information from unjustified access and intrusion, however »personal« that information may be. Whereas in the first case the very integrity of the body and issues of self determination are at stake, in the second, the far weaker concepts of informational privacy and personal data protection apply.«[193] Ergo bedeutet die Entgrenzung von Körper und Information das Verschwimmen des rechtlichen Status des Subjekts.[194]

1. Datenkörper im Datenrecht

Der digitale Zwilling ist ein technologisches Mischwesen.[195] Sein Kernstück sind zwar Daten, Algorithmen und KI-Systeme und entsprechend ist der rechtliche Rahmen dieser Elemente zentral.[196] Dabei darf aber nicht vergessen werden, dass, wie *Wiedemann* zu bedenken gibt, der Datenkörper einer gewissen »Körperpflege« bedarf, denn er ist nicht nur mit der Generierung und Analyse von Daten beschäftigt, vielmehr müssen auch »die Technologien umsorgt werden, indem sie aufgeladen, kalibriert, upgedatet oder gewartet werden.«[197]

Wem diese »Körperpflege« obliegt, ist indes ungeklärt. Angesichts des Umstands, dass es die großen privaten Technologieunternehmen sind, die digitale Zwillinge entwickeln, ist es ohnehin fraglich, inwiefern Zugang zu den zu umsorgenden Technologien überhaupt möglich wäre, zumal etwa der Code für die Algorithmen von diesen privaten Unternehmen unter Verschluss gehalten werden dürfte.[198]

Der fehlende Zugang zu den Machine-Learning-Modellen bedeutet auch, dass sie einer Überprüfung auf mögliche Verzerrungen nicht zugänglich sind. Ferner sind Transparenz, Erklärbarkeit und Fairness von Algorithmen zentral für das Vertrauen der Menschen in die Modelle und deren Entwickler.[199]

193 van der Ploeg 2012, S. 18.
194 Vgl. Kämpf 2022, S. 60.
195 Vgl. Popa u.a. 2021, S. 3.
196 Teller 2021, S. 2.
197 Wiedemann 2022, S. 88.
198 Vgl. Geneux 2021.
199 Vgl. Korenhof/Blok/Kloppenburg 2021, S. 1766 f.

Die Opazität der Modelle ist umso problematischer, als dass digitale Zwillinge so konzipiert sind, dass sie schwerwiegende gesundheitliche Ereignisse vorhersagen und in einem frühen Stadium weitreichende Interventionen empfehlen können.[200] Angesichts dieser großen Risiken sind Datenqualität und Modellgenauigkeit elementar.[201] Ebenso ist es wichtig sicherzustellen, dass die Diagnose auf den Daten des richtigen digitalen Zwillings beruhen.[202] Entsprechend sind beim Einsatz des digitalen Zwillings zudem Verantwortungs- und Haftungsfragen zentral, wobei sich die Verantwortung auf einer »sliding scale« zwischen dem Hersteller, der Akteure im Gesundheitswesen und dem Patienten bewegt.[203]

Rechte- und Verantwortungszuschreibungen sind also uneindeutig. Einen für den Fortgang der rechtlichen Betrachtung des digitalen Zwillings als einigermaßen »sicher« zu unterstellenden rechtlichen Anhaltspunkt scheint indes das Datenrecht respektive der Datenschutz zu geben. Denn klar dürfte sein, dass der digitale Zwilling »digital« in dem Sinn ist, dass er jedenfalls durch digitale Datenverarbeitung entsteht und bestehen bleibt.[204] Daten sind demnach gleichsam das »Lebenselixier« des digitalen Zwillings.

Der Datenschutz dürfte damit ein Schlüsselinstrument sein, um einigen der potenziell negativen Auswirkungen des digitalen Zwillings zu begegnen.[205] Zugleich bildet der Datenschutz eine der größten Herausforderungen, mit denen digitale Zwillinge konfrontiert sind: die Erfassung, Analyse und Speicherung derart großer Mengen von (meist sensiblen) Daten über lange Zeit werfen erhebliche Bedenken hinsichtlich der Einhaltung des Datenschutzes auf und erhöhen das Risiko von Datenschutzverletzungen.[206]

Wie bereits festgestellt, agiert der digitale Zwilling in keinem rechtsfreien Raum. Unter anderem die Datenschutzgrundverordnung (DSGVO)[207] findet angesichts der mit dem digitalen Zwilling verbundenen Verarbeitung personenbezogener Daten Anwendung.[208] Der DSGVO kann sich der digitale Zwilling auch nicht entziehen, indem etwa versucht wird, die Daten zu anonymisieren und so den digitalen Zwilling aus dem Anwendungsbe-

200 Mittelstadt 2021, S. 405.
201 Ebd.
202 Popa u.a. 2021, S. 16.
203 Iqbal/Krauthammer/Biller-Andorno 2022, S. 590 ff.
204 Vgl. Korenhof/Blok/Kloppenburg 2021, S. 1755.
205 Bruynseels/Santoni de Sio/van den Hoven 2018, S. 8.
206 Armeni u.a. 2023, S. 6.
207 Europäische Kommission 2016.
208 Ebenso Teller 2021, S. 3; Geneux 2021.

reich der DSGVO herauszuholen. Es ist gerade der Personenbezug, der den Datenkörper für den medizinischen Einsatz wertvoll macht.

Vor dem Hintergrund der Vision, dass der digitale Zwilling eine »*life cycle healthcare*«[209] für den Patienten leisten soll und sich den Aspekt des »Lebendigen« des digitalen Zwillings in Erinnerung rufend, soll nachfolgend anhand des »Lebenszyklus« des digitalen Zwillings sowie seines menschlichen Gegenübers aufgezeigt werden, wo sich (datenschutz-)rechtlich relevante Probleme ergeben könnten. Es geht dabei weniger darum, diese Probleme zu lösen, sondern vielmehr darum, die verschiedenen Herausforderungen herauszuarbeiten und aufzufächern, damit diese der Debatte zugeführt werden können. Wir folgen hierzu dem Dreiklang eines »Werden/Zusammensetzung«, »Seins/Verschränkung« und »Vergehens/Entkopplung« des digitalen Zwillings respektive der damit einhergehenden Mensch-Maschinen-Beziehung. Auch wenn diese einzelnen Stadien nicht trennscharf zu unterscheiden sind, erweisen sie sich dennoch als hilfreich, um mögliche Herausforderungen nicht nur zu identifizieren, sondern auch zu verorten, zumal nicht jede Frage mit der gleichen Dringlichkeit und nicht alle Akteure mit der gleichen Relevanz auftreten, sondern vom jeweiligen Stadium sowohl des digitalen Zwillings als auch seines physischen Gegenübers abhängen. So verlangen etwa im Stadium der menschlich-maschinellen Verschränkung zwischen digitalem und analogem Zwilling andere Akteure Zugang zum Datenkörper, als dies bei dessen Entkopplung von seinem analogen Gegenüber der Fall ist. Die Zugangsfragen beschränken sich jedoch nicht nur auf den Datenkörper, vielmehr geht es auch um Fragen des Zugangs zu Körperdaten, um diesen Datenkörper zu formieren, respektive »am Leben zu erhalten«.

Eine Fragestellung ist indes derart zentral, dass sie nicht in dem nachfolgenden Dreiklang aufgeschlüsselt wird, sondern direkt hier zur Sprache kommen soll: Womit haben wir es aus Perspektive der DSGVO mit dem digitalen Zwilling eigentlich zu tun?

Zunächst scheint es, als vermöge Art. 4 Ziff. 4 DSGVO den digitalen Zwilling datenschutzrechtlich zu fassen.[210] Art. 4 Ziff. 4 versteht unter Profiling

209 Hassani/Huang/MacFeely 2022, S. 7.

210 Petri 2020 scheint diese Beobachtung zu teilen, wenn er schreibt: »Das Sammeln, Ordnen und Analysieren von persönlichen Daten erzeugt Bilder von der betroffenen Person. Bei zahlreichen Anwendungen liegt es sogar nahe, dass die jeweilige Verarbeitung von Gesundheitsdaten etwa im Rahmen der Gesundheitsversorgung oder im kommerziell geprägten Wellness- oder Fitnessbereich primär darauf abzielt, Aspekte der physischen, psychischen, physiologischen oder genetischen Identität einer natürlichen Person abzubilden. Das Datenschutzrecht bezeichnet ei-

»jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen.«

Aber so einfach ist es nicht: In ihrer Untersuchung zum Profiling stellt *Lorentz* fest, dass die Erhebung, Sammlung und Speicherung von Daten keine Verarbeitungsschritte sind, die unter die ProfilingDefinition des Art. 4 Ziff. 4 DSGVO fallen, denn die personenbezogenen Daten werden zwar automatisiert verarbeitet, sie werden jedoch nicht für die Bewertung von persönlichen Aspekten »verwendet«. Ferner liegt in der Datenerhebung keine Bewertung, Analyse oder Vorhersage der genannten Persönlichkeitsaspekte. Die gesammelten Daten ermöglichen zwar im Rahmen ihrer weiteren Verarbeitung eine Bewertung, Analyse oder Vorhersage von Persönlichkeitsaspekten, die Bewertung liegt aber nicht bereits in den erhobenen und gesammelten Daten selbst. Dies ist ebenfalls der Fall bei der Datenspeicherung.[211]

In Anbetracht dessen ist anzunehmen, dass die Erhebung, Sammlung und Speicherung von Daten für die Formierung und den Betrieb des digitalen Zwillings nicht von Art. 4 Ziff. 4 DSGVO erfasst werden. Einzig die Analyse und die Prädiktion, die anhand dieser Daten erfolgen, lassen sich unter die Profiling-Definition subsumieren. Die unterschiedlichen konstitutiven Vorgänge des digitalen Zwillings werden also vom Datenschutzrecht allenfalls fragmentarisch adressiert. Damit dürfte auch das wechselseitige »Aufeinander-Bezogen-Sein und In-Beziehung-Stehen«[212] des digitalen Zwillings sowie seines Gegenübers kaum adäquat begriffen sein.

1.1 Werden – Zusammensetzung

Wie soeben erwähnt, bedarf es für die Formierung des digitalen Zwillings der Erhebung, Sammlung und Speicherung von Daten. In diesem Stadium

---

nen solchen Prozess der Erstellung eines solchen Datendoubles als »Profiling«, ihr Ergebnis als »Persönlichkeitsprofil«. Ausgangspunkt für die Erzeugung derartiger Profile ist der Versuch, ein Individuum unter bestimmten Aspekten einordnen und bewerten zu können.« S. 43.

211 Lorentz 2020, S. 139.

212 Wiedemann 2022, S. 82.

präsentieren sich weniger Fragen nach der Beziehung zwischen Mensch und Maschine, sondern vielmehr Fragen nach dem Zugang zu den Körperdaten, aus denen sich der Datenkörper konstituieren kann.

Damit der Datenkörper den komplexen analogen Körper möglichst akkurat und damit nützlich abbilden kann, bedarf es der Erfassung möglichst großer Mengen von vielfältigen multimodalen Daten.[213] Je mehr Daten die prädiktiven Berechnungsmodelle haben, desto genauer sind ihre Vorhersagen.[214]

Die Daten[215] können aus elektronischen Gesundheitsakten, klinischen Daten wie Bildgebungs- und Labortestergebnissen, genomischen Daten und anderen Arten von Forschungsdaten wie Biomarkern, Stoffwechsel- und Bildgebungsdaten sowie einer Vielzahl von persönlichen Daten und Sensordaten stammen.[216] Dabei geht es auch um die Übersetzung des analogen Körpers in die digitale Repräsentation.[217] Entsprechend liegt der Formierung des digitalen Zwilling ein Prozess der »Datafizierung« zugrunde.[218] Ferner kommt es zu Interpretations- und Auswahlprozessen, etwa wenn es darum geht, zu entscheiden, welche Daten eines Datenbestandes als relevant erachtet werden.[219]

Der Akteur, der in diese Prozesse involviert ist, scheint unterschiedlich sein zu können.[220] Wohl werden es Technologieunternehmen des privaten Wirtschaftssektors oder aber »hybride Akteure« sein. Unter dem Gesichtspunkt, dass der Auswahlprozess der Daten nicht neutral ist und zu einem »verzerrten« Zwilling führen kann,[221] ist dies bedenklich.

Je nach Akteur wird sich zudem die Möglichkeit des Zugangs zu Daten unterscheiden. Nebst den großen Datenmengen, die Technologieunterneh-

213 Acosta u.a. 2022, S. 1776.

214 Geneux 2021.

215 Sahal/Alsamhi/Brown 2022, S. 17 unterscheiden bei den gesammelten Daten zweierlei: historische Daten und Echtzeitdaten. Die historischen Daten werden aus den medizinischen Aufzeichnungen gesammelt. Die Echtzeitdaten werden von Sensoren (bspw. angeschlossenen medizinischen Geräten) erfasst.

216 Cho/Martinez-Martin 2023, S. 45.

217 Blok 2023, S. 20.

218 Korenhof u.a. 2023, S. 2.

219 Blok 2023, S. 20.

220 Falls auch der Patient involviert ist, dann könnte er sich allenfalls seines Rechts auf Datenportabilität gemäß Art. 20 DSGVO bedienen, um Daten, die er einem Verantwortlichen bereitgestellt hat, zu erhalten und an den für die Entwicklung des digitalen Zwillings Verantwortlichen zu übermitteln.

221 Blok 2023, S. 20.

men des privaten Wirtschaftssektors bereits zur Verfügung stehen, haben diese auch die entsprechenden finanziellen Mittel, um Daten zu produzieren oder Zugang zu ihnen zu erhalten – im Unterschied zu den begrenzten Budgets von Universitäten und öffentlichen Forschungseinrichtungen.[222] Die Formierung des digitalen Zwillings findet sich damit eingebunden in ein Ringen darum, wer ausreichenden Zugang zu Daten und Daten produzierenden Technologien hat.[223]

In jedem Fall bedarf es bei der Erhebung und Sammlung personenbezogener Daten der Einwilligung des Patienten.[224] Dabei wird wohl in der Regel eine ausdrückliche Einwilligung nötig sein, zumal es sich bei den meisten Daten um Gesundheitsdaten handeln wird (vgl. Art. 9 Abs. 2 lit. a DSGVO). Die DSGVO verlangt unter anderem, dass die Einwilligung informiert und freiwillig erfolgt (vgl. Art. 4 Nr. 11 DSGVO). Ob dies vorliegend gegeben sein wird, ist fraglich, zumal es aufgrund der Funktionsweise des digitalen Zwillings bei dessen Formierung schwierig sein wird, den Patienten so zu informieren, dass dieser die möglichen Konsequenzen seiner Entscheidung abschätzen kann.[225] Ohnedies stellt sich während des gesamten In-Beziehung-Stehens von digitalem und analogem Zwilling die generelle Frage nach der prinzipiellen Möglichkeit einer freiwilligen und informierten Einwilligung – sowohl betreffend die Datenverarbeitung als auch die medizinische Behandlung.

Schließlich gilt es zu bedenken, dass es Patienten geben kann, die aufgrund ihres Alters (bspw. Kinder) oder ihrer Beeinträchtigung keine wirksame Einwilligung in die für die Formierung des digitalen Zwillings notwendigen Datenverarbeitungen geben können. Gemäß *Krutzinna* führt dies entweder dazu, dass man diesen Personen den Zugang zur Technologie des digitalen Zwillings verwehrt, oder aber diese durch jemanden vertreten zu lassen, der in ihrem Namen handelt. Jedoch sind laut *Krutzinna* beide Möglichkeiten unbefriedigend: »First, how can digital twins become an ethically justifiable form of representation if those most in need of appropriate representation are barred from participation? Alternatively, if those unable to give consent require someone else to control and manage their digital twins, how can we avoid the illegitimate space of substitution, aggravated by the combination

222 Korenhof u.a. 2023, S. 11.
223 Korenhof u.a. 2023, S. 10.
224 Vgl. zur Einwilligung auch der Beitrag von Böning/Riechert in diesem Band.
225 Vgl. Huang/Kim/Schermer 2022, S. 5.

of proxy representation and decision making?«[226] An der von *Krutzinna* angesprochenen Problematik wird wiederum ersichtlich, dass der digitale Zwilling nicht zwingend zu einem menschlicheren Gesundheitswesen führt, zumal er zur Exklusion führen kann.

Betrachtet man ferner die Daten, aus denen sich der Datenkörper formiert, ist zu bedenken, dass dieser eben nicht nur aus Daten, die sich auf den Einzelnen beziehen, sondern auch aus geteilten Daten (»Daten im Plural«), insb. genetischen Daten, besteht. Damit ist zu fragen, ob geteilte Daten respektive Informationen, die eine Relation zu einem Dritten aufweisen, sich zugleich aber auf den analogen Patienten beziehen, vom digitalen Zwilling erfasst werden können. Die Herausforderung bei der Formierung, und insofern vorgreifend auch im restlichen »Lebenszyklus« des digitalen Zwillings, besteht also unter anderem darin, die Rechte des Patienten in Bezug auf seine Daten mit den Rechten einer anderen Person zu vereinbaren.[227]

Der Umstand, dass der digitale Zwilling voraussetzt, eine möglichst umfassende und dauerhaft gespeicherte Sammlung von Daten zur Verfügung zu halten, um seine nützliche, gesundheitsdienliche Funktion über die gesamte Lebensspanne des Einzelnen zu erfüllen, dürfte sich zudem im Hinblick auf den Grundsatz der Speicherbegrenzung (vgl. Art. 5 Abs. 1 lit. e DSGVO) und der Datenminimierung (vgl. Art. 5 Abs. 1 lit. c DSGVO) als problematisch erweisen.

1.2 Sein – Verschränkung

In der soeben beschriebenen Formierung des Datenkörpers im Sinne eines Zusammenziehens möglichst vieler Daten zwecks exakter Repräsentation und Simulation scheint sich der Wunsch zu manifestieren, die fragmentierten Teile des Datenkörpers (Gesundheitsdaten aus verschiedenen Quellen, Daten aus den sozialen Medien etc.) wieder zu vereinen – zu einem Datenkörper, über den sein analoger Zwilling Verfügungsbefugnis und Verfügungsmacht hat und insbesondere über die Zugänge zu diesem entscheiden kann. Beobachten wir hier also nicht etwas, das in seinen Grundzügen eine Idee des Datenschutzrechts wiedergibt? Geht man davon aus, dass das gegenwärtige Datenschutzrecht (noch immer) individualistisch geprägt ist, insbesondere die Idee der Kontrolle des Einzelnen über seine Daten

226 Krutzinna 2021, S. 403.
227 Teller 2021, S. 3.

verfolgt, dann scheint das Konzept des digitalen Zwillings in der Form eines Datenkörpers diese Idee geradezu zu verkörpern. Diese Schlussfolgerung könnte sich indes als Trugschluss erweisen, vergegenwärtigt man sich, dass sich der digitale Zwilling unter anderem aus geteilten Daten (unter anderem genetischen Daten) sowie aus Algorithmen formiert und damit aus Elementen, die nicht gänzlich seiner uneingeschränkten Kontrolle unterliegen. Wie aber präsentiert sich das Verhältnis zwischen dem analogen Zwilling und dem digitalen Zwilling? Zahlreiche Publikationen lassen sich dahingehend verstehen, dass sie der Ansicht sind, der analoge Zwilling müsse Eigentum an oder jedenfalls eine eigentumsanaloge Kontrolle über seinen Zwilling innehaben. Wie *Braun* indes richtig feststellt, suggeriert die Debatte über das Eigentum am Datenkörper eine falsche Alternative: »Die Frage ist nicht, ob eine Person Eigentümerin ihrer Simulation ist oder nicht, sondern ob die Person das Recht und die Kontrollmacht hat, die Art und Weise der Nutzung ihrer Simulation zu bestimmen.«[228] Zudem fragt sich, ob und wie sich der Einzelne dem Einsatz eines digitalen Zwillings entziehen kann respektive können soll. Dabei ist auch der Umstand zu berücksichtigen, dass ein digitaler Zwilling wohl von einem privaten Unternehmen zur Verfügung gestellt werden wird,[229] sich also auch die Frage stellt, wie sich die Rechte zwischen der Person, auf die sich der digitale Zwilling bezieht und den Schöpfern des Zwillings präsentieren.[230] Es eröffnet sich damit eine weitere Zugangsfrage: die Frage, inwiefern sichergestellt werden kann, dass dem Einzelnen Zugang zu seinem digitalen Zwilling gewährt wird. Darüber hinaus, und wie bereits herausgearbeitet, gestaltet sich die Beziehung zwischen analogem und digitalem Zwilling komplexer, denn deren bidirektionale Beziehung lässt die Unterscheidung zwischen Kontrollierendem und Kontrolliertem verschwimmen.[231]

228 Braun 2022, S. 216 f.

229 Vgl. Bruynseels/Santoni de Sio/van den Hoven 2018, S. 2 f.

230 Teller 2021, S. 4.

231 Darin liegt ein weiteres Argument gegen eine Kontrolle durch den analogen Zwilling, wie es Kerckhove 2021 formuliert: »The physical twin […] would be responsible for the DT's actions to conform with the law. This would be a different kind of responsibility […]. It is at this level that legal issues come into play, starting with access, ownership, management and control of data. Then, the ownership and management of the PDT […]. There follows the thorny issue of liability in cases where the PDT either ›abuses‹ its autonomy or causes an offence for a manufacturing defect.« S. 10.

Die Hoffnung besteht nun darin, dass es der DSGVO gelingt, es dem analogen Zwilling zu ermöglichen, selbst zu bestimmen, wie sein digitaler Zwilling genutzt wird und sicherzustellen, dass diese Nutzung mit seinen Vorlieben und Werten übereinstimmt.[232] Vor dem Hintergrund der Komplexität der Beziehung scheint das gegenwärtige Datenrecht dieser Hoffnung jedoch kaum gerecht werden zu können. Diesen Eindruck gewinnt man jedenfalls, versucht man die Geschehnisse im Stadium des »Seins« datenschutzrechtlich ansatzweise zu erfassen: Hier liefert der digitale Zwilling seinem Gegenüber Informationen, die auf der Grundlage von Indikatoren gewonnen werden, die mit Hilfe von Datenanalysetechnologien vorhergesagt werden, welche anhand historischer Daten trainiert und durch kontinuierliche Aktualisierung der Echtzeitdaten bewertet werden.[233] Diese Form der Datenverarbeitung ist wohl als Profiling zu qualifizieren und bedarf damit einer ausdrücklichen Einwilligung.

Damit bewegen wir uns wieder im schwierigen Gelände der Einwilligung. So kann etwa gefragt werden, inwieweit noch von einer freiwilligen Einwilligung die Rede sein kann, bedenkt man, dass die Bereitschaft Daten zugänglich zu machen auch vom jeweiligen Gesundheitszustand abhängen kann. Mit anderen Worten: »data protection is something for healthy people.«[234] Wie bereits bei der Formierung des Datenkörpers sehen wir uns auch hier mit der Problematik der geteilten Daten konfrontiert. Damit wird auch beim digitalen Zwilling die Frage aktuell: »What sorts of control might best accommodate the use of digital twins? Are any of the various new models of consent developed for datadriven medicine fit for the task? Why, if at all, should we accept dynamic consent over open-consent, broad-consent or meta-consent?«[235]

Indes präsentiert sich die Einwilligung nicht nur im Bereich des Profilings respektive der Datenverarbeitung als schwieriges Feld. Vergegenwärtigt man sich, dass der digitale Zwilling unter anderem Behandlungsempfehlungen macht, ist zu fragen, inwiefern wir es bei der Einwilligung in eine Behandlung mit einer autonom getroffenen Entscheidung zu tun haben, zumal es sich beim digitalen Zwilling um eine Steuerungstechnik handelt, deren Empfehlungen wohl im Sinne der Optimierung erfolgen.[236]

232 Amram u.a. 2023, S. 80.
233 Sahal/Alsamhi/Brown 2022, S. 17.
234 Popa u.a. 2021, S. 10.
235 Tigard 2021. S. 407.
236 Vgl. Wieser 2019, S. 444.

Vor dem Hintergrund des Oszillierens des digitalen Zwillings zwischen freiheitsermöglichender und freiheitsbeschränkender Technik ist zudem zu fragen, ob und wie es dem analogen Patienten gelingen kann, dem digitalen Zwilling gegenüber Freiheitsräume abzuringen, insbesondere in Anbetracht dessen prädiktiver Fähigkeiten.[237] Braucht es gegenüber dem digitalen Zwilling so etwas wie ein Recht auf Nichtwissen,[238] ein »right to be let alone by oneself«?[239] Inwieweit ein solches Recht auszugestalten ist, ist ungewiss. *Braun* spricht sich dafür aus, dass dem digitalen Zwilling nicht untersagt wird, eine bestimmte Form der Prädiktion zu erstellen, der analoge Zwilling aber ein Recht haben soll, sich gegen die Mitteilung einer bestimmten Warnung oder auch spezifischen Risikowahrscheinlichkeit einer Krankheit zu entscheiden.[240] Eine Möglichkeit, ein solches Recht auszuüben, könnte im Erstellen einer Liste bestehen, auf der jene Arten von Entscheidungen erfasst werden, für die ein Patient medizinische Informationen erhalten respektive nicht erhalten möchte.[241] *Tretter* gibt dabei aber zu bedenken, dass auch eine präventive Deaktivierung bestimmter Funktionen durch den Nutzer oder durch Voreinstellung den digitalen Zwilling nicht daran hindern kann, das Verhältnis des Patienten zur Welt hermeneutisch umzugestalten, denn der Patient kann nie gänzlich sicher sein, weshalb sein digitaler Zwilling »schweigt«.[242]

Der analoge Zwilling steht seinem digitalen Zwilling damit mit einer gewissen Ohnmacht gegenüber. Dies ist umso brisanter, ruft man sich eine Beobachtung von *Manfred Faßler* in Erinnerung: »Du, User, wendest eine Technologie auf Dich an, die Du nicht nur nicht kontrollieren kannst. Sie wird Dein gesamtes soziobiologisches Körpergeschehen verändern, als nach-genetische Entwicklung.«[243]

237 Braun 2021, S. 396.
238 Iqbal/Krauthammer/Biller-Andorno 2022, S. 590 f.
239 van der Sloot 2021, S. 223.
240 Braun 2022, S. 219.
241 Geneux 2021.
242 Tretter 2021, S. 411.
243 Faβler 2019, S. 196.

1.3 Vergehen – Entkopplung

Während der Einsatz eines digitalen Zwillings für ältere Menschen thematisiert wird,[244] erfährt der Umstand, dass der analoge Zwilling irgendwann sterben wird, bislang kaum Beachtung. In diesem schwierigen Feld gelangt man zu zahlreichen Anschlussfragen, die sich spätestens mit dem Tod der Patienten stellen und dann auch nicht mehr durch ein starkes Datenschutzregime ausgeschlossen werden können, zumal Erwägung 7 der DSGVO explizit statuiert, dass die Verordnung nicht für die personenbezogenen Daten Verstorbener gilt. Damit stellt sich dann auch die Frage nach der Daseinsberechtigung respektive einer möglichen Weiterexistenz des digitalen Zwillings. Was also passiert mit dem Datenkörper eines verstorbenen Patienten und welche Zugangsfragen können sich ergeben?

Zunächst ist festzustellen, dass der Patient, wie oben erläutert, grundsätzlich mittels Einwilligung den Zugang zu seinem Datenkörper kontrolliert. Nach dem Tod des Patienten ist sein Datenkörper verwaist, kann aber immer noch zugänglich sein, der verstorbene Patient kann jedoch den Zugang nicht mehr kontrollieren.[245] Damit stellt sich die Frage, wer Zugang zum Datenkörper erhält und wer die Zugänge verwaltet.

Die Antwort auf diese Fragen hängt auch davon ab, für welche rechtliche Lösung des Umgangs mit dem Datenkörper man sich entscheidet. *Malgieri* folgend gibt es (mindestens) drei verschiedene Szenarien für den Umgang mit personenbezogenen Daten nach dem Tod der betroffenen Person: Zunächst gibt es das Szenario der »Datenfreiheit«, wonach der für die Datenverarbeitung Verantwortliche die personenbezogenen Daten ohne jegliche Einschränkung und ohne jeglichen Schutz für den Verstorbenen und die Hinterbliebenen verarbeiten darf.[246] Des Weiteren gibt es das Szenario des »Quasi-Eigentums«, bei dem personenbezogene Daten von Verstorbenen ähnlich der Rechte des geistigen Eigentums an immateriellen Gütern »vererbt« werden,[247] Teil des digitalen Nachlasses bilden. Schließlich gibt es das Szenario des postmortalen Datenschutzes, bei dem die Privatsphäre der betroffenen Person auch nach ihrem Tod durch spezifische Maßnahmen geschützt wird, etwa indem das Datensubjekt im Voraus

244 Liu u.a. 2019.
245 Morse/Birnhack 2022, S. 5.
246 Malgieri 2018, S. 3 f.
247 Ebd., S. 3.

bestimmte Weisungen erteilen und eine Person seines Vertrauens mit der postmortalen Datenverarbeitung beauftragen kann.[248]

Gehört also der postume digitale Zwilling etwa zum digitalen Nachlass, vergleichbar einem Facebook-Account?[249] Eine solche Auffassung ließe sich jedenfalls für höchstpersönliche Belange der Datengeber schwer begründen. Gehören digitale Zwillinge dann aber schon ohne weiteres zum Schutzbereich eines »postmortalen Persönlichkeitsrechts«? Auch diese Sicht ist mit Rücksicht auf die (relative) Autonomie und Beteiligung Dritter am Digital-Twin-Modell keineswegs zwanglos begründbar. Jedenfalls hat auch die postume Nachwirkung des Persönlichkeitsrechts irgendwann ein Ende – und spätestens dann, »post-post«, stellt sich erneut die Frage nach den Löschungsansprüchen versus berechtigten Nutzungsinteressen.

2. Recht der Datenkörper

In Anbetracht der selektiv angeschnittenen daten(schutz)rechtlichen Problemlagen, die sich in der Beziehung des analogen mit dem digitalen Zwilling präsentieren, ist erst recht zu fragen, ob es nicht angezeigt ist, dass sich der Datenschutz anstatt auf die informationelle Selbstbestimmung der Nutzer, auf ihre vermeintliche Herrschaft über ihre personenbezogenen Daten, zu rekurrieren, den neuen informationstechnologischen Entwicklungen anpasst, die neue Bereiche der Persönlichkeitsentfaltung herausbilden.[250] Besonders mit Blick auf informationstechnische Systeme wie dem digitalen Zwilling kommt dabei zunehmend auch die Verselbständigung von bislang nur als Objekte oder Teile der menschlichen Persönlichkeit beobachteten Artefakte in Betracht. Der digitale Zwilling könnte nunmehr auch – als verkörperte Technik ebenso wie als technisierter Körper – zu einem möglichen Adressaten subjektivierender, personifizierender Zuschreibungen gehören.[251]

Wenn man hierbei zunächst den Fokus auf den Gesichtspunkt der Datensubjektivität beibehält, drängt sich eine erste Analogie zur haftungsrechtlichen Debatte um die sogenannte »e-Person« auf, die vorübergehend so-

248 Malgieri 2018, S. 3, 21.
249 Vgl. BGH 219, 243 (Urteil vom 12.07.2018, III ZR 183/17).
250 Vgl. Gruber 2015, S. 171.
251 Vgl. ebd., S. 8.

gar in europäischen Gesetzgebungsinitiativen[252] diskutiert worden ist. Im Unterschied zur elektronischen Person weist der digitale Zwilling aber zwei Merkmale auf, die zu einer anderen Bewertung führen könnten: Einerseits lässt sich sein möglicher Subjekt-Status anders als im Falle der e-Personhood nicht auf eine eigene Autonomie stützen, da er sich aus den Identitätsmerkmalen seines physischen Zwillings konstituiert. Andererseits sind dies jedoch Merkmale einer menschlichen personalen Identität, die eine Akzeptanz des digitalen Zwillings als »Datenperson« immerhin erleichtern könnten.[253]

Indes hat die DSGVO enge Vorstellungen davon, wer als Datensubjekt zu qualifizieren ist.[254] Grundsätzlich können nur natürliche Personen, d.h. Menschen, Datensubjekte sein.[255] Inwiefern diese Personen allerdings auch auf der Welt sein müssen, um geschützt zu werden, ist insoweit unscharf, als die DSGVO offenlässt, ob Informationen, die sich auf ein noch ungeborenes Kind (nasciturus) beziehen, personenbezogene Daten sind oder nicht.[256] Die Daten von Verstorbenen werden von der DSGVO gemäß Erwägungsgrund 27 nicht geschützt, da die DSGVO *Gola* zufolge von der Vorstellung geprägt ist, dass das Datensubjekt eine handelnde Person sein müsste.[257]

Man kann in der Formierung des Datenkörpers auch den Wunsch verkörpert sehen, die fragmentieren Teile des Datenkörpers wieder zu vereinen und es dem Datensubjekt zu ermöglichen, selbst über die Zugänge zu diesem Datenkörper zu bestimmen. Mag man diesen Gedanken weiterentwickeln, könnte man Parallelen zu gegenwärtigen Bestrebungen wie den Projekten »MyData«[258] und »Solid«[259] ziehen.[260] Solid (Social Linked Data) etwa ist ein

252 Siehe Europäisches Parlament 2018.

253 Ein häufiges, geradezu affekthaft gegen das Konzept der e-Personhood vorgebrachtes Argument bezieht sich auf die Sorge vor einem Verlust der menschlichen Sonderstellung im Recht; siehe z.B.: Wendehorst (»ethisch bedenkliche Verwirrungen«).

254 Vergleiche zum Datensubjekt auch den Beitrag von Brieske/Schweitzer in diesem Band.

255 Arning/Rothkegel 2019, Rn. 15.

256 Arning/Rothkegel 2019, Rn. 21.

257 Gola 2022, Rn. 29.

258 https://mydata.org/ [21.5.2024].

259 https://solidproject.org/ [21.5.2024].

260 Die Designüberlegungen für den digitalen Zwilling von Schwartz u.a. 2020 jedenfalls scheinen dieser Idee zu ähneln, wenn sie schreiben: »To bring the digital twin concept to life, people must have access to an integrated set of tools, content, and services all existing within a single internally consistent live and digital experience that helps both patient and practitioner make data-based health choices. These data create the person's health data repository. There must also be a mechanism for people to access the resultant insights. In one model, people could create person-

laufender Versuch, die Kontrolle über Daten zu dezentralisieren, indem die Speicherung von persönlichen Daten von Silos in sogenannte Pods (personal online data stores) verlagert wird, die von Einzelpersonen respektive den jeweiligen Datensubjekten kontrolliert werden. Die Einzelpersonen, die den Pod verwenden, kontrollieren, wie und wann Anwendungen auf Daten zugreifen können, indem sie den Zugriff jederzeit gewähren oder widerrufen können. Durch die Kontrolle des Zugriffs auf ihre Daten innerhalb von Pods erhalten Einzelpersonen auch die Möglichkeit, die Daten an anderer Stelle für konkurrierende Dienste oder für andere Funktionen (wieder-)zu verwenden.[261] Die Möglichkeit, seine eigenen Daten auf diese Weise zu verwalten, kann indes wiederum zu einer nicht wünschenswerten Responsibilisierung des einzelnen Datensubjekts führen, indem es am Einzelnen liegt, unter anderem über die Gewährleistung der Zugänge zu seinen Daten zu entscheiden und diese zu verwalten.[262]

Neue Perspektiven könnten sich allerdings bereits daraus ergeben, dass die Modellierung und Konstitution des digitalen Zwillings von Dritten, namentlich von intermediären (Provider-)Diensten abhängig ist, deren Betrieb ein gewisses Maß an Datennutzung, mithin Datenzugang voraussetzt. Die europäische Gesetzgebung versucht in dieser und anderen Hinsichten, mit einer umfassenden »Datenstrategie« auf das komplexe Verhältnis von Datenschutz und Datenzugänglichkeit, auch im eigenen Interesse der geschützten Datengeber, zu antworten. Ein Bestandteil dieser Strategie liegt naheliegenderweise darin, die Funktion der Intermediäre und Mittler so auszugestalten, dass das Vertrauen der Datengeber auf den Schutz ihrer personenbezogenen Daten auch im Falle einer Datennutzung durch Dritte gestärkt wird. In diesem Sinne soll vor allem der Data Governance Act (DGA)[263] die missbrauchsfreie Nutzung geschützter Daten mithilfe

alized accounts via a website or downloaded app. It is also possible that entities, such as health systems or regional or national governments, might create the digital twin system for enrolling their members or citizens. […] Once an account is created for an individual, including unique identity markers, the user could permission various data sources to interface with the digital twin to avoid potential data misuse or abuse. Once data sources are connected to the system, the individual would then return to the account to view insights and feedback over time« S. 4.

261 van Damme u.a. 2022, S. 563 f.

262 Vgl. ebd., S. 572.

263 Europäische Kommission 2022.

von Datenvermittlungsdiensten[264], wie beispielsweise Datentreuhändern, gewährleisten.

Die nähere Ausgestaltung solcher Datenmittler ist allerdings noch offen und wird derzeit – je nach Anwendungskontext höchst variantenreich – diskutiert. Im Fall der digitalen Zwillinge wird davon auszugehen sein, dass deren Betrieb und Pflege eine dauerhafte Datenspeicherung im technischen Einflussbereich eines Datentreuhänders voraussetzt, so dass elegantere Lösungen wie etwa ein »transaktionsbasiertes Treuhandmodell«[265] hier wohl nicht in Betracht kommen. Geht man in der Regel von der allgemeinen Zielsetzung aus, dass Datentreuhänder als Plattformen ein geeignetes digitales Identitätsmanagement (oder »PIM«, Personal Information Management) vorhalten und im Ergebnis eine neutrale Äquidistanz zwischen Datengebern und -nutzern herstellen müssen, wäre vorliegend womöglich doch ein erhöhtes Schutzbedürfnis der physischen Zwillinge als Datengeber im medizinischen Bereich zu bedenken. Das würde gegebenenfalls nicht nur entsprechende gesellschaftsrechtliche Gestaltungen der Datentreuhand mit größerer Schutzwirkung zugunsten der Datengeber erfordern (Stiftung, nicht-rechtsfähiger Verein), sondern auch technische Lösungen, etwa zur Verwirklichung eines *Rechts auf Nichtwissen* der (simulierten) zukünftigen Zwillings-Krankengeschichten. Bereits in derartigen Konstellationen könnte die Ablösung des digitalen Zwillings als eigenständiges Datensubjekt eine *Repräsentations- und Stellvertreterfunktion* für die dahinter stehenden physischen Menschen aus Fleisch und Blut übernehmen. Die Vertretung solcher digitalen Datensubjekte könnte ihrerseits innerhalb der Datentreuhand gesellschaftsrechtlich organisiert werden.

V. Ausblick: Ein transsubjektives Daten(schutz)recht?

Im digitalen Zwilling begegnet das Datenrecht offenbar der Dynamik einer derzeit noch kaum überschaubaren Technologie, die in Anlehnung an *Erich Hörls* und *Michael Hagners* Studie zur Kulturgeschichte der Kybernetik als Fortsetzung der »Transformation des Humanen« gelesen werden kann: Demzufolge habe die zunehmend verbreitete informationstheoretische

264 Dazu gehören öffentliche Stellen, Anbieter von Diensten für die gemeinsame Datennutzung oder eingetragene Einrichtungen, die Datenaltruismus-Dienste (vgl. Art. 15 DGA) erbringen.

265 Buchheim/Augsberg/Gehring 2022, S. 1141 ff.

Beobachtungsweise von Leben, Technik sowie Gesellschaft dazu geführt, auch den Menschen selbst nicht mehr auf seine individuelle Eigenart hin zu befragen, sondern als einen »komplexen Funktionsmechanismus« zu betrachten, der sich nicht prinzipiell von Maschinen unterscheidet.[266] Mit derartigen technizistischen Modellierungen ändert sich folglich auch das hergebrachte Menschenbild. Dessen »permanente, oftmals kaum wahrnehmbare Transformation angesichts der wissenschaftlich-technischen Prozesse«, die damit einhergehenden »Verschiebungen zwischen den menschlichen und technologischen Bedingungen«, nicht zuletzt auch die Veränderungen des menschlichen Selbstverständnisses, die mitunter schon die Selbstwahrnehmung »als Teil von Mensch-Maschinen-Kopplungen« in sich bergen[267] – dies alles mag erneut an die Rede vom »Ende des Menschen« erinnern, wie Michel Foucault[268] anknüpfend an Nietzsche[269] den Tod des neuzeitlichen Subjekts genannt hat, und zwar im doppelten Wortsinn verstanden als »Verenden eines metaphysischen Großbegriffs«[270] und als Delegation von ehedem zutiefst menschlichen Merkmalen an einen digital generierten, bioartifiziellen Datenkörper. Der digitale Zwilling erweist sich damit als eine Mensch-Maschine-Assoziation *par excellence*, die aus der Perspektive der Akteur-Netzwerk-Theorie Bruno Latours ein Geflecht von wirkungsmächtigen, mithin handlungswirksamen »Mittlern« darstellt: »Subjektivität ist keine Eigenschaft menschlicher Seelen, sondern des Versammelns selber – natürlich nur, sofern es dauert.«[271] Statt der als »unteilbar« erdachten menschlichen Individuen sind es also »Mittler, die andere Mittler dazu bringen, Dinge zu tun«, und damit werden Akteure zum Handeln gebracht.[272]

Die juridische Konzeption des Rechtssubjekts wird den damit angedeuteten Wandel zur postanthropozentrischen Gesellschaft gewiss überdauern. Aber es steht zu erwarten, dass sie eine funktionale Umstellung in einer Weise erfahren wird, die Gunther Teubner als »transsubjektive Dimensionen subjektiver Rechte«[273] kennzeichnet. Rechtssubjektivität bestimmt sich

266 Vgl. hierzu Hörl/Hagner 2008, S. 11.
267 Ebd., S. 10 f.
268 Vgl. hierzu Foucault 1997 [1974], S. 460 ff.
269 Vgl. Nietzsche 1994 [1883], S. 97 und 286.
270 Vgl. entsprechend Hörl/Hagner 2008, S. 10.
271 Vgl. Latour 2007, S. 368 ff., insbesondere S. 375 ff.
272 Siehe etwa Latour 2007, S. 76 ff., 186 und 374 f.; vgl. dazu auch Gruber 2015, S. 224 ff., m.w.N.
273 Vgl. Teubner 2018, S. 360 ff.

demzufolge nicht etwa anhand vorgebenener »Subjektwesenheiten«[274] in der Umwelt des Rechts, wie es die häufige Gleichsetzung von »Person« und »Mensch« nahezulegen scheint. Vielmehr resultiert sie aus kommunikativen Zuschreibungsprozessen, die neue rechtliche »Zurechnungspersonen«[275] erzeugen. Es ist dann nicht unmittelbar entscheidend, wie dieses Gegenüber beschaffen ist, das durch die »symbolische Auszeichnung mit Kommunikationsteilnahmekompetenz« den Status als Rechtsperson erhält.[276] Vielmehr kommt es darauf an, jenseits der individualistischen Fixierungen subjektiver Rechtezuschreibungen auf »den« Menschen auch die heute immer deutlicher zutage tretenden Dimensionen der Kommunikationen, der Kollektivakteure und der Kommunikationsmedien in den Blick zu nehmen.[277]

Die Frage der Rechtssubjektivität und insbesondere der Datensubjektivität entscheidet danach nicht nur über die abstrakte rechtstheoretische Möglichkeit einer Inklusion neuer Akteure und deren Teilnahme an Kommunikation. Sie hat auch Bedeutung für die naheliegenden rechtlichen Folgefragen, die etwa auch die mit den Debatten um »Big Data« aufgekommenen Debatten über die Rechte an eigenen Daten (»Dateneigentum«, »Datenbesitz«, »Datenerzeugerrecht«) betreffen. Die jeweiligen Antworten hängen davon ab, wer als berechtigtes Datensubjekt überhaupt in Betracht kommt, wem Datenrechte, ob als Dateneigentums- oder als Datenzugangsrechte, zugewiesen werden und welche Bedeutung den betreffenden Daten, etwa als Gesundheits- oder KI-Trainingsdaten, für die jeweiligen Rechtssubjekte überhaupt zugeschrieben wird. Auf allen diesen weiten Feldern lässt sich zeigen, wie die Rechte- und Verantwortungszuschreibungen uneindeutig werden, weil sie durch Kollektivitäts-Phänomene der digitalen Welt unterlaufen werden, die vor allem von Intermediären und deren vielfältigen Verflechtungen geprägt sind. Unter diesen komplexen Bedingungen, deren Unsicherheit durch die Multiplizität der daran mitwirkenden Akteure und Aktanten noch gesteigert wird, wäre es an der Zeit, neue kollektive Datensubjekte versuchsweise als Rechtsgestaltungsmodelle zu erproben, die den Anforderungen eines transsubjektiven Datenrechts nachkommen. Transsubjektives Datenschutz- und Datenrecht mag den von den Verheißungen der personali-

274 Vgl. hierzu Fuchs 2003, S. 23.

275 Teubner 2006, S. 23.

276 Vgl. ebd., S. 12; zum historischen Wandel dieser Inklusionsmechanismen von normativen Zurechnungssubjekten auch Augsberg 2016, S. 349 ff.

277 Vgl. hierzu Teubner 2018, S. 361.

sierten Medizin betroffenen Menschen, hier insbesondere den individuellen »physischen Zwillingen«, neue Chancen auf Teilhabe eröffnen, indem es rechtliche Zugänge für eine kollektive Wahrnehmung partizipativer Rechte schafft. Soweit es mit solchen Rechten gelingt, die Möglichkeiten der Mitbestimmung und Beteiligung an Innovationsprozessen zu verbessern, verbinden sich damit auch neue Aussichten auf einen den Entwicklungen angepassten künftigen Schutz der physischen und psychischen Integrität der Menschen.

Literatur

Acosta, Julián N./Falcone, Guido J./Rajpurkar, Pranav/Topol, Eric J. (2022): Multimodal biomedical AI, in: *Nature Medicine* 28, Heft 9, S. 1773–1784.

Amram, Benjamin/Klempner, Uri/Leibler, Yehuda/Greenbaum, Dov (2023): In Their Own Image: Ethical Implications of the Rise of Digital Twins/Clones/Simulacra in Healthcare, in: *The American Journal of Bioethics* 23, Heft 9, S. 79–81.

Armeni, Patrizio; Polat, Irem; Rossi, Leonardo Maria de; Diaferia, Lorenzo; Visioli, Giacomo; Meregalli, Severino; Gatti, Anna (2023): Digital Twins for Health: Opportunities, Barriers and a Path Forward, in: Korhan, Orhan (Hg.): *Digital Twin Technology. Fundamentals and Applications*, London, S. 19–40.

Armeni, Patrizio/Polat, Irem/Rossi, Leonardo Maria de/Diaferia, Lorenzo/Meregalli, Severino/Gatti, Anna (2022): Digital Twins in Healthcare: Is It the Beginning of a New Era of Evidence-Based Medicine? A Critical Review, in: *Journal of Personalized Medicine* 12, Heft 8, S. 1–14.

Arning, Marian Alexander/Rothkegel, Tobias (2019): Art. 4 DSGVO, in: Taeger, Jürgen/Gabel, Detlev (Hg.): *DSGVO – BDSG*, dritte Auflage, Frankfurt am Main, S. 87–250.

Augsberg, Steffen (2016): Der Anthropozentrismus des juristischen Personenbegriffs – Ausdruck überkommener (religiöser) Traditionen, speziesistischer Engführung oder funktionaler Notwendigkeiten?, in: *Rechtswissenschaft (RW)*, Heft 3, S. 338–362.

Bagaria, Namrata/Laamarti, Fedwa/Badawi, Hawazin Faiz/Albraikan, Amani/Martinez Velazquez, Roberto Alejandro/El Saddik, Abdulmotaleb (2020): Health 4.0: Digital Twins for Health and Well-Being, in: El Saddik, Abdulmotaleb/Hossain, M. Shamim/Kantarci, Burak (Hg.): *Connected Health in Smart Cities*, Basel, S. 143–152.

BBC News (2022): *Why you may have a thinking digital twin within a decade*, 13.6.2022, https://www.bbc.com/news/business-61742884 [21.5.2024].

Becker, Konrad (2003): *Die Politik der Infosphäre*, World-Information.Org, Wiesbaden.

Björnsson, Bergthor/Borrebaeck, Carl/Elander, Nils/ Gasslander, Thomas/Gawel, Danuta R./Gustafsson, Mika/Jörnsten, Rebecka/Lee, Eun Jung/Li, Xinxiu/Lilja, Sandra/Martínez-Enguita, David/Matussek, Andreas/Sandström, Per/Schäfer, Samuel/Stenmar-

ker, Margaretha/Sun, X. F./Sysoev, Oleg/Zhang, Huan/Benson, Mikael (2019): Digital twins to personalize medicine, in: *Genome Medicine* 12, Heft 1, S. 1–4.

Blok, Vincent (2023): Philosophy of technology in the digital age: The datafication of the World, the homo virtualis, and the capacity of technological innovations to set the World free, Antrittsvorlesung, 7.9.2023, https://edepot.wur.nl/639666 [21.5.2024].

Boer, Bas de (2020): Experiencing objectified health: turning the body into an object of attention, in: *Medicine, Health Care and Philosophy* 23, Heft 3, S. 401–411.

Braun, Matthias (2022): Digitale Zwillinge und Verschiebungen im Verhältnis von Gesundheit und Krankheit, in: *Zeitschrift für medizinische Ethik*, Heft 2, S. 209–222.

Braun, Matthias (2021): Represent me: please! Towards an ethics of digital twins in medicine, in: *Journal of Medical Ethics* 47, Heft 6, S. 394–400.

Bruynseels, Koen/Santoni de Sio, Filippo/van den Hoven, Jeroen (2018): Digital Twins in Health Care: Ethical Implications of an Emerging Engineering Paradigm, in: *Frontiers in Genetics* 9, S. 1–11.

Buchheim, Johannes/Augsberg, Steffen/Gehring, Petra (2022): Transaktionsbasierte Datentreuhand. Nutzungsszenarien, Kennzeichen und spezifische Leistungen eines neuen Modells gemeinsamer Datennutzung, in: *JuristenZeitung* 77, Heft 23, S. 1139–1147.

Cellina, Michaela/Cè, Maurizio/Alì, Marco/Irmici, Giovanni/Ibba, Simona/Caloro, Elena/Fazzini, Deborah/Oliva, Giancarlo/Papa, Sergio (2023): Digital Twins: The New Frontier for Personalized Medicine?, in: *Applied Sciences* 13, Heft 13, S. 1–16.

Chiodo, Simona (2023): Engineered humans, in: *Studi di estetica* 1, Heft 25, S. 157–181.

Cho, Mildred K./Martinez-Martin, Nicole (2023): Epistemic Rights and Responsibilities of Digital Simulacra for Biomedicine, in: *The American Journal of Bioethics* 23, Heft 9, S. 43–54.

Coveney, Peter/Highfield, Roger (2023): *Virtual you. How building your digital twin will revolutionize medicine and change your life*, Princeton.

DSI Strategy Lab (2022): *Künstliche Intelligenz in der Medizin*, https://www.dsi.uzh.ch/de/research/projects/strategy-lab/strategy-lab-22.html [21.5.2024].

Europäische Kommission (2023a): *EU-Initiative für das Web 4.0 und virtuelle Welten: mit Vorsprung in den nächsten technologischen Wandel*, 11.7.2023, COM(2023) 442 final, https://ec.europa.eu/transparency/documents-register/api/files/COM(2023)442_0/090166e5 ff2b668 f?rendition=false [21.5.2024].

Europäische Kommission (2023b): *European Virtual Human Twins Initiative*, 21.12.2023, https://digital-strategy.ec.europa.eu/en/news/virtual-human-twins-launch-european-virtual-human-twins-initiative?pk_source=ec_newsroom&pk_medium=email&pk_campaign=Shaping%20Europe%E2%80%99s%20Digital%20Future [21.5.2024].

Europäische Kommission (2022): *Verordnung (EU) 2022/868 des Europäischen Parlaments und des Rates vom 30. Mai 2022 über europäische Daten-Governance und zur Änderung der Verordnung (EU) 2018/1724 (Daten-Governance-Rechtsakt)*, Amtsblatt L 152/1, https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32022R0868 [21.5.2024].

Europäische Kommission (2016): *Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)*, Amtsblatt L 119/1, https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679 [21.5.2024].

Europäisches Parlament (2018): *Entschließung vom 16. Februar 2017 mit Empfehlungen an die Kommission zu zivilrechtlichen Regelungen im Bereich Robotik*, Amtsblatt C 252/25 vom 16.12.2017, https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52017IP0051 [21.5.2024].

Faßler, Manfred (2019): Vom Subjekt zum User – und zurück?, in: Gentzel, Peter u.a. (Hg.): *Das vergessene Subjekt*, Wiesbaden, S. 185–206.

Foucault, Michel (1997 [1974]): *Die Ordnung der Dinge. Eine Archäologie der Humanwissenschaften*, Frankfurt am Main.

Fuchs, Peter (2003): *Der Eigen-Sinn des Bewusstseins. Die Person, die Psyche, die Signatur*, Bielefeld: transcript.

Geneux, Valérie (2021): *How healthy is your digital twin?*, EPFL News, 14.5.2021, https://longread.epfl.ch/en/dossier/how-healthy-is-your-digital-twin/ [21.5.2024].

Gola, Peter (2022): Art. 4 DS-GVO, in: Gola, Peter/Heckmann, Dirk (Hg.): *Datenschutz-Grundverordnung – Bundesdatenschutzgesetz*, dritte Auflage, München, S. 240–282.

Gruber, Malte-Christian (2023): Mensch-Maschine-Beziehungen in der »Deep Medicine«: Zur Herausbildung neuer Haftungsmodelle am Beispiel medizinischer KI-Systeme, in: *Rechtswissenschaft (RW)*, Heft 3, S. 277–305.

Gruber, Malte-Christian (2015): *Bioinformationsrecht. Zur Persönlichkeitsentfaltung des Menschen in technisierter Verfassung*, Tübingen.

Haggerty, Kevin D./Ericson, Richard V. (2000): The surveillant assemblage, in: *British Journal of Sociology* 51, Heft 4, S. 605–622.

Haleem, Abid/Javaid, Mohd/Pratap Singh, Ravi/Suman, Rajiv (2023): Exploring the revolution in healthcare systems through the applications of digital twin technology, in: *Biomedical Technology* 4, S. 28–38.

Hassani, Hossein/Huang, Xu/MacFeely, Steve (2022): Impactful Digital Twin in the Healthcare Revolution, in: *Big Data and Cognitive Computing* 6, Heft 3, S. 1–17.

Huang, Pei-Hua/Kim, Ki-Hun/Schermer, Maartje (2022): Ethical Issues of Digital Twins for Personalized Health Care Service: Preliminary Mapping Study, in: *Journal of Medical Internet Research* 24, Heft 1, S. 1–12.

Hörl, Erich/Hagner, Michael (2008): Überlegungen zur kybernetischen Transformation des Humanen, in: Hagner, Michael/Hörl, Erich (Hg.): *Die Transformation des Humanen. Beiträge zur Kulturgeschichte der Kybernetik*, Frankfurt am Main, 7–37.

Iqbal, Jeffrey D./Krauthammer, Michael/Biller-Andorno, Nikola (2022): The Use and Ethics of Digital Twins in Medicine, in: *The Journal of Law, Medicine & Ethics* 50, Heft 3, S. 583–596.

Iqbal, Jeffrey D./Biller-Andorno, Nikola (2022): The regulatory gap in digital health and alternative pathways to bridge it, in: *Health Policy and Technology* 11, Heft 3, S. 1–7.

Kamel Boulos, Maged N./Zhang, Peng (2021): Digital Twins: From Personalised Medicine to Precision Public Health. In: *Journal of Personalized Medicine* 11, Heft 8, S. 1–12.

Kämpf, Katrin M. (2021): Bits & Pieces versorgen. Ein Plädoyer, in: *Zeitschrift für Medienwissenschaft* 13, Heft 1, S. 58–64.

Kerckhove, Derrick de (2021): The personal digital twin, ethical considerations, in: *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 379, Heft 2207, S. 1–12.

Korenhof, Paulan/Blok, Vincent/Kloppenburg, Sanneke (2021): Steering Representations – Towards a Critical Understanding of Digital Twins, in: *Philosophy & Technology* 34, Heft 4, S. 1751–1773.

Krüger, Oliver (2019): *Virtualität und Unsterblichkeit. Gott, Evolution und die Singularität im Post- und Transhumanismus*, zweite Auflage, Freiburg im Breisgau.

Krutzinna, Jenny (2021): Simulating (some) individuals in a connected world, in: *Journal of Medical Ethics*, Heft 6, S. 403–404.

Latour, Bruno (2007): *Eine neue Soziologie für eine neue Gesellschaft. Einführung in die Akteur-Netzwerk-Theorie*, Frankfurt am Main.

Laubenbacher, Reinhard/Sluka, James P./Glazier, James A. (2021): Using digital twins in viral infection, in: *Science* 371, Heft 6534, S. 1105–1106.

Liu, Ying/Zhang, Lin/Yang, Yuan/Zhou, Longfei/Ren, Lei/Wang, Fei/Liu, Rong/Pang, Zhibo/Deen, M. Jamal (2019): A Novel Cloud-Based Framework for the Elderly Healthcare Services Using Digital Twin, in: *IEEE Access* 7, S. 49088–49101.

Liu, Zheng/Meyendorf, Norbert/Mrad, Nezih, (2018): The role of data fusion in predictive maintenance using digital twin, in: *AIP Conference Proceedings* 1949, Heft 1, S. 020023–1-6.

Lobe, Adrian (2019): *Speichern und Strafen. Die Gesellschaft im Datengefängnis*, München.

Lorentz, Nora (2020): *Profiling – Persönlichkeitsschutz durch Datenschutz?*, Tübingen.

Lupton, Deborah (2021): Language matters: the ›digital twin‹ metaphor in health and medicine, in: *Journal of Medical Ethics* 47, Heft 6, S. 409.

Lupton, Deborah (2016): Digital companion species and eating data: Implications for theorising digital data–human assemblages, in: *Big Data & Society* 3, Heft 1, S. 1–5.

Maeyer, Christel de/Markopoulos, Panos (2020): Are Digital Twins Becoming Our Personal (Predictive) Advisors? Our Digital Mirror of Who We Were, Who We Are and Who We Will Become, in: Gao, Qin/Zhou, Jia Zhou (Hg.): *Aspects of IT for the Aged Population. Healthy and Active Aging*, Basel, S. 250–268.

Malgieri, Gianclaudio (2018): R.I.P.: Rest in Privacy or Rest in (Quasi-)Property? Personal Data Protection of Deceased Data Subjects between Theoretical Scenarios and National Solutions, in: Leenes, Ronald u.a. (Hg.): *Data Protection and Privacy: The Internet of Bodies*, Oxford, S. 143–168, abgerufen von SSRN: https://ssrn.com/abstract=3185249 [21.5.2024].

Miller, Michael E./Spatz, Emily (2022): A unified view of a human digital twin, in: *Human-Intelligent Systems Integration* 4, Heft 1–2, S. 23–33.

Mittelstadt, Brent (2021): Near-term ethical challenges of digital twins, in: *Journal of Medical Ethics* 47, Heft 6, S. 405–406.

Mocanu, Diana/Sibony, Anne-Lise (2023): EU consumer law meets digital twins, in: *Revue européenne de droit de la consommation* 1, S. 229–257.

Morse, Tal/Birnhack, Michael (2022): The continuity principle of digital remains, in: *New Media & Society*, OnlineFirst, S. 1–19.

Nietzsche, Friedrich (1994 [1883]): Also sprach Zarathustra. Ein Buch für Alle und Keinen, in: ders.: *Werke in drei Bänden*, Band 2, Köln, S. 93–419.

Noller, Jörg (2022): *Digitalität. Zur Philosophie der digitalen Lebenswelt*, Basel.

Petri, Thomas (2020): Der Mensch im zukünftigen Gesundheitswesen und sein Datendouble, in: Manzeschke, Arne/Niederlag, Wolfgang (Hg.): *Ethische Perspektiven auf Biomedizinische Technologie*, Berlin, S. 42–48.

Popa, Eugen Octav/van Hilten, Mireille/Oosterkamp, Elsje/Bogaardt, Marc-Jeroen (2021): The use of digital twins in healthcare: socio-ethical benefits and socio-ethical risks, in: *Life Sciences, Society and Policy* 17, Heft 6, S. 1–25.

Rubeis, Giovanni (2023): Hyperreal Patients. Digital Twins as Simulacra and their impact on clinical heuristics, in: Loh, Janina/Grote, Thomas (Hg.): *Medizin – Technik – Ethik*, Berlin/Heidelberg, S. 193–207.

Sahal, Radhya/Alsamhi, Saeed H./Brown, Kenneth N. (2022): Personal Digital Twin: A Close Look into the Present and a Step towards the Future of Personalised Healthcare Industry, in: *Sensors* 22, Heft 15, S. 1–35.

Schwartz, Steven M./Wildenhaus, Kevin/Bucher, Amy/Byrd, Brigid (2020): Digital Twins and the Emerging Science of Self: Implications for Digital Health Experience Design and »Small« Data, in: *Frontiers in Computer Science* 2, S. 1–16.

Sharon, Tamar (2018): When digital health meets digital capitalism, how many common goods are at stake?, in: *Big Data & Society* 5, Heft 2, S. 1–12.

Sharon, Tamar (2017): Self-Tracking for Health and the Quantified Self: Re-Articulating Autonomy, Solidarity, and Authenticity in an Age of Personalized Healthcare, in: *Philosophy & Technology* 30, Heft 1, S. 93–121.

Shengli, Wei (2021): Is Human Digital Twin possible?, in: *Computer Methods and Programs in Biomedicine Update* 1, Heft 1, S. 1–8.

Sparrow, Robert/Hatherley, Joshua (2020): High hopes for ›Deep Medicine‹? AI, economics, and the future of care, in: *Hastings Center Report* 50, Heft 2, S. 14–17.

Sun, Tianze/He, Xiwang/Li, Zhonghai (2023): Digital twin in healthcare: Recent updates and challenges, in: *Digital Health* 9, S. 1–13.

Sun, Tianze/He, Xiwang/Song, Xueguan/Shu, Liming/Li, Zhonghai (2022): The Digital Twin in Medicine: A Key to the Future of Healthcare?, in: *Frontiers in Medicine* 9, S. 1–8.

Stalder, Felix (2002): Privacy Is Not the Antidote to Surveillance, in: *Surveillance & Society* 1, Heft 1, S. 120–124.

Teller, Marina (2021): Legal aspects related to digital twin, in: *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 379, Heft 2207, S. 1–7.

Teubner, Gunther (2018): Zum transsubjektiven Potential subjektiver Rechte. Gegenrechte in ihrer kommunikativen, kollektiven und institutionellen Dimension, in: Fischer-Lescano, Andreas/Franzki, Hannah/Horst, Johan (Hg.): *Gegenrechte. Recht jenseits des Subjekts*, Tübingen, S. 357–375.

Teubner, Gunther (2006): Elektronische Agenten und große Menschenaffen: Zur Ausweitung des Akteursstatus in Recht und Politik, in: *Zeitschrift für Rechtssoziologie* 27, Heft 1, S. 5–30.

Tigard, Daniel W. (2021): Digital twins running amok? Open questions for the ethics of an emerging medical technology, in: *Journal of Medical Ethics* 47, Heft 6, S. 407–408.

Topol, Eric J. (2020): *Deep Medicine: Künstliche Intelligenz in der Medizin. Wie KI das Gesundheitswesen menschlicher macht*, Frechen.

Topol, Eric J. (2019): High-performance medicine: the convergence of human and artificial intelligence, in: *Nature Medicine* 25, Heft 1, S. 44–56.

Tretter, Max (2021): Perspectives on digital twins and the (im)possibilities of control, in: *Journal of Medical Ethics* 47, Heft 6, S. 410–411.

Vallée, Alexandre (2023): Digital twin for healthcare systems, in: *Frontiers in Digital Health* 5, S. 1–6.

van Damme, Sander/Mechant, Peter/Vlassenroot, Eveline/Van Compernolle, Mathias/Buyle, Raf/Bauwens, Dorien (2022): Towards a Research Agenda for Personal Data Spaces: Synthesis of a Community Driven Process, in: Janssen, Marijn u.a. (Hg.): *Electronic Government*, EGOV 2022, Basel, S. 563–577.

van der Ploeg, Irma (2012): The body as data in the age of information, in: Ball, Kirstie/Haggerty, Kevin D./Lyon, David (Hg.): *Routledge Handbook of Surveillance Studies*, Abingdon, S. 176–185.

van der Sloot, Bart (2021): The right to be let alone by oneself: narrative and identity in a data-driven environment, in: *Law, Innovation and Technology* 13, Heft 1, S. 223–255.

van der Valk, Hendrik/Haße, Hendrik/Möller, Frederik/Arbter, Michael/Henning, Jan-Luca/Otto, Boris (2020): A Taxonomy of Digital Twins, in: *Americas Conference on Information Systems 2020 Proceedings*, S. 1–10, https://www.researchgate.net/publication/341235159_A_Taxonomy_of_Digital_Twins [21.5.2024].

Wang, Yuntao/Su, Zhou/Guo, Shaolong/Dai, Minghui/Luan, Tom H./Liu, Yiliang (2023): A Survey on Digital Twins: Architecture, Enabling Technologies, Security and Privacy, and Future Prospects, in: *IEEE Internet of Things Journal* 10, Heft 17, S. 14965–14987.

Wiedemann, Lisa (2022): Digitale und analoge Körper, in: Gugutzer, Robert/ Klein, Gabriele/Meuser, Michael (Hg.): *Handbuch Körpersoziologie 2. Forschungsfelder und methodische Zugänge*, Wiesbaden, S. 75–90.

Wieser, Bernhard (2019): Digitale Gesundheit: Was ändert sich für den Gesundheitsbegriff?, in: *Österreichische Zeitschrift für Soziologie* 44, Heft 4, S. 427–449.

Zugangs(begrenzungs)konsequenzen: Gesundheitsdaten – (nicht) nur für die Gesundheit?

Der europäische Gesundheitsdatenraum: Ein Paradigmenwechsel in der Verarbeitung von Gesundheitsdaten?

Fabiola Böning und Anne Riechert

1. Einleitung

Auf EU-Ebene sollen Datenbestände besser nutzbar gemacht werden. Die EU will gleichermaßen Vorbild und Vorreiterin einer »datennutzenden Gesellschaft« sein.[1] Die verbesserte Nutzung von Gesundheitsdaten verspricht nicht nur eine verbesserte Versorgung, sondern auch erhebliche wirtschaftliche Vorteile.[2] Der Zusammenführung verschiedener Daten wohnt ein enormes Potential inne,[3] welches auch dem europäischen und dem deutschen Gesetzgeber bekannt ist. Die elektronische Patientenakte (ePA) ist ein Beispiel dafür. Dennoch gibt es strukturelle und individuelle Herausforderungen der Datenzusammenführung, da eine solche bislang einem stark individualzentriertem Regelungsregime unterfiel. Mit neuen Gesetzesakten auf beiden Ebenen wird nun der Versuch unternommen, einen Ausgleich zwischen dem informationellen Selbstbestimmungsrecht der PatientInnen einerseits und der Forschungsfreiheit andererseits zu finden. Weiterhin relevant sind die verbesserte grenzüberschreitende Versorgung von PatientInnen sowie ein funktionierendes und kosteneffizientes Gesundheitssystem. Inwiefern dabei individuelle Rechte der PatientInnen gewahrt werden und welche Alternativen es zur individuell ausgeübten Kontrolle gibt, will der Beitrag untersuchen.

---

1 Hennemann/von Ditfurth 2022, S. 1905.

2 Siehe dazu nur Lupiáñez-Villanueva u.a. (2021): S. 147 ff. und zu den Nutzungspotentialen im Hinblick auf die Kostenreduzierung durch die Digitalisierung des Gesundheitswesens in Deutschland z. B. McKinsey & Company 2022.

3 Ein Beispiel ist die Zusammenführung der Daten aus der ePA mit Registerdaten.

Mit Gesetzgebungsakten wie etwa dem Data Act[4] (DA) oder dem Data Governance Act[5] (DGA) sollen horizontale und sektorübergreifende Maßstäbe für den Zugang zu Daten gesetzt werden. Beide Verordnungen sollen den Datenaustausch fördern und erleichtern. Während der DGA Regelungen zur Weiterverwendung von Daten öffentlicher Stellen ohne Zugangsanspruch sowie Regelungen zu Datenvermittlungsdiensten und zum vom Gesetzgeber sogenannten »Datenaltruismus« enthält, beschäftigen sich die Vorschriften des DA unter anderem mit der sektorübergreifenden Bereitstellung von personenbezogenen und nicht personenbezogenen Daten.[6]

Speziell für den Austausch sogenannter »elektronischer Gesundheitsdaten«[7] soll außerdem ein europäischer Datenraum (European Health Data Space, EHDS) geschaffen werden, der als Blaupause für weitere Datenräume dienen soll. Nachdem die EU-Kommission im Mai 2022 einen Vorschlag für einen Verordnungstext (EHDS-VO-E) vorgelegt hat,[8] haben auch das Europäische Parlament (EHDS-VO-PE)[9] und der Rat (EHDS-VO-RE)[10] Vorschlagsänderungen erarbeitet.[11] Der Verordnungsentwurf ist zwar sektorspezifisch ausgerichtet, baut jedoch auf den sektorenübergreifenden DA und DGA auf[12] und regelt unter anderem die Sekundärnutzung von elektronischen Gesundheitsdaten für die dort festgelegten Zwecke.[13] Ungeklärt bleibt an vielen Stellen jedoch das Verhältnis des EHDS-VO-E zu schon bestehenden Regelungen im Hinblick auf den Zugang zu Forschungsdaten. Beispielsweise sollen die Regelungen der DS-GVO »unberührt« bleiben. Diese Formulierung klärt das Konkurrenzverhältnis der grundsätzlich gleichrangigen Verordnungen aber nicht und schafft insofern Rechtsunsicherheit.

---

4 Europäische Kommission 2023.

5 Europäische Kommission 2022a.

6 Siehe zum Regelungsinhalt des DA auch Specht-Riemenschneider 2022, S. 812 ff. und zum Regelungsgehalt von DGA und DA Specht-Riemenschneider 2023, S. 661 sowie Art. 1 Abs. 1 DA.

7 Siehe zum Begriff und zur Abgrenzung von Gesundheitsdaten im Sinne der DS-GVO die Ausführungen unter 2.1.

8 Europäische Kommission 2022b.

9 Europäisches Parlament 2023a.

10 Rat der Europäischen Union 2023.

11 Änderungen an den für den Text relevanten Gesetzestexten auf nationaler und europäischer Ebene konnten bis zum 13.03.2024 berücksichtigt werden.

12 EHDS-VO-E, S. 5.

13 Siehe Art. 2 Abs. 2 lit. e EHDS-VO-E und im Vergleich dazu die Begriffsbestimmung der Sekundärnutzung in § 2 Nr. 8 GDNG, der nicht explizit Daten enthält, die nur zum Zwecke der Sekundärnutzung erhoben wurden.

Auf Bundesebene wird die Sekundärnutzung von Versorgungsdaten zu Forschungszwecken insbesondere durch das am 14.12.2023 vom Bundestag verabschiedete Gesundheitsdatennutzungsgesetz (GDNG)[14] geregelt werden,[15] das unter anderem die Vorbereitung der Anbindung des deutschen Gesundheitswesens an den EHDS verfolgt.[16] Kern des Gesetzes ist die erleichterte Nutzbarkeit von Gesundheitsdaten für gemeinwohlorientierte Zwecke. Dazu wird unter anderem eine dezentrale Gesundheitsdateninfrastruktur mit einer zentralen Datenzugangs- und Koordinierungsstelle aufgebaut, die beim Bundesinstitut für Arzneimittel und Medizinprodukte eingerichtet wird. Flankiert wird das GDNG durch das Gesetz zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz DigiG),[17] welches schwerpunktmäßig die Einrichtung der ePA behandelt.[18]

Im Hinblick auf die stark überlappenden Regelungsgegenstände des GDNG und der EHDS-VO stellt sich die Frage, inwieweit für die Anwendung des GDNG bei Inkrafttreten der vollharmonisierenden Verordnung Raum bleibt. Dafür bedarf es einer Anordnung des Fortbestands einer nationalen Regelung oder einer Öffnungsklausel zugunsten der Mitgliedstaaten.[19] Diese Frage wird jedoch bei den folgenden Erwägungen ausgeklammert.

Einen Überblick über das Antragsverfahren nach dem GDNG gibt die folgende Grafik:

14 Siehe Deutscher Bundestag 2023a und 2023b.

15 Exemplarisch erwähnt seien speziell auf Bundesebene weiterhin das Krankenhauszukunftsgesetz (KHZG), das Patientendaten-Schutz-Gesetz (PDSG), das Digitale Versorgung-und-Pflege-Modernisierungs-Gesetz (DVPMG) und das Krankenhauspflegeentlastungsgesetz (KHPflEG), ohne dass diese Aufzählung einen Anspruch auf Vollständigkeit erhebt.

16 Siehe Deutscher Bundestag 2023a, S. 2.

17 Siehe Deutscher Bundestag 2023c und 2023d.

18 Vorausgegangen ist sowohl dem GDNG als auch dem DigiG die Verabschiedung des Gesetzes für eine bessere Versorgung durch Digitalisierung und Innovation (Digitale-Versorgung-Gesetz – DVG), siehe Deutscher Bundestag 2019.

19 Siehe ausführlich zum Anwendungsvorrang Roßnagel 2017, Rn. 1 ff.; Kumkar 2022, S. 492 f.

20 Prozessvisualisierung des Bundesministeriums für Gesundheit in: Deutscher Bundestag 2023a, S. 87.

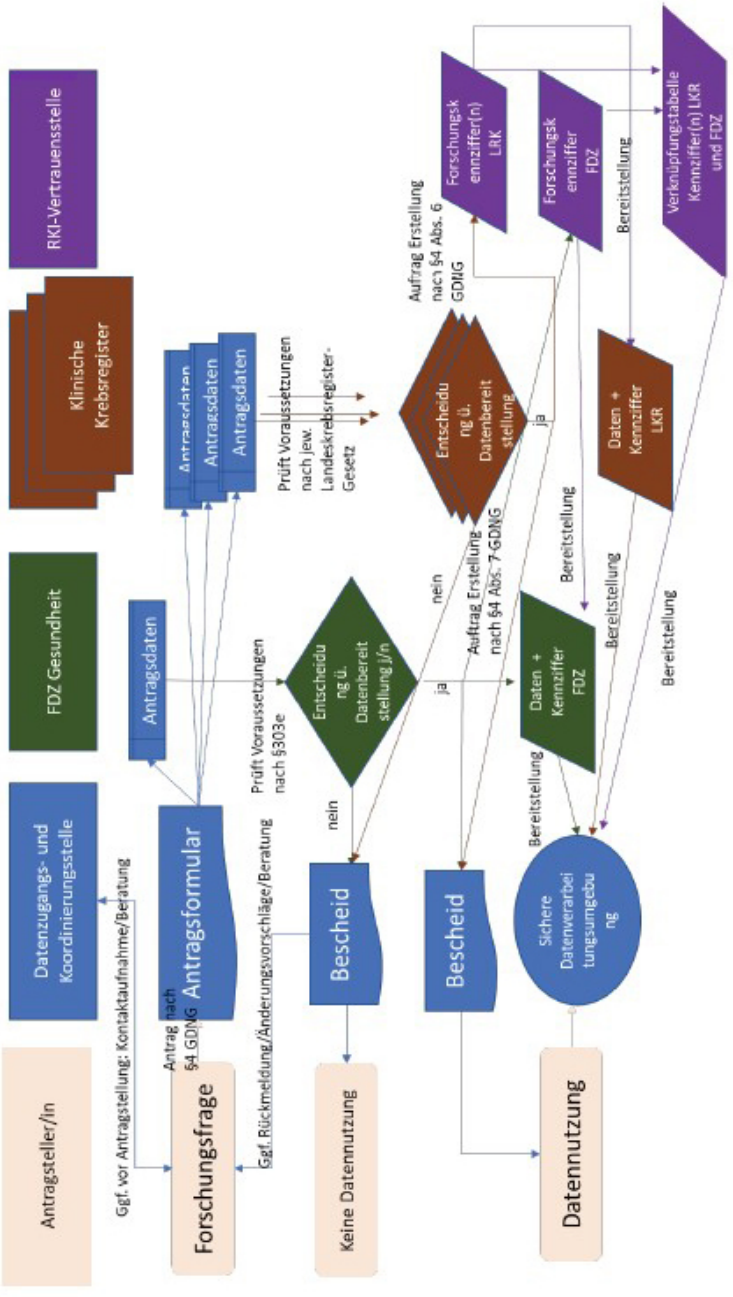

Abb.1: Überblick über den Ablauf des Antragsverfahrens nach dem GDNG[20]
Quelle: Deutscher Bundestag 2023a, S. 87

Bei den genannten europäischen Gesetzgebungsakten wird zwar die Verbesserung der Kontrollrechte der betroffenen Person, aber nicht zwangsläufig die Einwilligung hervorgehoben – das »klassische, verfassungsrechtlich legitimierte Instrument, um Eingriffe in Persönlichkeitsrechte zu gestatten« und das informationelle Selbstbestimmungsrecht umzusetzen.[21] Nach dem DA sollen Verbraucher mehr Kontrolle über ihre Daten erhalten,[22] und er zielt auf eine Förderung und Ausweitung des Rechts auf Datenübertragbarkeit und die damit verbundene Sicherstellung der Interoperabilität der Systeme ab. Auch der DGA nimmt auf verbesserte Handlungsfähigkeit und die Kontrolle der oder des Einzelnen über die ihn oder sie betreffenden Daten Bezug, etwa durch die Schaffung geeigneter Mechanismen, die es den betroffenen Personen ermöglichen, ihre Rechte zu kennen und effektiv wahrzunehmen.[23] Dies kann gleichermaßen technische Maßnahmen umfassen. Das allgemeine Ziel des EHDS-VO-E besteht darin, sicherzustellen, dass natürliche Personen in der EU in der Praxis mehr Kontrolle über ihre elektronischen Gesundheitsdaten erhalten.[24] Dagegen benennt der Entwurf des GDNG andere Ziele, etwa die schnellere Nutzbarmachung der im Forschungsdatenzentrum Gesundheit (FDZ Gesundheit) vorliegenden Abrechnungsdaten der gesetzlichen Krankenkassen, die erleichterte Verknüpfung von Gesundheitsdaten, die Vereinfachung der Abstimmungsverfahren mit den Datenschutzaufsichtsbehörden oder die umfassende und repräsentative Bereitstellung der Daten aus der ePA für die Forschung.[25] Die Stärkung des informationellen Selbstbestimmungsrechts wird vor allem im Zusammenhang mit einem Zeugnisverweigerungsrecht für mit Gesundheitsdaten Forschende und einem Beschlagnahmeverbot für Gesundheitsdaten diskutiert.

Daher stellt sich die Frage, inwieweit das informationelle Selbstbestimmungsrecht mit den genannten europäischen und nationalen Regulierungsvorhaben im Einklang steht und ob »verbesserte Kontrolle« auch zugleich eine Stärkung der Betroffenenrechte bedeutet. Aus datenschutzrechtlicher Sicht kann eine verbesserte Kontrolle mit einer Einwilligung assoziiert werden. Der Beitrag nimmt daher auf die Bedeutung der Einwilligung in den unterschiedlichen Rechtsakten Bezug, um darauf aufbauend generelle

21 Taeger 2022.

22 Siehe z. B. EG 33 und 102 DA.

23 Siehe z. B. EG 5, 23, 30, 32 und 33 DGA.

24 Siehe z. B. Art. 1 Abs. 2 lit. a EHDS-VO-E sowie die Ausführungen in den EG 1, 9, 16, 54, 67.

25 Siehe hierzu die Ausführungen des Gesetzgebers unter »A. Probleme und Ziele« im GDNG.

Überlegungen zur möglichen Architektur einer einwilligungsunabhängigen Nutzung am Beispiel von Patientendaten anzustellen, die dennoch das informationelle Selbstbestimmungsrecht und damit verbundene Kontrollrechte sicherstellt und stärkt. Insgesamt bedarf es eines Gerüsts, welches unter Wahrung des Verhältnismäßigkeitsgrundsatzes das europäische Grundrecht auf Datenschutz (Art. 8 GRCh) und die Interessen der Allgemeinheit gleichermaßen wahrt. Im Fokus der Untersuchung stehen daher ebenso die individuellen und kollektiven Zugangsmöglichkeiten bzw. -beschränkungen wie die Teilhabemöglichkeiten natürlicher und juristischer Personen mit Blick auf Forschungsdaten.

2. Gegenstand der Sekundärnutzung

Ein Datum kann grundsätzlich sowohl ein »Gesundheitsdatum« im Sinne der DS-GVO als auch ein elektronisches Gesundheitsdatum im Sinne des EHDS-VO-E sein. Anknüpfungspunkt für die Anwendbarkeit des jeweiligen Gesetzes ist daher der Regelungskontext sowie die damit zusammenhängende Prüfung, ob die jeweiligen gesetzlichen Voraussetzungen vorliegen. Auch das GDNG knüpft an den Begriff des Gesundheitsdatums im Sinne der DS-GVO an und stellt darüber hinaus klar, dass auch Sozialdaten im Sinne des § 67 Sozialgesetzbuch (SGB) X von dem Gesetz erfasst sein sollen. Die Definition, die auf ein Datum anwendbar ist, hat erhebliche Auswirkungen auf den Rechtsanwender.

2.1 Gesundheitsdaten im Sinne der Datenschutz-Grundverordnung

Sowohl Art. 2 Abs. 2 lit. c EHDS-VO-E als auch § 2 Nr. 1 GDNG beziehen sich auf Gesundheitsdaten im Sinne des Art. 4 Nr. 15 DS-GVO, der diese definiert als personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen. Sie zählen zu den besonderen Kategorien personenbezogener Daten, und es besteht ein grundsätzliches Datenverarbeitungsverbot nach Art. 9 Abs. 1 DS-GVO, es sei denn es gibt eine Rechtsgrundlage für die Datenverarbeitung. Eine mögliche Rechtsgrundlage ist die ausdrückliche Einwilligung in die Datenverarbeitung nach

Art. 9 Abs. 2 lit. a DS-GVO, für die erhöhte Anforderungen im Vergleich zu den Einwilligungsvoraussetzungen des Art. 7 DS-GVO in Verbindung mit Art. 4 Nr. 11 DS-GVO gelten.

2.2 Elektronische Gesundheitsdaten im Sinne der EHDS-VO-E

Elektronische Gesundheitsdaten im Sinne des Art. 2 Abs. 2 lit. c EHDS-VO-E setzen sich aus personenbezogenen elektronischen Gesundheitsdaten (Art. 2 Abs. 2 lit. a, c EHDS-VO-E) und nicht personenbezogenen elektronischen Gesundheitsdaten (Art. 2 Abs. 2 lit. b, c EHDS-VO-E) zusammen. Liegt kein Personenbezug vor, ist die DS-GVO und sind folglich Art. 4 Nr. 15 und Art. 9 Abs. 1 DS-GVO nicht anwendbar. Der Begriff der personenbezogenen elektronischen Gesundheitsdaten geht über die Definition von Gesundheitsdaten des Art. 4 Nr. 15 DS-GVO insofern hinaus, als auch Daten über Gesundheitsfaktoren und Daten im Zusammenhang mit der Erbringung von Gesundheitsdienstleistungen ausdrücklich erwähnt werden (siehe Art. 2 Abs. 2 lit. a EHDS-VO-E und Art. 33 Abs. 1 lit. b EHDS-VO-E) die nicht unbedingt von der Definition des Art. 4 Nr. 15 DS-GVO erfasst sind, sofern sie keinen tatsächlichen Rückschluss auf den Gesundheitszustand zulassen. Auch bei gesundheitsbezogenen Einflussfaktoren wie dem beruflichen Status oder dem Verhalten einer Person, s. EG 39 EHDS-VO-E liegt nicht zwangsläufig ein Gesundheitsdatum im Sinne von Art. 4 Nr. 15 DS-GVO vor. In welchem Verhältnis Gesundheitsfaktoren zu gesundheitsbezogenen Einflussfaktoren stehen, wird aus dem Entwurfstext nicht klar.[26] Weiterhin unklar bleibt, inwiefern die genannten Formulierungen nach dem Trilog noch in der EHDS-VO enthalten sein werden.[27]

In Art. 61 EHDS-VO-E wird wiederum festgelegt, dass nicht personenbezogene elektronische Daten, die auf elektronischen Daten einer natürlichen Person beruhen und unter eine der Kategorien des Art. 33 lit. a, e, f, i, j, k oder m EHDS-VO-E fallen, unter bestimmten Voraussetzungen als hoch-

26 Vgl. dazu auch die englische Fassung des Kommissionsentwurfs: EG 39 EHDS-VO-E: »data with an impact on health«, Art. 2 Abs. 2 lit a EHDS-VO-E: determinants of health, Art. 33 Abs. 1 lit. b EHDS-VO-E: data impacting on health, including social, environmental behavioural determinants of health.

27 Im Ratsentwurf wurden die Formulierungen »determinants of health« in Art. 2 Abs. 2 lit. a EHDS-VO-RE und »data impacting on health« in Art. 33 Abs. 1 lit. b EHDS-VO-RE hingegen gestrichen.

sensibel im Sinne von Art. 5 Abs. 13 DGA gelten.[28] Die in Art. 5 Abs. 13 DGA erwähnten hochsensiblen Daten sind ebenso wie die in Art. 61 EHDS-VO-E geregelten Daten nicht personenbezogen,[29] sodass sie keine Gesundheitsdaten im Sinne von Art. 4 Nr. 15 DS-GVO sein können.

2.3 Gesundheits- und Sozialdaten im Sinne des Gesundheitsdatennutzungsgesetz

§ 2 Nr. 1 GDNG verweist bezüglich der Definition von Gesundheitsdaten auf Art. 4 Nr. 15 DS-GVO, enthält jedoch den ausdrücklichen Zusatz, dass auch Gesundheitsdaten erfasst sein sollen, die zugleich Sozialdaten nach § 67 SGB X sind.

Sozialdaten sind in § 67 Abs. 2 S. 1 SGB X legaldefiniert als personenbezogene Daten im Sinne des Art. 4 Nr. 1 DS-GVO, die von einer in § 35 SGB I genannten Stelle im Rahmen ihrer Aufgabenerfüllung verarbeitet werden. Die Eigenschaft der Sozialdaten ist mithin vor allem davon abhängig, wer die Daten verarbeitet. Dabei ist jedoch zu beachten, dass die Verarbeitung durch eine in § 35 SGB I genannte Stelle zwar konstitutiv ist, diese »qualifizierte Form«[30] der personenbezogenen Daten jedoch bestehen bleibt, wenn sie einmal vorhanden war.[31]

Medizinische Sozialdaten können darüber hinaus zugleich Gesundheitsdaten im Sinne des Art. 4 Nr. 15 DS-GVO sein,[32] wenn die entsprechenden

---

28 Sofern ihre Übertragung in Drittländer angesichts der begrenzten Zahl der an diesen Daten beteiligten natürlichen Personen, der geografischen Streuung oder der in naher Zukunft zu erwartenden technologischen Entwicklungen das Risiko einer Rekonstruktion der Identität birgt. EG 19 DGA enthält Ausführungen dazu, dass im übrigen Unionsrecht festgelegt werden sollte, welche nicht personenbezogenen öffentlichen Daten als hochsensibel gelten und erwähnt dabei ausdrücklich auch den europäischen Gesundheitsdatenraum als ein Beispiel. Die Maßnahmen zum Schutz dieser »hochsensiblen« Daten werden in dem delegierten Rechtsakt nach Art. 15 Abs. 3 DGA festgelegt, Art. 61 Abs. 2 EHDS-VO-E.

29 Art. 5 Abs. 13 DGA regelt etwa, dass nach besonderen Rechtsakten der Union bestimmte Kategorien nicht personenbezogener Daten, die im Besitz öffentlicher Stellen sind, als hochsensibel gelten können, wenn die Übertragung dieser Daten in Drittländer Ziele des Gemeinwohls der Union, beispielsweise in den Bereichen Sicherheit und öffentliche Gesundheit, gefährden könnte oder die Gefahr einer erneuten Identifizierung anhand nicht personenbezogener, anonymisierter Daten birgt.

30 Fromm 2023, Rn. 65; Leopold 2022, Rn. 98.

31 Siehe Leopold 2022, Rn. 100.

32 Westphal 2023, Rn. 6.

Voraussetzungen der DS-GVO vorliegen. Dagegen sind Gesundheitsdaten im Sinne der DS-GVO nicht automatisch auch Sozialdaten im Sinne des § 67 Abs. 2 S. 1 SGB X.[33]

2.4 Zwischenergebnis

Nach der Definition in § 67 Abs. 2 S. 1 SGB X liegen nur dann Sozialdaten vor, wenn die entsprechenden Daten personenbezogene Daten im Sinne des Art. 4 Nr. 1 DS-GVO sind. Gesundheitsdaten im Sinne des GDNG können demnach sowohl personenbezogene Daten sein, die von einer in § 35 SGB I genannten Stelle verarbeitet werden, als auch personenbezogene Daten, die nicht von einer in § 35 SGB I genannten Stelle verarbeitet werden.

Der EHDS-VO-E erfasst mit den nicht personenbezogenen elektronischen Gesundheitsdaten auch Daten, bei denen der für die Anwendbarkeit der DS-GVO notwendige Personenbezug nicht vorhanden ist, wovon etwa anonymisierte Daten aus elektronischen Patientenakten umfasst sein können. Andererseits geht die Definition der personenbezogenen Gesundheitsdaten über die Definition von »Gesundheitsdaten« in der DS-GVO hinaus. Der Rechtsanwender muss insofern genau prüfen, ob neben den Vorschriften des EHDS-VO-E gleichermaßen die Vorschriften der DS-GVO anzuwenden sind, die jedoch einen Personenbezug voraussetzen. Dies gilt insbesondere für Rechtsanwender, die sowohl den Regelungen der kommenden EHDS-VO als auch denen des GDNG unterliegen.[34]

3. Individuelle Kontroll- und Einflussmöglichkeiten

Aus Sicht der natürlichen Person, die zugleich eine betroffene Person im Sinne der DS-GVO sein kann, stellt sich die Frage, inwiefern aus individueller Ebene Kontrolle über die Datenverarbeitung ausgeübt, bzw. Einfluss auf die Datenverarbeitung genommen werden kann.

---

33 Siehe auch Leopold 2022, Rn. 40.

34 Wobei insgesamt fraglich ist, inwieweit bei Inkrafttreten der EHDS-VO noch Raum für die Anwendungen des GDNG bleibt.

3.1 Die Einwilligung in die Sekundärnutzung von Gesundheitsdaten zu Forschungszwecken

Eine Möglichkeit des Individuums, Kontrolle über die Verarbeitung der eigenen Daten auszuüben, ist die Entscheidung, ob in die Datenverarbeitung eingewilligt werden soll.

3.1.1 Einwilligung im Sinne der Datenschutz-Grundverordnung

In der Vorstellung, die den Vorschriften der DS-GVO zugrunde liegt, hat die betroffene Person die Möglichkeit, die Kontrolle über die sie betreffenden personenbezogenen Daten insbesondere dadurch auszuüben, dass sie in den Fällen, in denen keine andere Rechtsgrundlage für die Datenverarbeitung vorliegt, durch die Einwilligung eine Rechtsgrundlage schaffen kann. Der Einwilligung wird teilweise eine überragende Bedeutung zugeschrieben.[35] Allerdings steht sie auf gleicher Stufe mit den übrigen Erlaubnistatbeständen der Art. 6 und 9 DS-GVO. Darüber hinaus ist sie in ihrer Umsetzung stets mit Schwierigkeiten behaftet. Separate Einwilligungserklärungen mit langen Informationstexten sind oftmals sowohl für Unternehmen als auch NutzerInnen gleichermaßen unpraktisch. Dies gilt ebenso für den Klinikbetrieb.

Für wissenschaftliche Zwecke erfolgt zwar eine Privilegierung v.a. hinsichtlich Zweckbindung und Speicherdauer, und es wird teilweise auf eine so genannte »breite« Einwilligungsmöglichkeit verwiesen.[36] Aus Art. 5 Abs. 1 lit. b DS-GVO ergibt sich allerdings nur, dass unter Berücksichtigung von Art. 89 Abs. 1 DS-GVO Daten für Forschungszwecke unter bestimmten Bedingungen weitergenutzt werden dürfen. Die Formulierung »breite Einwilligung« findet sich in der DS-GVO nicht. Der Europäische Datenschutzausschuss nimmt in diesem Zusammenhang auf EG 33 DS-GVO Bezug, der unter bestimmten Umständen die Möglichkeit eröffnet, die Spezifizierung der Einwilligung flexibler abzuschwächen, indem diese für »bestimmte Bereiche wissenschaftlicher Forschung«[37] gegeben werden

35 Siehe z. B. Taeger 2022, Rn. 2 und Frenzel 2021, Rn. 1 f.

36 Siehe kritisch dazu Fröhlich/Spiecker gen. Döhmann 2022; demgegenüber Graf von Kielmansegg 2023; siehe ausführlich zum broad consent mit einem Schwerpunkt auf der Genomforschung Hallinan 2020.

37 EDSA 2020, Rn. 154.

kann, sich also offenbar nicht auf ein spezifisches Einzelforschungsvorhaben beziehen muss. Darauf basierend verweist der Europäische Datenschutzausschuss auch auf Verfahren, um die Transparenz der Verarbeitung während des Forschungsprojekts zu erhöhen, z. B. um die Einwilligung zurückziehen oder präzisieren zu können.[38] In diesem Sinne hat die Medizininformatik-Initiative ein modular aufgebautes Einwilligungsformular für klinische Studien unter Einbeziehung von Datenschutzaufsichtsbehörden entwickelt, das unter anderem eine zeitliche Befristung der Einwilligung von fünf Jahren vorsieht.[39] Grundvoraussetzungen sind dabei, neben der Einwilligungserklärung, die ausführliche Information der Betroffenen, die Freiwilligkeit der Einwilligung sowie ihre jederzeitige Widerrufbarkeit.

3.1.2 Die Einwilligung in DA, DGA und EHDS-VO-E

Weder im DGA noch im DA kommt der Einwilligung eine überragende Rolle zu, wenngleich der DGA zumindest eine abgestimmte europäische Vorgehensweise im Rahmen der Nutzung von Daten für Ziele im allgemeinen Interesse, wie etwa die Gesundheitsversorgung (sogenannter »Datenaltruismus«), hinsichtlich der Einwilligungserklärungen vorsieht, s. Art. 25 DGA.[40] Im Rahmen der Sekundärnutzung, wie sie im EHDS-VO-E geregelt ist, ist die Einwilligung allerdings gänzlich bedeutungslos. Der Zugang zu elektronischen Gesundheitsdaten in Art. 34 EHDS-VO-E wird nur von den dort genannten Zwecken,[41] nicht aber von der Einwilligung der betroffenen Person abhängig gemacht. Dagegen sieht Art. 33 Abs. 5a EHDS-VO-PE ausdrücklich vor, dass die »Zweitnutzung«[42] (»secondary use«) bestimmter Daten[43] von der Einwilligung der natürlichen Person anhängig gemacht wird.

---

38 Ebd., Rn. 156 ff.

39 Medizininformatik-Initiative, Mustertext Patienteneinwilligung, V. 1.6d; zustimmend dazu DSK 2020.

40 Brieske/Schweitzer betonen in ihrem Beitrag in diesem Band das Ziel des DA, die generierten Daten von einzelnen, marktmächtigen Unternehmen zu lösen und damit eine insgesamt gerechtere Zugänglichkeit und Nutzbarkeit der Daten zu gewährleisten.

41 Siehe im Hinblick auf die Zwecke der Datenverarbeitungen die Ausführungen unter 4.

42 Gemeint ist mangels anderweitiger Anhaltspunkte und vor dem Hintergrund der englischen Sprachfassung, die sich auf den »secondary use« bezieht, wohl die Sekundärnutzung.

43 Genauer von Auszügen aus humangenetischen, genomischen und proteomischen Daten wie etwa genetische Marker, Art. 33 Abs. 1 lit. e EHDS-VO-PE, Daten aus Wellness-Anwendungen, Art. 33 Abs. 1 lit. fa EHDS-VO-PE und elektronischen Gesundheitsdaten aus Biobanken und speziel-

Werden die elektronischen Gesundheitsdaten lediglich pseudonymisiert verarbeitet, sodass ein Personenbezug hergestellt werden kann und der Anwendungsbereich der DS-GVO eröffnet ist, so kommt für die Datenverarbeitung zwar die Einwilligung als Rechtsgrundlage in Betracht. Sie ist indes dann nicht nötig, wenn die Vorschriften des EHDS-VO-E taugliche Rechtsgrundlagen im Sinne von Art. 6 Abs. 1 DS-GVO bzw. Art. 9 Abs. 2 DS-GVO darstellen.[44]

3.1.3 Die Bedeutung der Einwilligung im Gesundheitsdatennutzungsgesetz

Im Rahmen des GDNG und der in diesem Zusammenhang erfolgten Änderungen des SGB V hat die Einwilligung in die Datenverarbeitung ebenfalls keine herausragende Bedeutung. So verdeutlicht z. B. der neu eingefügte § 25b SGB V n.F.,[45] dass die versicherte Person in die Datenverarbeitung durch die Kranken- und Pflegekassen nicht einwilligen muss, sofern einer der dort aufgezählten Zwecke vorliegt und die Datenverarbeitung dem Gesundheitsschutz dient. Der Gesetzgeber stellt an dieser Stelle auf ein Widerspruchsrecht der versicherten Person ab.[46] Hervorzuheben ist, dass von der Datenverarbeitung ebenso Daten der elektronischen Patientenakte umfasst sind. In diesem Sinne regelt § 363 Abs. 2 SGB V n.F., dass die Daten an das FDZ Gesundheit nach § 303d SGB V automatisiert übermittelt und dabei automatisiert pseudonymisiert werden. § 363 Abs. 1 SGB V a.F. erlaubte bislang die Freigabe der Daten der elektronischen Patientenakte an das FDZ Gesundheit nur beim Vorliegen einer informierten Einwilligung der oder des Versicherten. § 363 SGB V n.F. regelt hingegen, dass die Daten der elektronischen Patientenakte für die in § 303e Abs. 2 SGB V n.F. aufgeführten Zwecke zugänglich gemacht werden, soweit Versicherte nicht der Datenübermittlung nach § 363 Abs. 5 SGB V n.F. widersprochen haben.[47]

Daher sind auch aufgrund der geplanten Änderungen im SGB V n.F. nun insgesamt vielfältige und bislang nicht erfasste Nutzungsmöglichkeiten von

---

len Datenbanken, Art. 33 Abs. 1 lit. m DS-GVO; soweit ersichtlich enthält das Verhandlungsmandat des Europäischen Rates keine vergleichbare Einschränkung.

44 Siehe dazu die Ausführungen unter 4.1.

45 Art. 3 Nr. 2 GDNG.

46 Siehe dazu insbesondere § 25 Abs. 3 SGB V n.F.; generell zur Kritik am § 25b SGB V n.F. z. B. Moreno 2023 und BfDI 2023, S. 4.

47 Siehe zur Änderung von § 363 Abs. 5 SGB V n.F. durch den Ausschuss für Gesundheit die Ausführungen unter 3.2.3 Fn. 65.

Gesundheitsdaten denkbar.[48] Zu berücksichtigen ist in diesem Zusammenhang ebenso, dass digitale Gesundheitsanwendungen ab dem 01.01.2024 so zu gestalten sind, dass die von ihnen verarbeiteten Daten in die elektronische Patientenakte des Versicherten nach § 341 SGB V übermittelt werden können (§ 6a – Digitale Gesundheitsanwendungen-Verordnung (DiGAV) – derzeit noch auf der Basis einer Einwilligung, wobei aber auch hier eine Widerspruchslösung grundsätzlich denkbar wäre.[49]

3.2 Betroffenenrechte

Nicht nur die Einwilligung in die Datenverarbeitung ist eine Möglichkeit zur Ausübung des informationellen Selbstbestimmungsrechts. Der nachträglichen Einwirkungsmöglichkeit auf Datenverarbeitungsvorgänge liegt gleichermaßen die Vorstellung zugrunde, dass das Individuum selbstbestimmt über die Datenverarbeitung entscheiden können soll.[50] Wenngleich die DS-GVO der betroffenen Person grundsätzlich verschiedene Betroffenenrechte einräumt, besteht teilweise die gesetzliche Möglichkeit, diese zu beschränken (siehe nachfolgend unter 3.2.1). So könnte die Datenbasis für eine kontinuierliche Forschung sichergestellt werden.

3.2.1 Einschränkung der Betroffenenrechte in der Datenschutz-Grundverordnung

Die Gesetzgeber der Mitgliedstaaten und der Union haben die Möglichkeit, die Betroffenenrechte nach Art. 23 DS-GVO einzuschränken. Art. 23 Abs. 1 lit. e DS-GVO bezieht sich in diesem Zusammenhang auf den Schutz wichtiger Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaats, auch im Bereich der öffentlichen Gesundheit und der sozialen Sicherheit. Art. 23 Abs. 1 lit. i DS-GVO erlaubt Beschränkungen für den Schutz der betroffenen Person oder der Rechte und Freiheiten anderer Personen. Bei der zuletzt genannten Regelung muss allerdings berücksichtigt werden, wer letztendlich durch die Maßnahmen geschützt

48 Siehe hierzu die Ausführungen unter 4.2.2.

49 Nach EG 19 DGA sollen zwar keine Daten aus e-Gesundheitsanwendungen weiterverwendet bzw. die Weiterverwendung von öffentlichen Stellen nicht gestattet werden. Dies bezieht sich jedoch nur auf den Zweck der Diskriminierung bei der Festlegung von Preisen.

50 Siehe z. B. Koch/Chatard 2022.

wird. Die sehr weit gefasste Vorschrift des Art. 23 Abs. 1 lit e DS-GVO[51] erfordert das Vorliegen eines öffentlichen Interesses von besonderem Gewicht,[52] das den datenschutzrechtlichen Interessen der betroffenen Person vorgeht.[53] Der Begriff der öffentlichen Gesundheit, der sich ausweislich der Erwägungen in EG 54 DS-GVO an der VO (EG) Nr. 1338/2008 und dort an Art. 3 lit. c orientiert, umfasst alle Elemente im Zusammenhang mit der Gesundheit. Der Schutz der öffentlichen Gesundheit kann also grundsätzlich als Möglichkeit der Einschränkung der Betroffenenrechte herangezogen werden, sofern die übrigen Voraussetzungen des Art. 23 DS-GVO erfüllt sind, also insbesondere das öffentliche Interesse von besonderem Gewicht die datenschutzrechtlichen Interessen der Betroffenen überwiegen.

Soll der Verantwortliche vor unverhältnismäßigen Belastungen geschützt werden, käme außerdem die Öffnungsklausel des Art. 89 Abs. 2 DS-GVO mit Blick auf Forschungszwecke in Betracht, der die Möglichkeit eröffnet, bestimmte Betroffenenrechte einzuschränken, wenn diese Rechte voraussichtlich die Verwirklichung der spezifischen Zwecke unmöglich machen oder ernsthaft beeinträchtigen und solche Ausnahmen für die Erfüllung der Zwecke notwendig sind. Die weite Auslegung des Forschungsbegriffs erfasst dabei grundsätzlich auch die kommerzielle Forschung,[54] die inhaltlich auch in Art. 34 Abs. 1 lit. f-h EHDS-VO-E als zulässiger Zweck des Zugangs zu den elektronischen Gesundheitsdaten neben der wissenschaftlichen Forschung, Art. 34 Abs. 1 lit. e EHDS-VO-E, vorgesehen ist.

3.2.2 Rechte der Individuen im europäischen Gesundheitsdatenraum

In dem EHDS-VO-E sind im Hinblick auf die Sekundärnutzung keine eigenständigen Betroffenenrechte normiert.[55] Allerdings bestehen die Daten der Sekundärnutzung nach Art. 2 Abs. 2 lit. e S. 2 EHDS-VO-E zum einen aus personenbezogenen elektronischen Gesundheitsdaten, die zunächst im Rahmen der Primärnutzung erhoben wurden und zum anderen aus elektronischen Gesundheitsdaten, also personenbezogenen und nicht per-

51 Siehe kritisch hierzu unter anderem Dix 2019, Rn. 27, der von einem »Blankettcharakter« spricht; Grages 2023, Rn. 1; Paal 2021, Rn. 31a.; Bäcker 2024, Rn. 22.

52 Siehe Paal 2021, Rn. 31a; Dix 2019, Rn. 27; für eine enge Auslegung auch Herbst 2024, Rn. 15.

53 Siehe Peuker 2022, Rn. 25.

54 Siehe Grages 2023, Rn. 6; siehe hierzu aber auch die Ausführungen unter 4.1.1.

55 Kritisch dazu zum Beispiel DSK 2023, S. 2.

sonenbezogenen Gesundheitsdaten, die zum Zwecke der Sekundärnutzung erhoben wurden.

3.2.2.1 Betroffenenrechte im Rahmen der Primärnutzung

Bezüglich der Daten, die im Rahmen der Primärnutzung erhoben wurden, fällt zunächst auf, dass es sich dabei um personenbezogene elektronische Gesundheitsdaten handelt. Liegt ein Personenbezug vor, ist beim Vorliegen der weiteren Voraussetzungen die DS-GVO anwendbar, sodass auf die dortigen Betroffenenrechte zu verweisen ist. Darüber hinaus gewährt aber auch der Art. 3 EHDS-VO-E der natürlichen Person Rechte hinsichtlich der Primärnutzung ihrer personenbezogenen elektronischen Gesundheitsdaten mit einem engen Bezug zu den Betroffenenrechten der DS-GVO, die zum Teil erweitert werden.[56] Diese Rechte erweitern insbesondere das Auskunftsrecht (Art. 15 DS-GVO) und das Recht auf Datenübertragbarkeit (Art. 20 DS-GVO), indem betroffenen Personen das Recht eingeräumt wird, sofort, kostenlos und in einem leicht lesbaren, gängigen und zugänglichen Format auf die Daten aus der Primärnutzung zuzugreifen. Hinzu treten weitere Rechte. So soll beispielsweise das Recht auf Berichtigung aus Art. 16 DS-GVO bezüglich der zur Primärnutzung verarbeiteten elektronischen Gesundheitsdaten über die in Art. 3 Abs. 5 lit. a EHDS-VO-E genannten Zugangsdienste für elektronische Gesundheitsdaten online beantragt werden können, s. Art. 3 Abs. 7 EHDS-VO-E.

In dem Vorschlag der Europäischen Kommission wird ebenso im Rahmen der Primärnutzung den natürlichen Personen kein Widerspruchsrecht eingeräumt. Dagegen befürworten – mittlerweile – sowohl das Europäische Parlament,[57] als auch der Rat[58] die Möglichkeit der Mitgliedstaaten, ein Widerspruchsrecht für natürliche Personen einzuführen, was die Betroffenenrechte der PatientInnen erheblich stärken würde.[59]

---

56 Kritisch zur nicht vollständigen Übereinstimmung z. B. EDSA/ EDSB 2022, S. 18 f.

57 Siehe Europäisches Parlament 2023a; siehe aber zur ursprünglichen Position des Parlaments Europäisches Parlament 2023b.

58 Siehe Rat der Europäischen Union 2023, Art. 8 f Abs. 1, S. 71 der jedoch eine Einschränkung für die erforderliche Verarbeitung von Gesundheitsdaten zum Schutz lebenswichtiger Interessen im Sinne von Art. 9 Abs. 2 lit. c DS-GVO enthält.

59 Siehe zum Widerspruchsrecht im Rahmen der Sekundärnutzung auch DSK 2023, S. 6; kritisch zum fehlenden Widerspruchsrecht gegen die Sekundärnutzung von Gesundheitsdaten und zum Verhältnis von EHDS-VO-E und DS-GVO z. B. Gassner 2022, S. 744 f.; siehe auch Bronner 2023, Anm. 2.

Jedoch könnte es schon durch den Widerspruch gegen die Primärnutzung der Daten in Bezug auf die Nutzbarkeit der Daten für die Sekundärnutzung zu Verzerrungen kommen, wenn man davon ausgeht, dass bestimmte Bevölkerungsgruppen der Verarbeitung ihrer Daten eher widersprechen werden, oder gar einzelne Mitgliedstaaten von dieser Öffnungsklausel Gebrauch machen, während andere dies nicht tun.

3.2.2.2 Eigene Betroffenenrechte im Rahmen der Sekundärnutzung?

Der Verordnungsentwurf der Kommission sieht keine eigene Betroffenenrechte spezifisch im Hinblick auf die Sekundärnutzung der Daten vor. Will man sich gegen eine Sekundärnutzung mit den Mitteln des EHDS-VO-E wehren, so käme nur die Ausübung der Betroffenenrechte im Rahmen der Primärnutzung in Betracht, was aber im Falle des Widerspruchsrechts dem Interesse der PatientInnen entgegenstehen könnte, von den Vorteilen der ePA in der Versorgung zu profitieren.

Unter diesem Gesichtspunkt ist der Verordnungsvorschlag des Europäischen Parlaments zu begrüßen, der in Art. 33 Abs. 5 S. 1 EHDS-VO-PE das Recht der natürlichen Person vorsieht, der Sekundärnutzung der Daten zu widersprechen. Der Widerspruch kann sich auf bestimmte Zwecke der Sekundärnutzung beziehen.[60] Auch der Vorschlag des Rates enthält in Art. 35F EHDS-VO-RE das Recht der natürlichen Person, der Datenverarbeitung zur Sekundärnutzung zu widersprechen, wobei sowohl das Ob des Widerspruchs als auch die Einzelheiten den Mitgliedstaaten überlassen werden.[61]

Wegen der grundsätzlichen Gleichrangigkeit der DS-GVO und des EHDS-VO-E stehen den betroffenen Personen damit weiterhin grundsätzlich die Betroffenenrechte der DS-GVO zu, sofern diese anwendbar ist. Damit ist die betroffene Person bezüglich ihrer Betroffenenrechte gegebenenfalls einem Umstand ausgesetzt, den sie selbst nicht unmittelbar beeinflussen kann. Werden die Daten z. B. anonymisiert verarbeitet, findet die DS-GVO keine Anwendung, und der natürlichen Person stehen – abhängig von den Ergebnissen des Trilogs – gegebenenfalls keine Betroffenenrechte im Hinblick auf die Sekundärnutzung mehr zu. Allerdings lässt sich durchaus die

60 Siehe Europäisches Parlament 2023a, Abänderung 311.
61 Rat der Europäischen Union 2023, S. 116.

Frage aufwerfen, inwiefern die Schutzwürdigkeit der natürlichen Person bei der vollständigen Anonymisierung noch gegeben ist.

Hervorzuheben ist in diesem Zusammenhang, dass der Sachverständigenrat zur Begutachtung der Entwicklung im Gesundheitswesen und in der Pflege die Weiterentwicklung von Einwilligungsverfahren dahingehend empfohlen hat, dass eine Sekundärnutzung von Behandlungsdaten im Interesse des Patientenwohls niederschwellig, unkompliziert und möglichst entkoppelt von der konkreten Behandlungssituation geregelt werden sollte. In diesem Sinne sollte – so der Sachverständigenrat – vorrangig geprüft werden, ob für Versorgungsdaten, die als besonders relevant für die Gesundheitsforschung gelten, auf Basis von Art. 9 Abs. 2 DS-GVO die Möglichkeit einer Verarbeitung auf gesetzlicher Grundlage ohne Zustimmungserfordernis oder Opt-out-Möglichkeit geschaffen werden kann.[62]

3.2.3 Betroffenenrechte im Gesundheitsdatennutzungsgesetz

Das GDNG kann hinsichtlich der Betroffenenrechte nicht betrachtet werden, ohne vorweg die Regelungen im Digital-Gesetz (DigiG)[63] zur Einrichtung einer ePA zu betrachten. Bei Daten, die von vornherein nicht an die ePA übermittelt werden, kommt auch keine Sekundärnutzung der Daten in Betracht, zumal der Gesetzgeber im GDNG keine Datenerhebung nur zum Zwecke der Sekundärnutzung vorsieht. Im DigiG sind im Rahmen der Primärnutzung von Daten in der Versorgung an zahlreichen Stellen Widerspruchsmöglichkeiten für die PatientInnen vorgesehen.[64]

Für die im GDNG geregelte Sekundärnutzung der Daten sieht dieses separate Widerspruchsmöglichkeiten gegen die Nutzung der Daten aus der ePA vor, § 363 Abs. 5 SGB V n.F. Der Widerspruch kann über die Benutzeroberfläche eines geeigneten Endgerätes oder gegenüber einer neu zu schaffenden Ombudsstelle gemäß § 342a SGB V n.F. geltend gemacht werden.[65]

---

62 Sachverständigenrat zur Begutachtung der Entwicklung im Gesundheitswesen und in der Pflege 2021, Teilziffer 23.

63 Deutscher Bundestag 2023c, in der 3. Lesung vom Bundestag angenommen am 14.12.2023.

64 Siehe z. B. schon gegen die Einrichtung der ePA in Art. 1 Nr. 44 lit. a DigiG (§ 342 Abs. 1 S. 2 SGB V n.F.) oder gegen die Datenübermittlung in die ePA in Art. 1 Nr. 44 lit. b DigiG (§ 342 Abs. 2 Nr. 1 lit. g und h SGB V n.F.); eine ausführliche Auseinandersetzung mit dem Opt-Out-Modell der ePA ist zu finden bei Lorenz 2023a und 2023b, siehe für einen kurzen Überblick auch Dochow 2022.

65 Siehe dazu und zur Erklärung des Widerspruchs gegenüber einer Ombudsstelle die Änderungen in Deutscher Bundestag 2023b, § 342a SGB V n.F. wurde in der Beschlussempfehlung und

Weitere Rechte der PatientInnen bezüglich der Datenverarbeitung im FDZ Gesundheit sind nicht vorgesehen, was schon bezüglich der in Rede stehenden Verfassungswidrigkeit der Datenverarbeitung im FDZ Gesundheit problematisch ist.[66] Die pseudonymisierte Verarbeitung der Daten im FDZ Gesundheit führt dazu, dass diese keine Möglichkeiten haben, die Kennziffer ihrer Daten zu erfahren. Sie können also ihre Betroffenenrechte aus der DS-GVO faktisch gar nicht ausüben.[67]

3.2.4 Zwischenergebnis

Die Einflussmöglichkeiten der natürlichen Person auf die Datenverarbeitung zu Primär- und Sekundärzwecken werden reduziert. Auf individueller Ebene ist es kaum noch möglich, die Datenverarbeitung den eigenen Bedürfnissen feingranular anzupassen. Zu berücksichtigen ist dabei, dass Daten, die das Verhalten und den Zustand, insbesondere den Gesundheitszustand einer Person beschreiben, tiefe Einblicke in deren Persönlichkeit zulassen, und daher keine belanglosen Daten sind, nicht unter den modernen Bedingungen der Datenverarbeitung. Entscheidend sind vielmehr ihre Nutzbarkeit und Verwendungsmöglichkeit.[68] Aus diesen Überlegungen folgt, dass es in den Zeiten moderner, vernetzter Datenverarbeitung besonderer Maßnahmen bedarf, um das informationelle Selbstbestimmungsrecht der oder des Einzelnen sicherzustellen.[69] In erster Linie ist hier der Gesetzgeber gefordert, obgleich dies nicht die Einzelne oder den Einzelnen von

---

Bericht des Ausschusses für Gesundheit zum DigiG neu eingefügt, Deutscher Bundestag 2023d. Gestrichen wurde in der Beschlussempfehlung des Ausschusses für Gesundheit die gesonderte Informationspflicht der Krankenkassen nach § 363 Abs. 5, S. 5 SGB V n.F. Dies vor allem mit dem Hinweis darauf, dass die die Nutzbarmachung der ePA-Daten nach § 363 SGB V aufgrund der neuen Sicherheitsarchitektur nicht mehr an die Nutzung eines Frontends gekoppelt sei und so eine zusätzliche Information bei erstmaliger Öffnung der Anwendung entbehrlich sei, siehe Deutscher Bundestag 2023b, S. 63 f. die Information der Versicherten durch die Krankenkassen soll nunmehr nach dem im DigiG neu eingeführten § 343 Abs. 1a Nr. 21 SGB V n.F. vor der Zurverfügungstellung der ePA erfolgen, siehe Deutscher Bundestag 2023d, S. 65 f.

66 Siehe dazu z. B. Weichert 2020b, S. 539 ff.; Netzwerk Datenschutzexpertise 2023b, S. 9; Netzwerk Datenschutzexpertise 2023a, S. 8.

67 Siehe z. B. Netzwerk Datenschutzexpertise 2023b, S. 9; siehe zu den Einzelheiten über das Lieferpseudonym auch Ziegler 2019, Rn. 247a f.

68 BVerfG, Urteil vom 15.12.1983 – 1 BvR 209/83 u.a. – BVerfGE 65, 1 43 ff.

69 Siehe hierzu die Ausführungen unter 6.

der Notwendigkeit entbindet, den eigenen Umgang mit Daten kritisch zu reflektieren.

4. Einwilligungsunabhängige Rechtsgrundlagen der Datenverarbeitung

Die Verarbeitung von Gesundheitsdaten kann auf verschiedene Rechtsgrundlagen gestützt werden. Wenngleich die augenfälligste Rechtsgrundlage die Einwilligung in die Datenverarbeitung darstellt, kommen gleichermaßen die weiteren in Art. 9 Abs. 2 DS-GVO genannten Rechtsgrundlagen in Betracht. Dabei ist zu beachten, dass zugleich eine Rechtsgrundlage nach Art. 6 DS-GVO vorliegen muss.[70]

4.1 Anforderungen an die Rechtsgrundlagen für die Verarbeitung von Sekundärdaten

4.1.1 Ausnahmen vom Verarbeitungsverbot

In Art. 9 Abs. 2 DS-GVO sind Ausnahmen vom Verarbeitungsverbot des Art. 9 Abs. 1 DS-GVO geregelt, z. B. die Verarbeitung für Zwecke der Gesundheitsversorgung (lit. h), aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit (lit. i) oder zu Forschungszwecken (lit. j). Dabei handelt es sich um Öffnungsklauseln, die dem Gesetzgeber ermöglichen, eigenständige Regelungen in diesem Bereich zu treffen. Das Merkmal der Erforderlichkeit, auf das sich die Ausnahmetatbestände des Art. 9 Abs. 2 lit. g bis lit. j DS-GVO und des Art. 6 Abs. 1 DS-GVO[71] beziehen, ist ein unionsrechtlich autonomer Begriff, der vom Europäischen Datenschutzausschuss eng ausgelegt wird, und zwar im Sinne einer objektiven, faktengestützten Erforderlichkeit.[72] Teilweise wird eine Abwägung mit dem möglichen Datenschutzrisiko (vgl. etwa Art. 9 Abs. 2 lit. g DS-GVO) oder eine gesetzliche Regelung des öffentlichen Interesses (vgl. Art. 9 Abs. 2 lit. i DS-GVO) verlangt. Beim zuletzt genannten Tatbestand

70 Siehe Petri 2019, Rn. 3; EuGH, Urteil C-667/21 vom 21.12.2023, Rn. 78 f.
71 Siehe zum »übergreifenden Prinzip der Erforderlichkeit« in Art. 6 Buchner/Petri 2024, Rn. 15.
72 EDSA 2019, S. 10.

des öffentlichen Interesses und Zwecken der öffentlichen Gesundheit (lit. i) stehen die Verwirklichung strategischer Ziele im Fokus, z. B. der Schutz der BürgerInnen vor Gefahren für ihre Gesundheit durch Verbesserung und Überwachung der Vorsorge, so dass darauf basierende angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person verhältnismäßig sein müssen. So stellt § 299 SGB V mit seinen konkreten Anforderungen zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten eine Umsetzung von Art. 9 Abs. 2 lit. i DS-GVO dar.[73]

Hervorzuheben ist außerdem, dass die Datenverarbeitung für Forschungszwecke (lit. j) nur dann verhältnismäßig ist, soweit es sich um unabhängige Forschung handelt. Es muss insbesondere das Erkenntnisinteresse und nicht eine auf die Entwicklung neuer Produkte ausgerichtete Forschung (z. B. der Pharmaindustrie) im Vordergrund stehen, es sei denn diese genügt den allgemeinen Anforderungen erkenntnisgetriebener Forschung.[74] EG 156 DS-GVO lässt sich entnehmen, dass für die Umsetzung nationale Vorschriften erforderlich sind, wie etwa im Bundesdatenschutzgesetz oder bereichsspezifischen landesgesetzlichen Regelungen erfolgt: § 27 BDSG gestattet die Verarbeitung auch ohne Einwilligung für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke, wenn die Verarbeitung zu diesen Zwecken erforderlich ist und die Interessen des Verantwortlichen an der Verarbeitung die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung erheblich überwiegen.[75] Das Merkmal des »erheblichen Überwiegens« ist allerdings keine Voraussetzung der DS-GVO, die an dieser Stelle offener ist als die Richtlinie 95/46/EG.[76]

---

73 Weichert 2024, Rn. 120. Aus EG 54 DS-GVO lässt sich darüber hinaus entnehmen, dass sich private Dritte grundsätzlich nicht hierauf berufen können (so Weichert 2024, Rn. 116 mit Verweis auf die Ausnahme eines beliehenen Unternehmens).

74 So Weichert 2020a, S. 20; siehe vertiefend zur wissenschaftlichen Forschung z. B. Hornung/Hofmann 2017, S. 3 ff.; Geminn 2018, S. 640 ff.; Werkmeister/Schwaab 2019, S. 85 f.

75 Einen entsprechenden Maßstab enthält ebenso § 39 des Bremischen Krankenhausgesetzes. Gemäß dieser Regelung ist eine Einwilligung nicht erforderlich, wenn das berechtigte Interesse der Allgemeinheit an der Durchführung des Forschungsvorhabens das Geheimhaltungsinteresse der PatientInnen erheblich überwiegt.

76 Ähnliche Regelungen waren bereits im BDSG a.F. verankert (z. B. § 14 Abs. 2 Nr. 9 BDSG a.F.). EG 34 der Richtlinie 95/46/EG bezog sich im Gegensatz zu EG 54 DS-GVO noch auf »wichtige« öffentliche Interessen, die als Ausnahmetatbestand die Verarbeitung sensibler Datenkategorien rechtfertigen konnten.

4.1.2 Prüfungsmaßstab

Im Rahmen der nationalen Umsetzungsvorschriften ist zu berücksichtigen, dass Art. 9 Abs. 4 DS-GVO zwar die Freiheit beinhaltet, die Datenverarbeitung eigenständig zu gestalten, aber diese Regelungsbefugnis stets durch das informationelle Selbstbestimmungsrecht sowie den Verhältnismäßigkeitsgrundsatz begrenzt ist.[77] Jede zusätzliche Anforderung muss für die jeweiligen Schutzzwecke geeignet, erforderlich und angemessen sein.[78] Bei der Ausgestaltung ist der Maßstab der Grundrechte des Grundgesetzes zugrunde zu legen, der seitens des Bundesverfassungsgerichts überprüft werden kann – und zwar unabhängig davon, ob die Vorschriften nach der Rechtsprechung EuGH zugleich als Durchführung des Unionsrechts im Sinne des Art. 51 Abs. 1, S. 1 GRCh angesehen werden können.[79] Etwas anderes gilt nur, sofern es sich um vollständig unionsrechtlich determiniertes Recht handelt. Hier stellt sich jedoch sogar umgekehrt die Frage, ob überhaupt Unionsrecht zur Anwendung gelangt oder die Gesundheitsdatenverarbeitung gemäß Art. 168 Abs. 7, S. 1 und S. 2 AEUV eine Angelegenheit der Mitgliedstaaten darstellt.[80] In diesem Sinne soll die Gesundheitspolitik, die Organisation des Gesundheitswesens und die medizinische Versorgung der Verantwortung der Mitgliedstaaten obliegen, da die DS-GVO gemäß Art. 2 Abs. 2 lit. a DS-GVO keine Anwendung auf die Verarbeitung personenbezogener Daten im Rahmen einer Tätigkeit findet, die nicht in den Anwendungsbereich des Unionsrechts fällt.[81] Der EuGH legt diese Regelung unter Berufung auf EG 16 DS-GVO allerdings eng aus und bezieht dies allein auf Verarbeitungen personenbezogener Daten, die von staatlichen Stellen im Rahmen einer Tätigkeit, die der Wahrung der nationalen Sicherheit dient, oder einer Tätigkeit, die derselben Kategorie zugeordnet werden kann, ausgeführt werden.[82] Der Anwendungsbereich des Unionsrechts soll danach nicht erst dann eröffnet sein, wenn eine mit einer Datenverarbeitung zusammenhängende hoheitliche Tätigkeit im konkreten Einzelfall durch unionsrechtliche Regelungen beeinflusst wird, sondern es soll aus-

77 Umstritten ist in diesem Zusammenhang zudem, inwieweit nationale Regelungen die Datenverarbeitung erleichtern können, siehe Mester 2022, Rn. 37; Kühling/Martini 2016, S. 53 ff.
78 Weichert 2024, Rn. 150.
79 Vgl. BVerfGE 155, 119, 165.
80 Vgl. Weichert 2024, Rn. 96 mit Verweis auf Dochow 2016, S. 403.
81 Vgl. BSG, Urteil vom 20.01.2021, B 1 KR 7/20 R, Rn. 28.
82 EuGH, Urteil vom 22.06.2021, C-439/19, Rn. 66.

reichen, dass die Verarbeitung bei abstrakter Betrachtung überhaupt einen Bezug zum Unionsrecht haben könne.[83] Ein solcher ergibt sich zumindest für Forschungsdaten, da Art. 179 Abs. 1 AEUV das Ziel zu entnehmen ist, einen europäischen Forschungsdatenraum zu schaffen.

4.2 Neue Rechtsgrundlagen für die Datenverarbeitung

Ein Grund dafür, dass die Einflussmöglichkeiten für die betroffene Person durch die Einwilligung zur Datenverarbeitung begrenzt ist, sind die zahlreichen gesetzlichen Rechtsgrundlagen, auf die die Datenverarbeitung gestützt werden können. Art. 9 Abs. 2 DS-GVO eröffnet dem nationalen Gesetzgeber aufgrund seiner Öffnungsklauseln weitreichende Gestaltungsmöglichkeiten im Gesundheitssektor. Es ist nahezu paradox, dass gerade der Bereich der sensitiven Daten eine derartige Flexibilität beinhaltet, was in Deutschland zu der Vielzahl unterschiedlicher, landesgesetzlicher Regelungen geführt hat. Daher bedarf es einer Harmonisierung dieser Regelungen im Gesundheitssektor. Eine europäische Verordnung, wie die kommende EHDS-VO, könnte zur Rechtssicherheit beitragen (siehe hierzu die nachfolgenden Ausführungen).

4.2.1 Neue Rechtsgrundlagen im EHDS-VO-E

Der EHDS-VO-E soll nach der Vorstellung des europäischen Gesetzgebers insgesamt die Rechtsgrundlage für die Datenverarbeitung im Rahmen der Sekundärnutzung von Gesundheitsdaten nach Art. 9 Abs. 2 lit. g, h, i und j DS-GVO darstellen, s. EG 37 EHDS-VO-E. Der grundsätzliche Ansatz der DS-GVO, nach der die Verarbeitung besonderer Kategorien personenbezogener Daten grundsätzlich verboten ist, bleibt also erhalten. Dagegen können weder der DA noch der DGA als Rechtsgrundlagen für die Datenverarbeitung herangezogen werden, s. EG 4, S. 2 DA und Art. 1 Abs. 3, S. 4 DGA sowie EG 7, S. 7 DA und Art. 5 Abs. 7 DA.

Dabei ist allerdings fraglich, ob der EHDS-VO-E insgesamt die Anforderungen an die Rechtsgrundlagen des Art. 9 Abs. 2 lit. g, h, i und j DS-GVO erfüllt. Außerdem verweist der EHDS-VO-E anders als der DGA nicht darauf, dass im Falle von Konflikten die DS-GVO vorrangig gelten soll, sondern

83 Bäcker 2023, Rn. 9.

die Regelungen der DS-GVO sollen letztendlich nur unberührt bleiben, was zu Rechtsunsicherheit führt.[84] Dies kann auch die Frage des Widerspruchrechts der Betroffenen im Rahmen der Sekundärnutzung von Gesundheitsdaten betreffen oder den Begriff der Forschung, da die entsprechenden Erwägungen der Literatur im Rahmen der DS-GVO nicht ohne weiteres auf den EHDS-VO-E übertragbar sind.[85]

4.2.2 Gesundheitsdatennutzungsgesetz

Die Verknüpfung und Verarbeitung von Sozial- und Gesundheitsdaten nach § 4 GDNG stützt der Gesetzgeber auf eine Datenverarbeitungsbefugnis gemäß Art. 6 Abs. 1 lit. c i.V.m. Art. 9 Abs. 2 lit. i und j DS-GVO.

Gemäß § 4 Abs. 1 GDNG ist die Verknüpfung von pseudonymisierten Daten des Forschungsdatenzentrums nach § 303d SGB V mit pseudonymisierten Daten der klinischen Krebsregister der Länder nach § 65c SGB V sowie die Verarbeitung dieser Daten für Forschungsvorhaben zulässig, wenn die Verknüpfung für eine nicht näher definierte »zu untersuchende Forschungsfrage« erforderlich ist. Anders als im SGB V erfolgt kein konkreter Bezug zu »wissenschaftliche[n]« Forschungszwecken (§ 303e Abs. 2 Nr. 4 SGB V n.F.). Darüber hinaus dürfen nach § 303e Abs. 2 Nr. 9 und 10 SGB V n.F. die dem FDZ Gesundheit übermittelten Daten von den Nutzungsberechtigten verarbeitet werden, soweit dies für die dort aufgezählten Zwecke erforderlich ist. Insbesondere die Zwecke der Entwicklung und Weiterentwicklung bestimmter Produkte, § 363 Abs. 2 Nr. 9 SGB V n.F., lassen darauf schließen, dass diese Regelung im weitesten Sinne gleichermaßen Forschungsfragen umfassen kann, wobei nicht zwangsläufig ein wissenschaftlicher Bezug vorausgesetzt wird.

§ 303e Abs. 2 Nr. 9 und10 SGB V n.F. haben insgesamt einen sehr weiten Anwendungsbereich, was deswegen bemerkenswert ist, weil der Kreis der Antragsberechtigten nicht festgelegt ist.[86] Faktisch erlaubt die Kombination

84 Auch in Art. 1 Abs. 3a EHDS-VO-RE steht ausdrücklich nur, dass die Vorschriften der DS-GVO »unberührt« bleiben sollen (»shall be without prejudice to«) während nach Art. 1 Abs. 4, S. 1 EHDS-VO-RE z. B. die Vorschriften des DA »ergänzt« werden sollen und in Art. 1 Abs. 4, S. 2 EHDS-VO-RE ausdrücklich normiert ist, dass die Vorschriften des EHDS-VO-RE im Konfliktfall vorgehen sollen.

85 Siehe dazu auch die Ausführungen unter 5.5.1.

86 Kritsch dazu z. B. Netzwerk Datenschutzexpertise 2023a, S. 7. Siehe außerdem die Ausführungen unter 5.4.

der weit gefassten Zwecke mit dem nicht mehr begrenzten Kreis an Antragsberechtigten den Zugang zu den Daten des FDZ Gesundheit einem nicht mehr überschaubaren Kreis an Antragsberechtigten.

Zwar belassen nicht nur Art. 6 Abs. 2 und Abs. 3 DS-GVO, sondern ebenso die Regelungen des Art. 9 Abs. 2 DS-GVO den Mitgliedstaaten bei der Ausgestaltung der Vorschriften erhebliche Gestaltungsspielräume.[87] Ebenso erlaubt Art. 9 Abs. 2 lit. j DS-GVO im Bereich des Art. 89 DS-GVO – der wissenschaftlichen Forschung – die Verarbeitung besonderer Kategorien personenbezogener Daten auf Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaates, womit gleichermaßen eine Zweckänderung der Daten und deren längerfristige Speicherung legitimiert (Art. 5 lit. b, lit. e DS-GVO) ist. Dennoch müssen die Regelungen eines Gesundheitsdatennutzungsgesetzes oder konkrete Regelungen zur kommerziellen Nutzung von Gesundheitsdaten den Anforderungen an eine verfassungsgemäße Schranke des Rechts auf informationelle Selbstbestimmung genügen, was insbesondere mit Blick auf die Gebote der Normenklarheit und Bestimmtheit gilt. Die betroffene Person muss das Ausmaß der Datenverarbeitung insgesamt vorhersehen können. Anlass, Zweck und Grenzen des Eingriffs müssen daher in der Ermächtigung bereichsspezifisch, präzise und normenklar festgelegt werden.[88]

Auch wenn die Datenverarbeitung im Rahmen von Forschungsprojekten mit Herausforderungen verbunden ist und oftmals der Zweck der Verarbeitung personenbezogener Daten im Rahmen der Forschung zum Zeitpunkt der Erhebung der personenbezogenen Daten nicht vollständig angegeben werden kann,[89] sind die Regelungen des SGB V sehr umfassend, so dass sich wiederum die Frage nach einem effektiven Schutz des informationellen Selbstbestimmungsrechts stellt.

5. Unbeschränkter Zugang zu Forschungsdaten?

Sowohl aus der Sicht der natürlichen Person als auch aus Sicht der an den Daten interessierten Akteure stellt sich die Frage danach, an welche Voraussetzungen der Zugang zu den Daten geknüpft ist. Die Voraussetzungen kön-

87 Vgl. BVerGE 155, 119, 165, außerdem Kühling/Martini 2016, S. 55.
88 Vgl. BVerfGE 65, 1, 44 ff. S. hierzu auch die Ausführungen unter 4.1.
89 Siehe oben 3.1.1.und nachfolgend unter 5.1.

nen in der Person des Antragstellers, aber gleichermaßen im Zweck der Datenverarbeitung begründet sein.

5.1 Die Forschungsprivilegierung in der Datenschutz-Grundverordnung

5.1.1 Die Forschungsprivilegierung in Art. 89 DS-GVO

Eine zentrale Anknüpfungsnorm im Hinblick auf die Forschungsprivilegierung in der DS-GVO ist Art. 89 DS-GVO. Dieser verlangt in Absatz 1 geeignete Garantien für die Rechte und Freiheiten der im Sinne der DS-GVO betroffenen Personen, wenn die Datenverarbeitung u.a. »wissenschaftlichen Forschungszwecken«[90] dient. Der Begriff der Forschung ist dabei nach EG 159, S. 2 DS-GVO weit auszulegen und umfasst insbesondere die Verarbeitung für beispielsweise die technologische Entwicklung und die Demonstration, die Grundlagenforschung, die angewandte Forschung und die privat finanzierte Forschung. Der Gesetzgeber unterscheidet bei der Forschungsprivilegierung grundsätzlich nicht zwischen Gesundheitsdaten im Sinne von Art. 4 Nr. 15 DS-GVO und anderen personenbezogenen Daten, wenngleich bei der Verarbeitung von besonderen personenbezogenen Daten auf Grundlage von Art. 9 Abs. 2 lit. j DS-GVO i.V.m. Art. 89 Abs. 1 DS-GVO die dort genannten Voraussetzungen vorliegen müssen.

Während auf der einen Seite geeignete Garantien vorliegen müssen, können auf der anderen Seite bestimmte Rechte der betroffenen Person eingeschränkt werden, wenn sie voraussichtlich die Verwirklichung des spezifischen Zwecks unmöglich machen oder ernsthaft beeinträchtigen und solche Ausnahmen für die Erfüllung dieser Zwecke notwendig sind, Art. 89 Abs. 2 DS-GVO.

5.1.2 Teilweise Aufhebung des Verarbeitungsverbots von besonderen personenbezogenen Daten

Das Verarbeitungsverbot des Art. 9 Abs. 1 DS-GVO für besondere personenbezogene Daten wird durch Art. 9 Abs. 2 DS-GVO für die dort normierten Fälle aufgehoben, die zum Teil an bestimmte Eigenschaften der datenschutzrechtlich Verantwortlichen anknüpfen. So ist die Datenverarbeitung

90 Siehe zur Eigenschaft als »Scharnierbegriff« z. B. Caspar 2019, Rn. 31.

auf Grundlage des Erlaubnistatbestandes des Art. 9 Abs. 2 lit. d DS-GVO[91] unter anderem an die Voraussetzung geknüpft, dass eine Organisation ohne Gewinnerzielungsabsicht handelt. Dahingegen enthält die Öffnungsklausel des Art. 9 Abs. 2 lit. j DS-GVO keine expliziten institutionellen oder personellen Einschränkungen. Die Datenverarbeitung zum Zwecke der wissenschaftlichen Forschung ist also nicht auf öffentliche Stellen, oder Stellen, die im öffentlichen Interesse handeln, beschränkt, s. auch EG 159, S. 2 DS-GVO.

Die Maßstäbe für die Forschung zu Zwecken der Weiterentwicklung von Arzneimitteln und Medizinprodukten müssen die Vorgaben des Art. 9 Abs. 2 DS-GVO einhalten. Zu berücksichtigen ist dabei, dass die Ausnahmen von Art. 9 Abs. 2 DS-GVO im Rahmen von Forschungszwecken nur greifen können, wenn es sich nicht um rein kommerzielle Forschung handelt.[92] Der Begriff der Forschung ist zwar weit auszulegen und umfasst ebenso Industrieforschung. Wissenschaftliche Forschung erfordert aber Unabhängigkeit und Selbstständigkeit. Der Erkenntnisgewinn muss im Vordergrund stehen, was zugleich Forschung, die auf rein kommerzielle Zwecke, wie die Entwicklung neuer Produkte, ausgerichtet ist, ausschließt.[93] Ansonsten bedarf es außerhalb der wissenschaftlichen oder historischen Forschung eines »öffentlichen Interesses« oder »gesundheitsbezogener Zwecke«, wenn Gesundheitsdaten für Forschungszwecke verarbeitet werden. Dann finden die Privilegierungen von Art. 9 Abs. 2 lit. j, lit. g oder lit. h DS-GVO Anwendung.[94] Art. 9 Abs. 2 lit. g DS-GVO verlangt dabei sogar ein erhebliches öffentliches Interesse und eine umfassende Abwägung mit dem Datenschutzrisiko des Betroffenen, was in einer ausdrücklichen Rechtsnorm abzubilden wäre.

5.2 Die Behandlung von Forschungsdaten im DA und DGA

Im DA und DGA, finden sich – soweit ersichtlich – grundsätzlich keine Beschränkungen des Zugangs zu den aufgeführten Daten, was dem gemeinsamen Zweck der Verordnungen entspricht, einen barrierefreien Bin-

91 Siehe dazu Kampert 2022, Rn. 11.
92 Siehe auch Weichert 2020a, S. 20 m.w.N.
93 Siehe hierzu auch die Ausführungen unter 4.1.1.
94 Siehe hierzu ebenfalls die Ausführungen unter 4.1.1.

nenmarkt zu ermöglichen.[95] Nach Art. 2 Nr. 16 DA kann der Datenempfänger grundsätzlich jede natürliche oder juristische Person sein, wenngleich gemeinnützige Forschungseinrichtungen hinsichtlich der der Gegenleistung für die Bereitstellung von Daten in Art. 9 Abs. 2 lit. a DA privilegiert werden. Auch im DGA kann der Datennutzer grundsätzlich jede natürliche oder juristische Person sein, die rechtmäßig Zugang zu personenbezogenen und nicht personenbezogenen Daten hat, s. Art. 2 Nr. 9 DGA. Allerdings können die nach nationalem Recht zuständigen öffentlichen Stellen den Zugang zu den Daten unter bestimmten Bedingungen auch verweigern. Diese Bedingungen könnten theoretisch auch an die Eigenschaft der Datennutzer anzuknüpfen, wenngleich die Bedingungen für die Weiterverwendung nach Art. 5 Abs. 2 DGA nicht der Behinderung des Wettbewerbs dienen dürfen und nichtdiskriminierend sein müssen. Eine Ausnahme besteht für den Bereich der wissenschaftlichen Forschung. Die Bedingungen für die Weiterverwendung sollten so gestaltet werden, dass wissenschaftliche Forschung gefördert wird, so dass beispielsweise die bevorzugte Behandlung der wissenschaftlichen Forschung als nichtdiskriminierend betrachtet werden sollte, s. EG 15, S. 3 DGA.[96]

5.3 Mögliche Zugangsbeschränkungen im EHDS-VO-E

In dem Kommissionsentwurf der EHDS-VO sind ebensowenig personelle oder institutionsbezogene Zugangsbeschränkungen enthalten. Ausdrücklich ist in Art. 45 EHDS-VO-E normiert, dass jede natürliche oder juristische Person bei der Zugangsstelle für Gesundheitsdaten einen Antrag auf Datenzugang für die in Art. 34 EHDS-VO-E genannten Zwecke stellen kann.[97] Dagegen sieht der Parlamentsentwurf eine Einschränkung in der Form vor, dass nur ein »Antragsteller für Gesundheitsdaten« den entsprechenden Antrag stellen kann.[98] Dieser Begriff bezeichnet indes »jede natürliche oder juristische Person, die nachweislich eine berufliche Verbindung zum

95 Siehe EG 4 DA-PE und EG 2 DGA.

96 Siehe auch Savary 2023, Rn. 67; siehe auch EG 27 DGA, der ausdrücklich darauf verweist, dass die wissenschaftliche Forschung die Nutznießerin davon sein soll, dass die Datenvermittlungsdienste Unternehmen aller Größenordnung Zugang zur Datenwirtschaft ermöglichen sollen.

97 Siehe auch Rat der Europäischen Union 2023, S. 132: »A natural Person may submit a data access application for the purposes referred to in Article 34 to the health data access body«.

98 Siehe Art. 45 Abs. 1 EHDS-VO-PE.

Gesundheitswesen, zur [sic!] Bereich der öffentlichen Gesundheit oder zur medizinischen Forschung hat und einen Antrag auf Gesundheitsdaten stellt«, s. Art. 2 Ab. 2 lit. Za EHDS-VO-PE.[99] Offen bleibt, inwiefern sich die medizinische Forschung von der wissenschaftlichen Forschung unterscheidet. Verstünde man unter der medizinischen Forschung jede Forschung mit einem Bezug zu medizinischen Zwecken, so gibt es zumindest keine Einschränkung im Hinblick auf (rein) kommerzielle Zwecke.

Der Katalog in Art. 34 Abs. 1 EHDS-VO-E enthält eine Aufzählung zulässiger Zwecke der Sekundärnutzung von elektronischen Gesundheitsdaten. Damit schafft der europäische Gesetzgeber neue Rechtsgrundlagen der Datenverarbeitung im Sinne der DS-GVO, wenn man davon ausgeht, dass nicht nur der Zugang zu den Daten in Art. 34 Abs. 1 EHDS-VO geregelt werden, sondern sich auch die Sekundärnutzung selbst auf diese Vorschrift stützt. Andernfalls braucht es für die Sekundärnutzung der Daten weiterhin geeigneter Rechtsgrundlagen außerhalb der geplanten EHDS-VO.

Die Zwecke des Art. 34 Abs. 1 EHDS-VO-E sind insgesamt denkbar weit gefasst. Die wissenschaftliche Forschung im Bereich des Gesundheits- oder Pflegesektors gehört ausdrücklich zu den nach den Art. 34 Abs. lit. e EHDS-VO-E erlaubten Zwecken.[100] Demgegenüber wird dieser weit gefasste Zweck durch den EHDS-VO-PE insofern eingeschränkt, als dass die Forschung zur öffentlichen Gesundheit oder zur technologischen Bewertung im Gesundheitswesen beitragen oder ein hohes Maß an Qualität und Sicherheit der Gesundheitsversorgung, von Arzneimitteln oder Medizinprodukten gewährleisten soll.[101]

Einen Bezug zur Forschung weisen auch die Art. 34 Abs. 1 lit. f und g EHDS-VO-E auf,[102] die ebenfalls weit gefasst sind und zum einen den Zugang zu den elektronischen Gesundheitsdaten für die Entwicklungs- und Innovationstätigkeit für bestimmte Produkte oder Dienste und zum anderen zu Zwecken des Trainings, der Erprobung und Bewertung von Algorithmen, gewähren. Dass die Kommission diese weiten Zwecke neben der wissenschaftlichen Forschung in Art. 34 Abs. 1 lit. e EHDS-VO-E als einen Zweck aufgenommen hat, zeigt, dass sie auch kommerzielle Zwecke der Datenverarbei-

99 Abänderung 105.

100 Siehe auch Rat der Europäischen Union 2023, S. 109: »scientific research related to health or care sectors«.

101 Art. 34 Abs. 1 lit. e EHDS-VO-PE.

102 Der EHDS-VO-PE enthält Art. 34 Abs. 1 lit. f und g nicht mehr, wobei teilweise eine inhaltliche Verschiebung nach Art. 34 Abs, 1 lit. e EHDS-VO-PE erfolgt.

tung in den Vordergrund rücken wollte. Ergänzend kann an dieser Stelle eine Parallele zu den erweiterten Möglichkeiten der Datenverarbeitung nach dem SGB V gezogen werden.[103]

Neben den erlaubten Zwecken werden in Art. 35 EHDS-VO-E zudem Verbote der Sekundärnutzung von elektronischen Gesundheitsdaten aufgezählt, die naturgemäß den Zugang der Antragsteller beschränken, und zwar unabhängig von der Person des Antragstellers. Diese Zwecke umfassen sowohl solche zum Nachteil einzelner natürlicher Personen,[104] also auch solche mit gesamtgesellschaftlichen Nachteilen sowie darüber hinaus bestimmte Entscheidungen, Tätigkeiten und die Entwicklung bestimmter Produkte. Ob ein konkreter Zweck verboten ist, muss also anhand der jeweiligen Auswirkungen der Datenverarbeitung bestimmt werden.

5.4 Der Zugang zur Forschungsdaten im Gesundheitsdatennutzungsgesetz

Mit der Verarbeitungsbefugnisnorm des § 303e Abs. 1 SGB V n.F. hat Deutschland von der Öffnungsklausel des Art. 9 Abs. 4 DS-GVO Gebrauch gemacht.

Im Rahmen des GDNG soll der Kreis der Nutzungsberechtigten der dem FDZ Gesundheit übermittelten Daten insofern erweitert werden, als dass grundsätzlich alle natürlichen und juristischen Personen antragsberechtigt sind, sofern die beantragten Daten für einen in § 303e Abs. 2 SGB V n.F. genannten Zweck erforderlich sind. Dagegen sah § 303e Abs. 1 SGB V a.F. noch einen abschließenden Katalog an Nutzungsberechtigten vor.[105] Der Wegfall des zuvor vorhandenen »Akteursbezugs«[106] korrespondiert mit den Vorschriften des EHDS-VO-E, die ebenfalls auf den Zweck der Datennutzung abstellen.

Die Zwecke des § 303e Abs. 2 SGB V n.F. sind, wie oben bereits dargestellt, weit gefasst und umfassen insbesondere die wissenschaftliche Forschung zu Fragestellungen aus den Bereichen Gesundheit und Pflege. Der Katalog der Zwecke der Datenverarbeitung in § 303e Abs. 2 SGB V a.F. sollte

103 Siehe hierzu die Ausführungen unter 4.2.2.

104 Siehe z. B. Art. 35 Abs. 1 lit. a EHDS-VO-E und Art. 35 Abs. 1 lit. c EHDS-VO-E, die aber im Parlamentsentwurf jeweils auf gesellschaftliche Gruppen erweitert werden.

105 Kritisch zur Erweiterung des Kreises der Nutzungsberechtigten z. B. Netzwerk Datenschutzexpertise 2023a, S. 7.

106 BfDI 2023, S. 20.

durch das GDNG insgesamt erweitert werden, was im Zusammenspiel mit dem Wegfall des Akteursbezugs zu einem erheblich vergrößerten Kreis von Antragsberechtigten führt.[107] Auffällig im GDNG-Stammgesetz, also dem Gesetz zur Nutzung von Gesundheitsdaten zu *gemeinwohlorientierten Forschungszwecken*, ist eben dieser Bezug zu dem Gemeinwohl, das neben dem Patientenwohl als ein wichtiges Ziel der Verarbeitung von Gesundheitsdaten herangezogen wird.[108] Gemeinwohlorientierte Forschungszwecke sind Teil der Zweckbestimmung in § 1 Abs. 1, Abs. 2 und Abs. 3 GDNG. Das Gemeinwohl wird im GDNG nicht explizit definiert, dient jedoch an zahlreichen Stellen als Anknüpfungspunkt.[109] Darüber hinaus sind in § 1 Abs. 2 GDNG-Stammgesetz die Verarbeitung von Gesundheitsdaten zu Forschungszwecken und zur Verbesserung der Gesundheitsversorgung und Pflege als im Gemeinwohl liegende Zwecke aufgezählt.[110] Diese ausdrücklich aufgeführten Zwecke sind jedoch keine abschließende Aufzählung. Vielmehr kommen noch weitere im Gemeinwohl liegende Zwecke in Betracht. Dazu gehören die Wahrnehmung öffentlicher Aufgaben im Bereich der Gesundheitspolitik und der Gesundheitssystemsteuerung.[111]Auffällig ist, dass in der Zweckaufzählung des § 303e Abs. 2 SGB V n.F. keine Einschränkung der Zwecke im Sinne des Gemeinwohls vorgenommen wird.[112] Daher bedarf es einer entsprechenden Konkretisierung und verbindlichen Auslegung dieses Begriffs.[113]

Die Erweiterung des Zugangs zu Gesundheitsdaten in § 303e SGB V n.F. bietet zudem die Gelegenheit, allgemeine Rechtmäßigkeitserwägungen in Bezug auf das Zusammenspiel zwischen dem GDNG und der künftigen EHDS-VO sowie der DS-GVO anzustellen. So kann man die Frage aufwerfen, ob die teils vage Formulierung der Zwecke in § 303e Abs. 2 SGB V n.F. den Anforderungen der Ausnahmeregelungen in Art. 9 Abs. 2 DS-GVO genügt.[114] Auch im Hinblick auf die in dem EHDS-VO-E neu geschaffenen Rechtsgrundlagen für die Datenverarbeitung lässt sich jedenfalls kritisch

107 Siehe hierzu auch die Ausführungen unter 4.2.2.
108 Siehe Bundesrat 2023, S. 27 und Deutscher Bundestag 2023a, S. 1.
109 Siehe kritisch zum vagen Gemeinwohlbezug BfDI 2023, S. 20.
110 Diese Zwecke werden in der Gesetzesbegründung konkretisiert, siehe Deutscher Bundestag 2023a, S. 49.
111 Siehe Deutscher Bundestag 2023a, S. 50.
112 Siehe BfDI 2023, S. 21.
113 Siehe hierzu die Ausführungen unter 6.2.
114 Kritisch dazu und zu den Zwecken in § 303e Abs. 2 SGB V a.F. z. B. Lorenz/Schild 2023, S. 167.

anmerken, dass die in § 303e Abs. 2 SGB V n.F. aufgeführten Zwecke künftig den Zwecken des Art. 34 EHDS-VO entsprechen müssen.

6. Überlegungen zur »Architektur« einer gemeinwohl- und patientenorientierten Nutzung

6.1 Konkretisierung

Sämtliche einschlägigen Regelungen des Art. 9 Abs. 2 DS-GVO (lit. g bis j) knüpfen an das Merkmal der Erforderlichkeit an. Daher bedarf dieses Merkmal gesetzlicher Konkretisierungen.

Eine generalklauselartige Vorschrift im nationalen Recht, die die Verarbeitung von Patientendaten zu Forschungszwecken oder zur Weiterentwicklung oder Nutzenbewertung von Arzneimitteln erlaubt, ist zwar legitim, insbesondere aufgrund der thematischen Offenheit von Forschungsthemen. Es ist jedoch zu berücksichtigen, dass ein verfassungsrechtlicher Auftrag an den Staat besteht, den Schutz der informationellen Selbstbestimmung sicherzustellen und den Einzelnen auch im Rahmen von privaten Rechtsverhältnissen hinreichend zu schützen. Die Ausgestaltung rechtlicher Rahmenbedingungen ist seine originäre Aufgabe, die er durch wirksame und dem Bestimmtheitsgebot genügende gesetzliche Regelungen zu erfüllen hat. Auch der europäische Verordnungsgeber hat höherrangiges (Primär-)Recht zu beachten, an dem sich die Vorschriften einer Verordnung messen lassen müssen, im Kontext der Sekundärnutzung von Gesundheitsdaten, also insbesondere die Art. 7 und 8 GRCh und im Hinblick auf die Datenverarbeitung zu Forschungszwecken Art. 13 GRCh.

Insgesamt gilt jedoch, dass es für den Gesetz- oder Verordnungsgeber nicht leistbar ist, jede Fallkonstellation in einen konkreten Tatbestand zu fassen. Dennoch könnten die wesentlichen Parameter einer Erforderlichkeitsprüfung festgelegt werden, die i.S.v. Art. 5 DS-GVO Umfang, Intensität und Umstände der Verarbeitung von Patientendaten berücksichtigt. So stellen etwa die Gewährleistung der Datensicherheit und die in Art. 5 Abs. 1 lit. f DS-GVO genannte »Integrität« und »Vertraulichkeit« grundlegende Schutzziele dar, für die der Gesetzgeber Maßstäbe vorgeben könnte, um diese Anforderungen spezifischer zu gestalten. Auch wenn aufgrund der Dynamik der technischen Entwicklung ein Gesetz grundsätzlich

technikoffen ausgestaltet werden sollte, kann es sich im Falle der besonders sensiblen Bereiche, wie der Verknüpfung von Patientendaten und dem Zugang zu diesen, empfehlen, ein technisches Schutzniveau gesetzlich zu verankern. Diese technischen und organisatorischen Maßnahmen könnten sogar Bedingungen und Verhaltenspflichten enthalten, die über den Stand der Technik hinausgehen. Aufgrund der Sensibilität der Datenverarbeitung wäre es vorstellbar, dass bestimmte Mindestanforderungen an Verschlüsselungsverfahren, Auswertungs- bzw. Verknüpfungsverfahren und Speicherverfahren gesetzlich festgeschrieben werden.

Eine Rechtsverordnung, die auch vom GDNG vorgesehen ist, oder delegierte Rechtsakte können daher zwar einen integralen Bestandteil einer rechtssicheren gemeinwohl- und patientenorientierten Nutzung bilden. Das sollte den Gesetzgeber aber nicht davon entbinden, der ihm eigenen Handlungsmöglichkeit nachzukommen und zu prüfen, inwieweit er mit Blick auf die Rechtssicherheit für alle Beteiligten, verbindliche und bestimmte Vorgaben einer rechtlich zulässigen Datenverarbeitung selbst vornehmen kann, so dass auf untergesetzlicher Ebene die von ihm gesetzten Maßstäbe lediglich zu konturieren sind.

6.2 Konkordanz und Verhaltensregeln

Vor diesem Hintergrund könnten die Merkmale »gemeinwohlorientiert« und »öffentliches Interesse« in nicht abschließender Form gesetzlich spezifischer gestaltet und darüber hinaus untergesetzlich Best-Practice-Beispiele und Standards definiert werden.[115] Dies unterstützt die Bildung einheitlicher Maßstäbe, die sektorübergreifend Relevanz haben könnten. Auf datenschutzrechtlicher Ebene bieten sich hierzu gleichermaßen die Instrumente der Verhaltensregeln (Art. 40 DS-GVO) oder Zertifizierungen (Art. 42 DS-GVO) an. Mit Blick auf eine Bildung und Anerkennung von verbindlichen sowie allgemeingültigen Standards einer gemeinwohl- und patientenorientierten Datennutzung, könnte eine unabhängige Stelle geschaffen werden, die gleichermaßen sowohl die Pluralität der Nutzungsberechtigten und Interessenträger widerspiegelt als auch DatenschutzexpertInnen umfasst. In diesem Sinne müsste die organisatorische und strukturelle Zusammensetzung dieser Stelle eine Verhandlungsparität garantieren. Eine solche

115 Siehe hierzu ebenfalls die Ausführungen unter 5.4.

Aufgabe könnte zwar gleichermaßen ein Forschungsdatenzentrum oder eine weisungsfrei agierende Koordinierungsstelle leisten. Aber an die Stelle eines beratenden Arbeitskreises (vgl. § 303 d Abs. 3 SGB V n.F.) oder einer kooperativen Zusammenarbeit, wie sie Art. 36 EHDS-VO-E bislang vorsieht, könnte eine rechtsgestaltende Mitwirkung treten – was über die derzeitigen gesetzlichen Möglichkeiten hinausgeht. So könnte eine gestaltende Mitwirkung von relevanten InteressenvertreterInnen zu einer echten Teilhabe und Konkordanz beitragen. Kompetenz und Fachwissen der Beteiligten stellen dabei sicher, dass Leitlinien für eine gemeinwohlorientierte Nutzung erarbeitet werden. Damit würde den einzelnen Nutzungsberechtigten letztendlich ein Partner gegenüberstehen, der die Erforderlichkeit der Verarbeitung der Patientendaten für Forschungszwecke und für die Nutzung zur Weiterentwicklung von Arzneimitteln sachkundig verhandeln kann.[116] Dies ist auch unter dem Gesichtspunkt zu sehen, dass einerseits das informationelle Selbstbestimmungsrecht zu gewährleisten ist und es eines Ausgleichs mit den Interessen der Allgemeinheit an der gemeinwohlorientierten Nutzung der Daten bedarf, aber andererseits die individuelle Einwilligung – wie in diesem Beitrag dargestellt – an Bedeutung verliert und in der Praxis zudem mit Schwierigkeiten behaftet ist.[117] Insgesamt beinhaltet dies keine Abkehr vom traditionellen Datenschutzrecht, sondern vielmehr die Erzeugung einer Konkordanz bspw. durch Verhaltensregeln, die die Interessen der Betroffenen abbilden.

6.3 Verhältnismäßigkeit

6.3.1 Nutzungsberechtigte und Zwecke

Die gerade skizzierten Voraussetzungen könnten ebenso eine Ausweitung von Nutzungsberechtigten und die Nutzung von Patientendaten für kom-

116 Gruber/Zihlmann diskutieren im Rahmen ihres Beitrages zum digitalen Zwilling in diesem Band die Möglichkeiten eines Treuhandmodells und die Möglichkeiten eines Repräsentations- und Stellvertretermodells.

117 Siehe dazu auch die Ausführungen unter 3.1.

merzielle Zwecke durch private Dritte erlauben.[118] Zu berücksichtigen ist in diesem Zusammenhang, dass der Zugang zu Patientendaten, etwa für Zwecke der Weiterentwicklung von Arzneimitteln oder Behandlungsmethoden, durchaus im öffentlichen Interesse liegen kann, insbesondere wenn die Festlegung der Kriterien für eine unabhängige, am Allgemeinwohl orientierte Forschung und Nutzung von Gesundheitsdaten durch die Pluralität von InteressenvertreterInnen umgesetzt wird.

In diesem Sinne könnte insgesamt ein verbindlicher Maßstab für Forschungszwecke, Weiterentwicklungs- und Nutzungszwecke festgelegt und sichergestellt werden, dass das Erkenntnisinteresse im Vordergrund steht. Dabei ist im Übrigen kein erhebliches Überwiegen gefordert, wie dies bspw. § 27 BDSG oder Landeskrankenhausgesetze entsprechend regeln. Aber es bedarf genauer Maßstäbe, anhand derer die Verhältnismäßigkeit bewertet werden kann. Dies umfasst Leitlinien und Verhaltensstandards, die aufzeigen, was von unabhängigen Forschungszwecken erfasst ist, inwieweit kommerzielle Forschung möglich ist, was Zwecke des Allgemeinwohls oder Erfordernisse zum Schutze der Rechte und Freiheiten anderer darstellen.

6.3.2 Widerspruchsrecht

Insgesamt spielt darüber hinaus die Beschränkung der Betroffenenrechte innerhalb der Gesamtarchitektur eine wichtige Rolle. Es bedarf einer wirksamen Rechtsdurchsetzung für die Betroffenen, und zur Wahrung des Verhältnismäßigkeitsgrundsatzes muss gleichermaßen ein Widerspruchsrecht gegen die Datenverarbeitung gewährleistet sein.[119] Während der ursprüngliche Kommissionsentwurf zur EHDS-VO ein solches ausklammerte, war es im Parlamentsentwurf und im Ratsentwurf enthalten.

Allerdings bestünde im Einzelfall dennoch die Möglichkeit, das Widerspruchsrecht mit Blick auf die Sekundärnutzung von Gesundheitsdaten zu wissenschaftlichen Forschungszwecken auszuschließen. Voraussetzung wäre die Begründung eines öffentlichen Interesses i. S. d. Art. 21 Abs. 6 DSGVO an einem solchen Ausschluss, welches sich nicht pauschal beurteilen

118 Siehe hierzu die Ausführungen unter 5.1.2. in denen ausgeführt wird, dass rein kommerzielle Forschung nicht vom Forschungsbegriff umfasst ist. Sichert jedoch eine Gesamtarchitektur den Schutz der Betroffenen, könnte eine Ausweitung der Forschung grundsätzlich auch für kommerzielle Zwecke in Betracht kommen.

119 Siehe hierzu die Ausführungen unter 3.2.2 und 5.5.2.

lässt. Daher könnten mit Blick auf die notwendigen Aspekte der Rechtssicherheit und der Rechtsklarheit und zum Schutz des informationellen Selbstbestimmungsrechts eindeutige Regelungen formuliert werden, die keinen Interpretationsspielraum, gerade bezüglich der Beschränkungsmöglichkeit aus öffentlichen Interessen erlauben. Letztendlich können Forschungszwecke, die im öffentlichen Interesse liegen, nur überwiegen, wenn Grundrechtsgarantien eingehalten werden, so dass eine Interessenabwägung im Rahmen des Art. 21 Abs. 6 DS-GVO erforderlich ist, um die kollidierenden Grundrechte der informationellen Selbstbestimmung einerseits und der Wissenschafts- bzw. Forschungsfreiheit andererseits in Einklang zu bringen.[120] Eine paritätisch besetzte Stelle, wie sie unter 6.2 erwähnt ist, hätte die Möglichkeit, entsprechende Anforderungen und Bedingungen zu gestalten und standardisierte Leitlinien für die Beschränkung des Widerspruchsrechts zu entwickeln. Dabei wäre auch zu prüfen, inwieweit gesetzlich festgelegte Anforderungen an technische sowie organisatorische Maßnahmen (etwa Verschlüsselungsverfahren, Anonymisierung) eine zusätzliche Garantie dafür darstellen könnten, dass Betroffenenrechte von vorneherein nicht beeinträchtigt werden.

Mit Blick auf eine zentrale Zugangsverwaltung könnte zudem eine Veröffentlichungspflicht angedacht werden, die sicherstellt, dass Aktivitäten und Datennutzungen der Nutzungsberechtigten nachgehalten und kontrolliert werden, um etwaige Pflichtverletzungen ebenfalls zu dokumentieren und zu veröffentlichen. Dies entspräche der Vorgehensweise im Digital Services Act und könnte zur Herstellung von Vertrauen und Akzeptanz der Betroffenen beitragen.

6.3.3 Subjektbezogenes Verständnis

Die obigen Ausführungen stehen unter der Annahme eines subjektbezogenen Verständnisses von Daten. Personenbezogene Daten oder konkret Gesundheitsdaten sind keine Ressource, die mit Wasser oder Boden vergleichbar wäre. Zu berücksichtigen ist vor allem, dass es ohne eine Person kein personenbezogenes Datum gibt, da die Information in Abhängigkeit von einem bestimmten Verhalten oder einem bestimmten Zustand des Betroffenen entsteht. Ein solches Datum stellt gerade das Abbild der Lebensumstände der Einzelnen dar und ist individuell (erzeugt), so dass sich nicht zwangs-

120 Siehe auch Martini 2021, Rn. 60.

läufig das gleiche Recht von Anderen ergibt, dieses auch zu nutzen.[121] Daher muss das subjektbezogene Verständnis aufrechterhalten werden. Würde man Daten frei zirkulieren lassen oder gar zum Allgemeingut erklären, wäre den Betroffenen die Möglichkeit abgeschnitten, ihre grundrechtlich garantierten Rechte auszuüben. Letztendlich garantiert diese Zuordnung nicht nur den Schutz des Persönlichkeitsrechts bzw. den Schutz des informationellen Selbstbestimmungsrechts sowie die Sicherstellung von Kontrollrechten, sondern kann ebenso Gestaltungsrechte und Teilhaberechte der oder des Einzelnen i. S. d. obigen Erwägungen und Ausführungen legitimieren.

7. Fazit und Ausblick

Die Einwilligung verliert in den europäischen Gesetzgebungsakten außerhalb der DS-GVO an Bedeutung, ebenso im Gesundheitssektor, wo gleichermaßen auf nationaler Ebene eine Widerspruchslösung präferiert wird. Mit Blick auf die Rechtspraxis muss im Falle des Inkrafttretens der EHDS-VO der Rechtsanwender im Einzelfall zudem prüfen, ob auch die Vorschriften der DS-GVO anzuwenden sind. Im EHDS-VO-E zeigt sich offenkundig die Tendenz zu einer stärkeren kollektiven Datennutzung, während nach tradiertem Datenschutzrecht eine individualzentrierte Fokussierung vorherrscht.[122]

Besondere Relevanz hat dies vor dem Hintergrund, dass sowohl der Kreis von Nutzungsberechtigten als auch die Zwecke der Datenverarbeitung ausgeweitet werden. Neben der »wissenschaftlichen Forschung« werden ebenso kommerzielle Zwecke der Datenverarbeitung in den Vordergrund gerückt. Vor diesem Hintergrund wurde am Beispiel der Verarbeitung von Gesundheitsdaten untersucht, inwieweit eine strukturelle Ausgestaltung des Datenzugangs die Betroffenenrechte auch ohne Einwilligung gewährleisten und die zugrundeliegende Architektur die Bedingung dafür darstellen kann, dass das öffentliche Interesse an der Verarbeitung von Gesundheitsdaten

121 Siehe im Kontext der verhaltensgenerierten Daten die Studie von Fezer 2018, S. 46 f. Interessant sind in diesem Zusammenhang außerdem die Ausführungen von Pfeiffer zum Digital Markets Act in diesem Band. Er verweist auf die gleiche Stoßrichtung in Art. 6 Abs. 8–11 DMA, da diese sowohl eine Teilhabe von Endnutzern als auch gewerblichen Nutzern an solchen Daten ermöglichen, an deren Generierung sie selbst partizipiert haben.

122 Siehe für den wissenschaftlichen Bereich, die damit verbundenen Datenzugänge sowie zur Teilhabe am Forschungsprozess die Ausführungen von Petra Gehring in diesem Band.

überwiegt und die notwendige Interessenabwägung auf einer technischen und organisatorischen Ebene abgebildet wird. Wichtige Leitplanken sollte der Gesetzgeber dabei selbst festlegen und nicht der Exekutive überlassen, ebenso wenig der Selbstregulierung einer verantwortlichen Stelle. Es ist daher eine Gestaltungsaufgabe des Gesetzgebers, den Datenzugang zu regeln und dabei die Möglichkeiten und Grenzen einer freien Datennutzung und des Allgemeinwohls im Spannungsverhältnis zur informationellen Selbstbestimmung zu bestimmen. Wesentlich ist dabei, das subjektbezogene Verständnis eines personenbezogenen Datums aufrecht zu erhalten, da eine solche untrennbare Beziehung zwischen Datum und Person mitwirkende Gestaltungs- und Teilhaberechte der Betroffenen letztendlich legitimiert. Betroffene dürfen nicht ausgegrenzt werden.

Zwar sind diese Erwägungen nicht ohne weiteres auf andere Sektoren übertragbar, insbesondere da Gesundheitsdaten aufgrund ihrer Sensibilität und der nationalen Gestaltungsmöglichkeiten aus Art. 9 Abs. 2 DS-GVO einem eigenen Anforderungsregime unterliegen können. Dennoch lässt sich daraus insoweit die Schlussfolgerung ziehen, dass die Einwilligung sowohl auf gesellschaftlicher als auch auf rechtlicher Ebene nur dann an Bedeutung einbüßen kann, wenn eine Konkordanz erzeugt wird, die die Interessen der Betroffenen und beteiligten Personengruppen abbildet. Standards und Verhaltensregeln kommen hier eine wichtige Bedeutung zu. Dies bietet bei den angedachten vielfältigen und breiten Datennutzungsmöglichkeiten unterschiedlicher Adressaten die Möglichkeit, das Spannungsverhältnis zwischen einem interessengerechten Datenzugang einerseits und dem Grundrechtsschutz andererseits auf der Basis einer rechtsgestaltenden Mitwirkung zu berücksichtigen.

Literatur

Bäcker, Matthias (2024): Art. 23 DS-GVO in: Kühling, Jürgen/Buchner, Benedikt (Hg.): *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG*, München.

Bäcker, Matthias (2023): Art. 2 DS-GVO, in: Wolff, Heinrich A./Brink, Stefan/von Ungern-Sternberg, Antje (Hg.): *BeckOK Datenschutzrecht. DS-GVO, DA, DGA, BDSG. Datenschutz und Datennutzung*, 47. Edition, Stand 1.8.2023, München.

BfDI [= Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit] (2023): Stellungnahme des Bundesbeauftragten für den Datenschutz und die

Informationsfreiheit zum Entwurf eines Gesetzes zur verbesserten Nutzung von Gesundheitsdaten (Kabinettbeschluss vom 30. August 2023, BR-Drs 434/23 vom 08. September 2023), 28.09.2023, https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Stellungnahmen/2023/StgN_verbesserte-Nutzung-Gesundheitsdaten.pdf?__blob=publicationFile&v=3 [13.05.2024].

Bronner, Pascal (2023): Die Verordnung über einen European Health Data Space (EHDS-VO): Wegbereiterin für die europäische Gesundheitsunion, in: *juris PraxisReport IT-Recht (jurisPR-ITR)*, Heft 18, Anm. 2.

Buchner, Benedikt/Petri, Thomas (2024): Art. 6 DS-GVO, in: Kühling, Jürgen/Buchner, Benedikt (Hg.): *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG*, München.

Bundesrat (2023): Entwurf eines Gesetzes zur Stärkung von Wachstumschancen, Investitionen und Innovation sowie Steuervereinfachung und Steuerfairness (Wachstumschancengesetz), Drucksache 433/1/23 vom 9.10.2023, https://dserver.bundestag.de/brd/2023/0433-1-23.pdf [21.5.2024].

Caspar, Johannes (2019): Art. 89 DSGVO in: Simitis, Spiros/Hornung, Gerrit/Spiecker gen. Döhmann, Indra (Hg.): *Datenschutzrecht. DSGVO mit BDSG*, Baden-Baden.

Dix, Alexander (2019): Art. 23 DSGVO, in: Simitis, Spiros/Hornung, Gerrit/Spiecker gen. Döhmann, Indra (Hg.): *Datenschutzrecht. DSGVO mit BDSG*, Baden-Baden.

DSK [= Datenschutzkonferenz] (2023): Stellungnahme der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 27. März 2023. Nutzung von Gesundheitsdaten braucht Vertrauen – Der Europäische Gesundheitsdatenraum darf das Datenschutzniveau der Datenschutz-Grundverordnung nicht aushöhlen, https://www.datenschutzkonferenz-online.de/media/st/2023-03-27_DSK-Stellungnahme_EHDS.pdf [13.05.2024].

DSK (2020): *Pressemitteilung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 24.04.2020*, https://www.datenschutzkonferenz-online.de/media/pm/20200427_Einwilligungsdokumente_der_Medizininformatik-Initiative.pdf [13.05.2024].

Deutscher Bundestag (2023a): *Entwurf eines Gesetzes zur verbesserten Nutzung von Gesundheitsdaten (Gesundheitsdatennutzungsgesetz – GDNG)*, Drucksache 20/9046 vom 01.11.2023, https://dserver.bundestag.de/btd/20/090/2009046.pdf [21.5.2024].

Deutscher Bundestag (2023b): *Beschlussempfehlung und Bericht des Ausschusses für Gesundheit*, Drucksache 20/9785 vom 13.12.2023, https://dserver.bundestag.de/btd/20/097/2009785.pdf [21.5.2024].

Deutscher Bundestag (2023c): *Entwurf eines Gesetzes zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG)*, Drucksache 20/9048 vom 1.11.2023, https://dserver.bundestag.de/btd/20/090/2009048.pdf [21.5.2024].

Deutscher Bundestag (2023d): Beschlussempfehlung und Bericht des Ausschusses für Gesundheit, Drucksache 20/9788 vom 13.12.2023, https://dserver.bundestag.de/btd/20/097/2009788.pdf [21.5.2024].

Dochow, Carsten (2022): Opt-ionen für die elektronische Patientenakte: Einwilligungs- oder Widerspruchsmodell?, in: *Datenschutz und Datensicherheit (DuD)*, Heft 12, S. 747–755.

Dochow, Carsten (2016): Gesundheitsdatenschutz gemäß EU-Datenschutzgrundverordnung, in: *GesundheitsRecht (GesR)*, Heft 7, S. 401–409.

EDSA [= Europäischer Datenschutzausschuss] (2020): *Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679*, Version 1.1, 4. Mai 2020, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_de.pdf [13.05.2024].

EDSA (2019): Leitlinien 2/2019 zur Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Bereitstellung von Online-Diensten für betroffene Personen, Version 2.0, 08.10.2019, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_de_0.pdf [13.05.2024].

EDSA/ EDSB [= Europäischer Datenschutzausschuss/ Europäischer Datenschutzbeauftragter] (2022): Gemeinsame Stellungnahme 3/2022 des EDSA und des EDSB zum Vorschlag für eine Verordnung über den europäischen Raum für Gesundheitsdaten, 12. Juli 2022, https://edpb.europa.eu/system/files/2023-04/edpb_edps_jointopinion_202203_europeanhealthdataspace_de.pdf [13.05.2024].

DA [= Europäische Kommission] (2023): Verordnung (EU) 2023/2854 des Europäischen Parlaments und des Rates vom 13. Dezember 2023 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung sowie zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie (EU) 2020/1828 (Datenverordnung), Amtsblatt L 2023/2854 vom 22.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2854/oj [21.5.2024].

DGA [= Europäische Kommission] (2022a): Verordnung (EU) 2022/868 des Europäischen Parlaments und des Rates vom 30. Mai 2022 über europäische Daten-Governance und zur Änderung der Verordnung (EU) 2018/1724 (Daten-Governance-Rechtsakt), Amtsblatt L 152 vom 3.6.2022, ELI: http://data.europa.eu/eli/reg/2022/868/oj [21.5.2024].

DS-GVO [= Europäische Kommission] (2016): Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Amtsblatt L 119/1, https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679 [21.5.2024].

DVG [= Deutscher Bundestag] (2019): *Gesetz für eine bessere Versorgung durch Digitalisierung und Innovation (Digitale-Versorgung-Gesetz DVG)*, Bundesgesetzblatt I 49 vom 18.12.2019, S. 2562, https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&start=//*%5b@attr_id=%27bgbl119s2562.pdf%27%5d#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl119s2562.pdf%27%5D__1717511739005 [04.06.2024].

EHDS-VO-E [= Europäische Kommission (2022b): Vorschlag der Europäischen Kommission für eine Verordnung des Europäischen Parlaments und des Rates über den europäischen Raum für Gesundheitsdaten, COM (2022) 197 final, Straßburg, https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52022PC0197 [21.5.2024].

EHDS-VO-PE [= Europäisches Parlament] (2023a): Europäischer Raum für Gesundheitsdaten. Abänderungen des Europäischen Parlaments vom 13. Dezember 2023 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über den Europäischen Raum für Gesundheitsdaten], (COM (2022) 0197 C9-0167/2022 2022/0140/COD)), https://www.europarl.europa.eu/doceo/document/TA-9-2023-0462_DE.pdf [21.5.2024].

EHDS-VO-RE [= Rat der Europäischen Union] (2023): *REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Health Data Space*], 2022/0140(COD), https://data.consilium.europa.eu/doc/document/ST-16048-2023-REV-1/en/pdf [21.5.2024].

Europäisches Parlament (2023b): Draft Compromise Amendments vom 24.11.2023, 2022/0140(COD), https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/CJ43/AMC/2023/11-28/Item4-EHDS-compromiseamendments_EN.pdf [21.5.2024].

Fezer, Karl-Heinz (2018): *Repräsentatives Dateneigentum. Ein zivilgesellschaftliches Bürgerrecht*, Sankt Augustin/Berlin, https://www.kas.de/documents/252038/253252/7_dokument_dok_pdf_52161_1.pdf/f828a351-a2 f6-11c1-b720-1aa08eaccff9?version=1.0&t=1539647605952 [13.05.2024].

Frenzel, Eike M. (2021): Art. 7 DS-GVO, in: Paal, Boris P./Pauly, Daniel A. (Hg.): *Datenschutz-Grundverordnung Bundesdatenschutzgesetz*, München.

Fromm, Veronika (2023): § 67, in: Schlegel, Rainer/Voelzke, Thomas (Hg.): juris Praxis-Kommentar SGB Sozialgesetzbuch Zehntes Buch. Sozialverwaltungsverfahren und Sozialdatenschutz (jurisPK-SGB X), Saarbrücken.

Fröhlich, Wiebke/Spiecker gen. Döhmann, Indra (2022): Die breite Einwilligung (Broad Consent) in die Datenverarbeitung zu medizinischen Forschungszwecken – der aktuelle Irrweg der MII, in: *GesundheitsRecht (GesR)*, Heft 6, S. 346–353.

Geminn, Christian L. (2018): Wissenschaftliche Forschung und Datenschutz. Neuerungen durch die Datenschutz-Grundverordnung, in: *Datenschutz und Datensicherheit (DuD)*, Heft 10, S. 640–646.

Gassner, Ulrich M. (2022): Forschung und Innovation im europäischen Gesundheitsdatenraum. Zur künftigen Sekundärnutzung elektronischer Gesundheitsdaten, in: *Datenschutz und Datensicherheit (DuD)*, Heft 12, S. 739–746.

Graf von Kielmansegg, Sebastian (2023): Der »Broad Consent« in der medizinischen Forschung – kein datenschutzrechtlicher »Irrweg«. Zugleich eine Replik zum Beitrag von Fröhlich/Spiecker, GesR 2022, 346, in: *GesundheitsRecht (GesR)*, Heft 22, S. 681–689.

Grages, Jan-Michael (2023): Art. 23 DSGVO, in: Plath, Kai-Uwe (Hg.): *DSGVO/BDSG/TTDSG*, Köln.

Hallinan, Dara (2020): Broad consent under the GDPR: an optimistic perspective on a bright future, in: *Life Sciences, Society and Policy*, Heft 1, S. 1–18.

Hennemann, Moritz/von Ditfurth, Lukas (2022): Datenintermediäre und Data Governance Act, in: *Neue Juristische Wochenschrift (NJW)*, Heft 27, S. 1905–1910.

Herbst, Tobias (2024): Art. 23 DSGVO, in: Eßer, Martin/Kramer, Philipp/von Lewinski, Kai (Hg.): *Auernhammer DSGVO BDSG Datenschutz-Grundverordnung, Bundesdatenschutzgesetz und Nebengesetze*, Hürth.

Hornung, Gerrit/ Hofmann, Kai (2017): Die Auswirkungen der europäischen Datenschutzreform auf die Markt- und Meinungsforschung, in: *Zeitschrift für Datenschutz (ZD)*, Heft 4, Beilage.

Kampert, David (2022): Art. 9 DS-GVO in: Sydow, Gernot/Marsch, Nikolaus (Hg.): *DS-GVO / BDSG. Datenschutz-Grundverordnung. Bundesdatenschutzgesetz*, Baden-Baden.

Koch, Stefan/Chatard, Yannick (2022): Der Missbrauchseinwand gegen Betroffenenrechte. Eine Standortbestimmung zum Umgang mit datenschutzfremden Motiven, in: *Zeitschrift für Datenschutz (ZD)*, Heft 9, S. 482–486.

Kumkar, Lea K. (2022): Klarnamenpflicht in sozialen Netzwerken unter der Datenschutz-Grundverordnung und § 19 TTDSG, in: *Zeitschrift für Urheber- und Medienrecht (ZUM)*, Heft 7, S. 489–496.

Kühling, Jürgen/Martini, Mario (Hg.) (2016): Die Datenschutz-Grundverordnung und das nationale Recht: Erste Überlegungen zum innerstaatlichen Regelungsbedarf, Münster.

Leopold, Anders (2022): § 67, in: Körner, Anne/Krasney, Martin/Mutschler, Bernd/Rolfs, Christian (Hg.): *beck-online. GROSSKOMMENTAR zum SGB: SGB X (Kasseler Kommentar)*, München.

Lorenz, Luisa (2023a): Die »ePA für alle« zwischen Gesundheits- und Datenschutz (Teil 1). Das für die elektronische Patientenakte angekündigte opt-out-Modell auf dem verfassungs- und EU-datenschutzrechtlichen Prüfstand, in: *Gesundheit und Pflege (GuP)*, Heft 4, S. 132–154.

Lorenz, Luisa (2023b): Die »ePA für alle« zwischen Gesundheits- und Datenschutz (Teil 2). Das für die elektronische Patientenakte angekündigte opt-out-Modell auf dem verfassungs- und EU-datenschutzrechtlichen Prüfstand, in: *Gesundheit und Pflege (GuP)*, Heft 5, S. 165–183.

Lorenz, Luisa/Schild, Hans-Hermann (2023): Datenübermittlung an GKV-Spitzenverband im Datentransparenzverfahren, in: *Zeitschrift für Datenschutz (ZD)*, Heft 3, S. 167–171.

Lupiáñez-Villanueva, Francisco/ Gunderson, Laura/ Vitiello, Simone/ Febrer, Nuria/ Folkvord, Frans/ Chabanier, Loic/ Filali, Nihal/ Hamonic, Raphaël/ Achard, Eline/ Couret, Hélène/ Arredondo, Maria Teresa/ Cabrera, Maria Fernanda/ García, Rebeca/ López, Laura/ Merino, Beatriz/ Fico, Giuseppe (2021): *Study on Health Data, Digital Health and Artificial Intelligence in Healthcare*, Brüssel, https://op.europa.eu/de/publication-detail/-/publication/179e7382-b564-11ec-b6 f4-01aa75ed71a1/language-en [13.05.2024].

Martini, Mario (2021): Art. 21 DS-GVO, in: Paal, Boris P./Pauly, Daniel A. (Hg.): *Datenschutz-Grundverordnung Bundesdatenschutzgesetz*, München.

McKinsey & Company (2022): *Digitalisierung im Gesundheitswesen: die 42-Milliarden-Euro-Chance für Deutschland*, https://www.mckinsey.de/~/media/mckinsey/locations/europe%20and%20middle%20east/deutschland/news/presse/2022/2022-05-

24%2042-mrd-euro-chance/220524_mckinsey_die%2042-mrd-euro-chance.pdf [13.05.2024].

Mester, Britta A. (2022): Art. 9 DSGVO, in: Taeger, Jürgen/Gabel, Detlev (Hg.): *DSGVO BDSG TTDSG*, München.

Moreno, Anna (2023): Mehr Gemeinwohlorientierung in der Datennutzung – Der Entwurf eines Gesundheitsdatennutzungsgesetz, in: *GesundheitsRecht (GesR)*, Heft 11, S. 689–694.

Netzwerk Datenschutzexpertise GbR (2023a): Stellungnahme des Netzwerks Datenschutzexpertise zum Entwurf eines Gesetzes zur verbesserten Nutzung von Gesundheitsdaten (Gesundheitsdatennutzungsgesetz GDNG-E), BT-Drs. 20/9046 (=BR-Drs. 434/23), https://www.netzwerk-datenschutzexpertise.de/sites/default/files/2023_stn_gdng.pdf [13.05.2024].

Netzwerk Datenschutzexpertise GbR (2023b): Gesundheitsdatennutzung contra heilberufliche Vertraulichkeit. Eine Kritik am Referentenentwurf für ein Gesundheitsdatennutzungsgesetz, https://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2023_08_gdng.pdf [13.05.2024].

Paal, Boris P. (2021): Art. 23 DS-GVO, in: Paal, Boris P./Pauly, Daniel A. (Hg.): *Datenschutz-Grundverordnung Bundesdatenschutzgesetz*, München.

Petri, Thomas (2019): Art. 9 DS-GVO in: Simitis, Spiros/Hornung, Gerrit/Spiecker gen. Döhmann, Indra (Hg.): *Datenschutzrecht. DSGVO mit BDSG*, Baden-Baden.

Peuker, Enrico (2022): Art. 23 DSGVO, in: Sydow, Gernot/Marsch, Nikolaus (Hg.): *DS-GVO / BDSG. Datenschutz-Grundverordnung. Bundesdatenschutzgesetz*, Baden-Baden.

Roßnagel, Alexander (2017): § 2 Anwendungsvorrang des Unionsrechts, in: ders. (Hg.): *Europäische Datenschutz-Grundverordnung. Vorrang des Unionsrechts Anwendbarkeit des nationalen Rechts*, Baden-Baden, S. 67–77.

Sachverständigenrat zur Begutachtung der Entwicklung im Gesundheitswesen (2021): *Digitalisierung für Gesundheit, Ziele und Rahmenbedingungen eines dynamisch lernenden Gesundheitssystems*, Gutachten 2021, https://www.svr-gesundheit.de/fileadmin/Gutachten/Gutachten_2021/SVR_Gutachten_2021.pdf [13.05.2024].

Savary, Fiona (2023): § 19, in: Steinrötter, Björn (Hg.): Europäische Plattformregulierung. DSA | DMA | P2B-VO | DGA | DA | AI Act | DSM-RL, Baden-Baden.

Schlegel, Rainer/Voelzke, Thomas (Hg.) (2023): juris PraxisKommentar SGB Sozialgesetzbuch Zehntes Buch. Sozialverwaltungsverfahren und Sozialdatenschutz (jurisPK-SGB X), Saarbrücken.

Specht-Riemenschneider, Louisa (2023): Datennutz und Datenschutz: Zum Verhältnis zwischen Datenwirtschaftsrecht und DSGVO, in: *Zeitschrift für Europäisches Privatrecht (ZEuP)*, Heft 3, S. 638–672.

Specht-Riemenschneider, Louisa (2022): Der Entwurf des Data Act. Eine Analyse der vorgesehenen Datenzugangsansprüche im Verhältnis B2B, B2C und B2G, in: *Zeitschrift für IT-Recht und Recht der Digitalisierung (MMR)*, Beilage, S. 809–826.

Stellpflug, Martin H./Hildebrandt, Ronny/Middendorf, Max (Hg.) (2023): Gesundheitsrecht: Kompendium für die Rechtspraxis, Heidelberg.

Taeger, Jürgen (2022): Art. 7 DSGVO, in: Taeger, Jürgen/Gabel, Detlev (Hg.): *DSGVO BDSG TTDSG*, München.

Werkmeister, Christoph/Schwaab, Michael (2019): Auswirkungen und Reichweite des datenschutzrechtlichen Forschungsprivilegs, in: *Computer und Recht (CR)*, Heft 2, S. 85–90.

Weichert, Thilo (2024): Art. 9 DS-GVO, in: Kühling, Jürgen/Buchner, Benedikt (Hg.): *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG*, München.

Weichert, Thilo (2020a): Die Forschungsprivilegierung in der DS-GVO. Gesetzlicher Änderungsbedarf bei der Verarbeitung personenbezogener Daten für Forschungszwecke, in: *Zeitschrift für Datenschutz (ZD)*, Heft 1, S. 18–24.

Weichert, Thilo (2020b): »Datentransparenz« und Datenschutz, in: *Medizinrecht (MedR)*, Heft 7, S. 539–546.

Westphal, Dirk (2023): § 67 SGB X, in: Rolfs, Christian/Giesen, Richard/Meßling, Miriam/Udsching, Peter (Hg.): *BeckOK Sozialrecht*, München.

Ziegler, Ole (2019): L. Datenschutzrecht im Gesundheitswesen, in: Stellpflug, Martin H./Hildebrandt, Ronny/Middendorf, Max (Hg.): *Gesundheitsrecht: Kompendium für die Rechtspraxis*, Heidelberg.

Datenzugangssouveränität: Selbstbestimmung, Schutz und Nutzen in einer digitalen Welt

Frank Niggemeier[1]

I. Ziel und Bezugsrahmen

Im Zusammenhang mit den Worten »Daten« und »Datenzugänge« ist das Wort »Souveränität« (wieder) in Mode gekommen. Und das nicht nur in Bezug auf Staaten, sondern auch auf Individuen: Der einzelne Mensch soll, so eine gängige Vorstellung, über »seine« Daten und den Zugang zu ihnen »souverän« entscheiden können. Oder, in den Worten einer Fernsehjournalistin in einem Tagesthemen-Kommentar zu den Plänen einer sog. Opt-out-ePA[2]: »Meine Daten gehören mir«[3]. Dergleichen Vorstellungen finden sich in vielen Varianten, als Forderung oder als Ziel deklariert, in Texten von Regierungen, Parteien, Unternehmen.

Den bereits zahlreichen, aus unterschiedlichen Perspektiven vorgenommenen Rekonstruktionen[4] des noch sehr fluiden, nicht selten flachen

1 Der Beitrag bringt ausschließlich die persönliche Ansicht des Verfassers zum Ausdruck.

2 Das Kürzel »Opt-out-ePA« steht für das Konzept einer umfassenden »elektronischen Patientenakte (ePA)«, wie es der Sachverständigenrat Gesundheit und Pflege in seinem im März 2021 erschienen Gutachten »Digitalisierung für Gesundheit« beschrieben hat (Sachverständigenrat 2021, S. 65 ff.). Diese ePA soll grundsätzlich für jeden Versicherten angelegt werden (der sie aber ablehnen kann). Im Koalitionsvertrag vom November 2021 (S. 83) wurde vereinbart: »Alle Versicherten bekommen DSGVO-konform eine ePA zur Verfügung gestellt; ihre Nutzung ist freiwillig (opt-out).« Mit dem im Dezember 2023 verabschiedeten Gesetz zur Beschleunigung der Digitalisierung des Gesundheitswesens (DigiG) wurde dieses Vorhaben umgesetzt, wenn auch nicht in allen Aspekten so, wie der Sachverständigenrat es ausgeführt hatte. Siehe unten Absatz VII und aus einer Perspektive de lege lata in diesem Band insbesondere der Beitrag von Böning/Riechert.

3 So die Formulierung in einem Tagesthemen-Kommentar vom 9.3.2023 – siehe https://x.com/tagesthemen/status/1633950783912779776 [29.5.2024].

4 Näheres findet sich in den Beiträgen in Augsberg/Gehring 2022.

Sprachspiels[5] mit diesen Vokabeln will vorliegender Beitrag nicht eine weitere hinzufügen. Vielmehr möchte er aus einer Perspektive philosophischer Ethik Anregungen geben, sich über die sehr unterschiedlichen Verwendungen dieses Wortes klarer zu werden und das Diskurselement »Einwilligung« (in Datenerhebung und -nutzung), das oft als Ausdruck von »Souveränität« verstanden wird, eher als praktische Selbstbestimmung zu denken, die – eigenen und / oder fremden – Nutzen intendiert und in lebensweltlichen Zusammenhängen erfolgt, die es zu beachten gilt, wenn man den Intentionen der Einwilligenden gerecht werden und den entsprechenden *Ge*brauch der Daten ermöglichen und sie vor *Miss*brauch *wirksam* schützen will.

Als Bezugsrahmen nehmen diese Anregungen die Werteordnung einer freiheitlichen, demokratischen Rechts- und Solidargemeinschaft, wie sie für die Deutschland vor allem in Art. 1–20 GG und für die Europäische Union in den Werten und Grundsätzen der EU-Verträge beschrieben ist. Die Anbindung an ein real *geltendes* Normengefüge erlaubt, ethischen *Anwendungsfragen* nachzugehen und rein theoretische Fragen wie die nach Letztbegründung der in Anschlag gebrachten Normen zurückzustellen. Zweifellos sind die beiden genannten, miteinander verschränkten Normengefüge nicht erst im *juristischen* Zusammenhang, sondern gerade auch bei Anwendung auf eine *ethische* Frage auslegungs- und abwägungsbedürftig. Doch das macht zugleich den Reiz und einen potenziellen Mehrwert des Versuchs aus.

Angewandte Ethik ist zwar eine akademische, an Universitäten gelehrte Disziplin[6] und hat insofern verschiedenste theoretische Ansätze und Ausprägungen. Insofern sie aber versucht, Fragen zu beantworten (oder zumindest Kriterien für die Beantwortung durch Gesellschaft und Politik zu erörtern), die sich in einem konkreten räumlichen und zeitlichen Zusammenhang stellen – z.B. die Frage: Wie wollen wir – *jetzt, in Deutschland* – den Umgang mit Daten gestalten? –, liegt es zumindest nahe, die in diesem *Raum* zu dieser *Zeit* geltende *Werteordnung*, im Beispielsfall also vor allem die des

5 Dass es in »Sprachspielen« zumeist um sehr ernste Dinge geht, ist von Wittgenstein her klar. Um dies deutlich zu machen, wird hier alternativ die von Habermas und anderen ins Begriffliche gehobene Vokabel »Diskurs« verwendet.

6 In der Regel als sogenannte Bereichsethik (z.B. Medizin-, Umwelt- oder Wirtschaftsethik) und *getrennt* von der Praktischen Philosophie als Teil der Philosophie. Auf die bedenkenswerte Kritik u.a. von Böhme (2008, S. 11) an der »Trennung von theoretischer und angewandter Ethik" kann im Rahmen dieses Beitrags nur hingewiesen werden, ebenso auf die grundsätzliche Kritik von Gehring (2006 und 2024) insbesondere an dem im Sinne Foucaults verstandenen Machtdispositiv »Bioethik/Biopolitik«.

deutschen Grundgesetzes, in Betracht zu ziehen. Angewandte Ethik könnte *diese* Werteordnung auf den Gegenstand ihres konkreten Nachdenkens (z. B. auf den Umgang mit Daten in Deutschland) anwenden, genauer: sie zum Bezugspunkt ihrer Reflexion auf das zuvor in seinem Sachgehalt erschlossene lebensweltliche *Phänomen* (hier »Daten«) nehmen. Dies schließt nicht aus, dass eine *kritische* Reflexion der sachlichen wie normativen Gehalte Änderungsbedarf erkennen lässt – in Bezug etwa auf gesellschaftlich gepflegte »Wertvorstellungen« oder auf rechtliche Regelungen (also in einer Perspektive de lege ferenda).

Wie so häufig bei modischer Semantik lässt die muntere, manchmal fast mantrische Nutzung der Vokabel »Souveränität« in Texten, die um Daten und die Zugänge zu ihnen kreisen, oft die begriffliche Klarheit vermissen, die zur *Erhellung* des Behandelten gefordert wäre. Letztere anzustreben wäre nicht nur aus akademischem Gusto, sondern auch aus dem Bedarf an handlungsorientierender Erschließung einer komplexen Lebenswirklichkeit wie der Digitalisierung und der Möglichkeiten, *mit* ihr umzugehen oder, vielleicht treffender: sich *in* ihr zu verhalten, wünschenswert, ja theoretisch wie praktisch geboten. Dass auf dem Weg zu solcher Erschließung begriffliche »Ambiguität [auch] als Chance« verstanden und genutzt werden kann[7], ist sicher fruchtbarer als bloßes beckmesserisches Beharren auf etabliertem Sprachgebrauch. Unsere Begriffe entspringen nicht wie die personifizierte Weisheit im altgriechischen Mythos ausgereift und bestens zum Kampf der Argumente gerüstet dem Haupt der höchsten Gottheit, sondern sie werden geboren, manchmal auch adoptiert – wie »Souveränität« im Datendiskurs –, und sie müssen und sollten sich entwickeln. »In der Auseinandersetzung um (neue) Begriffe wird ein Stück Zukunft verhandelt.«[8] In dieser Verhandlung ist zugleich die Gefahr zu vermeiden, dass »Souveränität« zum Buzzword wird oder Erwartungen weckt, die so etwa im Hinblick auf Datenzugänge nicht eingehalten werden *können*, vielleicht auch – aufgrund handlungstheoretischer und normativer[9] Abwägungen – so nicht eingehalten werden *sollten*.

7 So Augsberg/Gehring 2022, S. 8.
8 Ebd.
9 Fischer-Bollin 2021, S. 1.

II. Souveränität als *Begriff*

Beim Wort »Souveränität« lassen sich zwei Verwendungsverweisen unterscheiden, die im Folgenden die »klassische« und die »metaphorische« genannt werden sollen.

Die klassische Verwendung bezieht »Souveränität« – im Kontext dieses Sammelbands oft durch das Attribut »digital« spezifiziert – auf ein national oder supranational organisiertes Gemeinwesen wie etwa die Bundesrepublik Deutschland oder die Europäische Union. Dieser Sprachgebrauch knüpft an die einschlägigen Texte politischer Philosophie, der Staatstheorie und des Völkerrechts an, die dem Wort eine gewisse *begriffliche* Klarheit verschafft und es zugleich durch die ihm zugeschriebenen »hohen« Bedeutungen auratisch aufgeladen haben.

Manche sehen den Souveränitätsbegriff so stark mit dem neuzeitlichen Nationalstaat und der Vorstellung von dessen umfassender »Unabhängigkeit nach außen und nach innen« verbunden, dass sie bereits seine Anwendung auf die EU für irreführend halten, ja vor den »Gefahren eines unerfüllbaren Versprechens« warnen – so z.B. Fischer-Bollin, dessen Analyse sich vor allem auf »Sicherheitspolitik als Kernbereich staatlicher Souveränität« bezieht, aber »den digitalen Bereich« explizit als Beispiel nennt[10]. Richtig ist, dass die EU, deren Kompetenzen auf dem Prinzip der begrenzten Einzelermächtigung durch die Mitgliedstaaten beruhen, rechtlich keine umfassende Souveränität hat (im Sinne einer »Kompetenzkompetenz«), sondern nur »souverän« ist, soweit die Mitgliedstaaten als die »Herren der Verträge« definierte (Teil-)Souveränität auf sie übertragen haben (in den Anfängen z.B. die Regelungshoheit über Kohle und Stahl, dann über Sicherheits- und Qualitätsstandards für Güter und Dienstleistungen aller Art zur Realisierung des Binnenmarktes). Mit Art. 39 EUV (für den »Datenschutz« im Bereich der Gemeinsamen Außen- und Sicherheitspolitik) und Art. 16 AEUV (für den »Schutz personenbezogener Daten« – innerhalb der EU und gegenüber Drittstaaten) gibt es allerdings eine primärrechtliche Kompetenzübertragung, so dass vorliegender Beitrag nicht weiter differenziert, inwiefern

10 »Gefahren eines unerfüllbaren Versprechens« könnten a forteriori drohen, wenn man den Souveränitätsbegriff von der Sphäre des Staatlichen auf die des Individuums überträgt, vor allem wenn dabei nicht kritisch untersucht wird, was das Individuum »staatsgleich« überhaupt leisten kann.

Daten(zugangs)souveränität von einem nationalstaatlichen, inwiefern von einem supranationalen *politischen* Akteur realisiert werden kann und soll:

In der »klassischen« Verwendung wird das Wort »Souveränität« mit drei Dimensionen verbunden[11], die je nach Autor und Standpunkt unterschiedlich hervorgehoben werden, aber sich austarieren und zusammendenken lassen. Das Wort bezeichnet, in innerstaatlicher Perspektive, zum einen die höchste, durch nichts und niemanden eingeschränkte (»absolute«) Macht und ihre Ausübung. Die einseitige oder sogar alleinige Hervorhebung dieser Dimension führte in der Vergangenheit zu absolutistischen Konzeptionen, in denen dann *ein* Mensch, als »Souverän« gedacht (im Unterschied zu seinen »Untertanen«), über jeglichem Gesetz steht (insofern er es erlassen, als oberster Richter anwenden und wiederum als Gesetzgeber verändern oder aufheben kann).

»Souveränität« bezeichnet in innerstaatlicher Perspektive zum anderem, insbesondere in demokratietheoretischer Wendung, die legitimierende Quelle solcher Macht – beispielhaft in der grundgesetzlichen Formel »Alle Staatsgewalt geht vom Volke aus«[12] – und bindet sie damit normativ, d.h.: schränkt insoweit ihre Absolutheit ein.[13] Dabei bleiben der Charakter dieser Bindung, ihre Durchsetzung und Kontrolle sowie nicht zuletzt die Bezugsgröße »Volk« näher zu bestimmen, etwa im Rahmen einer Verfassung und weiteren gesetzten Rechts. Die Verbindung zur ersten Dimension lässt sich darin sehen, dass in einer repräsentativen Demokratie letztlich »das Volk« die höchste Gewalt ist, die es dann im Wege der Gewaltenteilung ausübt, indem es durch gewählte Repräsentanten Gesetze erlässt, sie anwendet (Recht wird »im Namen des Volkes« gesprochen), sie umsetzt (durch die

11 Siehe hierzu ausführlicher der instruktive Überblick von Gehring 2022, 21 ff.

12 »Ursprünglicher Souverän« ist demnach nicht jeder einzelne, sondern eine (durch welche Momente auch immer definierte) Gemeinschaft von einzelnen. Diesen Zusammenhang der – in einem demokratischen Rechtsstaat – *kollektiven* Konstituierung von Souveränität verwischt das vom Deutschen Ethikrat in der Stellungnahme »Big Data und Gesundheit« vorgeschlagene Souveränitätsverständnis, wonach der »Souveränitätsanspruch des ursprünglichen Souveräns« der *jedes* Individuums sei, dem deshalb »weitreichende Kontrollmöglichkeiten« zustünden (Deutscher Ethikrat 2017, S. 203).

13 Insofern ein absolutistischer Herrscher als »von Gottes Gnaden« eingesetzter Souverän gedacht wird, könnte diese Denkfigur selbst ihn binden (insofern er nicht gegen die Gebote des ihn legitimierenden Gottes verstoßen darf). Auch das Konzept »natürlicher Rechte« eines jeden Menschen qua Mensch, das im Rahmen der Naturrechtslehre entwickelt wurde, schränkt absolute Verfügungsgewalt über »Untertanen« grundsätzlich ein. Siehe z.B. Welzel 1980, insbesondere S. 48–161.

Exekutive einschließlich – im Rahmen des Gewaltmonopols – Polizei und Armee), sie verändert und aufhebt.

Drittens steht »Souveränität« in zwischenstaatlicher Perspektive für die »Hoheit« der Staaten, die auf die Achtung der Unverletzlichkeit ihres jeweiligen Territoriums sowie des Lebens und des Eigentums ihrer Bürger bestehen – und dies notfalls mit (militärischer) Gewalt verteidigen. Auch das Prinzip der Nicht-Einmischung in die inneren Angelegenheiten des jeweils anderen ist Ausdruck dieses Verständnisses von Souveränität in seiner zwischenstaatlichen Dimension.

Von dieser »klassischen« Verwendung, in der das Wort »Souveränität« zumindest gewisse begriffliche Klarheit erlangte, wird hier die »metaphorische« unterschieden – für den Zweck dieses Beitrags verstanden als »übertragener Gebrauch«: also Anwendung eines im Hinblick auf *einen* Wirklichkeitsbereich (hier: den Staat) bestimmten Begriffs auf einen anderen Wirklichkeitsbereich – z.B. den einzelnen Menschen. Dass alle Begriffe ursprünglich metaphorisch waren – wie das Wort »Begriff« selbst noch immer, fast handgreiflich, zeigt – und wie sie gerade in ihrer Metaphorizität neue Sinnhorizonte erschließen können, ist eigener erkenntnistheoretischer Erörterungen wert[14], hier aber nicht zielführend, da es »nur« darum gehen soll aufzuhellen, inwieweit konkrete Bestimmungsmomente, die begriffsgeschichtlich in staatstheoretischem Kontext entwickelt und mit dem Wort – um nicht zu sagen »Namen«[15] – Souveränität verbunden wurden, auf einzelne Menschen und den Zugang zu sie betreffenden Daten mit Erkenntnisgewinn übertragen werden können[16] und in welchen Hinsichten

14 Siehe exemplarisch Blumenberg 2013.

15 Siehe das provokante Dictum Hegels (1975 [1830], § 462 Anmerkung): »Es ist in Namen, dass wir denken.« Der »Name« ist »*Äußerlichkeit*«, steht aber durch »Assoziation« für »die *Sache*, wie sie *im Reiche der Vorstellung* […] Gültigkeit hat.« (Hervorhebungen im Original).

16 Hiervon zu unterscheiden ist, wenn z.B. Gernot Böhme 2008, S. 149 im Hinblick auf das Individuum eine *neue* Verwendung des Wortes »Souveränität« vorschlägt: Er setzt dem »Ideal des autonomen Menschen« im Sinne eines »intelligible[n] […] leiblose[n], unberührbare[n] Subjekt[s]« »das Ideal des souveränen Menschen« entgegen. Dieser Mensch sei »souverän […], insofern er sich etwas geschehen lassen kann«, er sei »das Subjekt, das anerkennt, dass es nicht Herr im eigenen Hause ist, das Subjekt, zu dem Erleiden ebenso gehört wie das Handeln.« Mit diesen in sich nachvollziehbaren Bestimmungsmomenten schafft Böhme einen neuen Begriff von Souveränität in Bezug auf den Einzelnen. Dieser neue Begriff löst sich von den denkgeschichtlich entwickelten staatstheoretischen Bestimmungsmomenten von Souveränität. Er lebt eher vom Kontrast, versucht auf jeden Fall nicht, in einem semantischen Hütchenspielertrick »Bedeutung« vom homophonen Vetter zu erschleichen.

eine solche Übertragung eher zu Missverständnissen oder gar in die Irre führt.

III. Souveränität im Umgang mit Daten und Digitalisierung

Alle drei Dimensionen des klassischen Souveränitätsbegriffs lassen sich auf den Umgang mit digitalen Daten[17] und Infrastrukturen beziehen – und sei es als Kontrastfolie, die helfen kann, Punkte auszumachen, an denen Souveränität im Hinblick auf Daten (und »Digitalität« insgesamt) vielleicht anders gedacht und realisiert werden muss als in der analogen Welt von Staatsgrenzen, Bodenschätzen u.ä. Zum Beispiel lässt sich im Hinblick auf das erste Begriffsmoment von Souveränität als höchster Macht fragen, ob in der Welt des Digitalen Souveränität im einseitigen Sinne von Absolutheit, das hieße wörtlich: der völligen Losgelöstheit, totalen Unabhängigkeit von allen anderen Digitalsystemen und Datenmengen außerhalb der digital- und datensouverän sein wollenden politischen Entität faktisch realisierbar und ethisch-normativ geboten wäre. Von der Beantwortung beider Fragen hängt die nach zu erlassenden Gesetzen und anderen zu ergreifenden Maßnahmen ab.

An der faktischen Realisierbarkeit einer so weitreichenden Souveränität lässt sich mit guten Gründen zweifeln: »A Europe fit for the digital age« war eine der sechs Hauptaufgaben, die Ursula von der Leyen in ihrer Bewerbungsrede für das Amt der EU-Kommissionspräsidentin 2019 programmatisch skizzierte – mit der einschränkenden Anmerkung: »It may be too late to replicate hyperscalers, but it is not too late to achieve *technological sovereignty* in some critical technology areas.«[18]

»Technologische Souveränität in einigen kritischen Technologiebereichen« dürfte gegenüber der Vorstellung einer »absoluten« Daten-Autarkie eine realistischere, in sich wiederum durchaus ambitionierte Zielsetzung

17 Warum es sinnvoll ist, die Rede von digitalen Daten *nicht* als pleonastische zu verstehen, wird im Folgenden (insbesondere in Abschnitt VI) erläutert.

18 Von der Leyen 2019a, S. 13 (Hervorhebung vom Verfasser). Der zitierte Satz lautet in der offiziellen deutschen Übersetzung: »Es mag zu spät sein, um Hyperscaler zu replizieren, aber es ist nicht zu spät, um in einigen kritischen Technologiebereichen eine technologische Vorreiterstellung zu erreichen.« von der Leyen 2019b, S. 15. In der Formulierung »technologische *Vorreiterstellung*« klingt stärker eine wettbewerblich-wirtschaftspolitische Zielsetzung an, während »technological *sovereignty*« eher die hier skizzierten drei Dimensionen des klassischen Souveränitätsbegriffs aufruft.

sein.[19] Manche mögen diese dennoch als Defätismus gegenüber faktischer Übermacht und Nichtmehreinholbarkeit – etwa der »hyperscalers« in den USA und China– werten, andere als eine womöglich sogar »ethisch«[20] gebotene Übertragung der »Großvokabel«[21] Souveränität. Zu dieser Übertragungsarbeit würden dann Aktivitäten wie die Entwicklung eines den »europäischen Werten« entsprechenden Rechtsrahmens oder die Schaffung eigenständiger digitaler Infrastrukturen gehören. Die EU-Datenschutzgrundverordnung und das Gaia-X-Projekt[22] wären jeweils ein Beispiel für solche Bemühungen. Unter Adaptierung des klassischen Souveränitätskonzepts an das Digitale wären auch die rechtliche Regulierung und technische Realisierung der Rahmenbedingungen zu subsumieren, unter denen der eine Souverän (z.B. die EU) zu gemeinwohldienlichen Zwecken und unter strengen Auflagen z.B. Gesundheitsdaten aus seinem jeweiligen Souveränitätsbereich mit einem anderen Souverän (z.B. den USA oder Israel) wechselseitig teilt.

Nun ist schon die innerstaatliche Datennutzung dem »Souverän« offensichtlich nur insofern möglich, als er gesetzliche und technische Verfügungsgewalt über die entsprechenden Daten hat – etwa durch eine gesetzliche Befugnisnorm, deren Schaffung Art. 9 Abs. 2 litt. a-j) Datenschutzgrundverordnung sowohl auf EU- als auf Mitgliedstaaten-Ebene ermöglicht. Dabei wird der tatsächliche Zugang zu und die Auswertung von Daten in demokratischen Rechtsstaaten in der Regel vermittelt und zwischen verschiedenen Instanzen aufgeteilt sein (z.B. zwischen Banken und Finanzämtern oder Krankenhäusern, Arztpraxen und Krankenkassen usw.) und nur unter wohldefinierten Bedingungen staatlichen Instanzen selbst erlaubt sein (z.B. im Rahmen von Ermittlungen). Mit allen einschlägigen Regelungen wird »Souveränität« – ob über Daten oder Infrastrukturen – an die legitimierende Quelle eben auch digitaler Machtausübung gebunden

19 Dafür spricht auch, dass von der Leyen die bescheidenere Formulierung »A Europe fit for the digital age« wählte – nicht etwa »Building a digitally sovereign EU«.

20 »Ethisch geboten«, insofern es zu einer Angewandten Ethik gehören könnte, das politisch jeweils erreichbare Gute (z.B. eine gewisse »technologische Souveränität«) zu identifizieren und zu verwirklichen. Dabei darf »das Erreichbare« weder wegen kurzsichtiger Partikularinteressen noch aus Defätismus oder Bequemlichkeit zu klein gedacht, sondern muss um des »bonum commune« willen ehrgeizig konzipiert werden. »Pushing the limits of the feasible« könnte die Maxime einer solchen Ethik der Realpolitik lauten.

21 Gehring 2022, S. 21.

22 Siehe hierzu die Darstellung von Person/Schütrumpf 2022.

– und damit die zweite Dimension des klassischen Souveränitätsbegriffs realisiert. Zugleich gibt diese Rückbindung der Ausgestaltung der dritten Dimension, der Durchsetzung der jeweiligen Hoheitsrechte gegenüber anderen »Souveränen«, die Richtung vor.

Die Finalität der internen und externen Machtausübung in Bezug auf Daten wird beispielhaft unter den »Allgemein geltenden Bestimmungen« des Vertrags über die Arbeitsweise der Europäischen Union deutlich gemacht:

»(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten. (2) Das Europäische Parlament und der Rat erlassen […] Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union sowie durch die Mitgliedstaaten im Rahmen der Ausübung von Tätigkeiten, die in den Anwendungsbereich des Unionsrechts fallen, und über den freien Datenverkehr. Die Einhaltung dieser Vorschriften wird von unabhängigen Behörden überwacht.« Art. 16 AEUV

Diese Bestimmungen übersetzen normative Grundvorstellungen von der Art und Ausübung digitaler Souveränität in einem demokratischen Rechtswesen in die Sprache des EU-Primärrechts, darauf gründende sekundärrechtliche Vorschriften buchstabieren sie aus. Der Leitmaßstab, aber nicht das einzige Schutzgut, ist dabei das Individuum und sein Recht auf *Schutz* der es »betreffenden personenbezogenen Daten« – nota bene: nicht *seiner* Daten im Sinne von Eigentum, erst recht nicht von »Souveränität«. Der Einzelne kann nicht im selben Sinne digital- oder daten-souverän sein wie die politische Entität, die hier auf den Schutz persönlicher Daten verpflichtet wird – und auf eine mit diesem Ziel vereinbare Regelung des »freien Datenverkehrs«: offensichtlich ein anderes, wenngleich einschränkbares Schutzgut. Mit der Achtungs- und Schutzverpflichtung werden zugleich Handlungsoptionen des politischen Souveräns – insbesondere im Sinne der oben skizzierten zweiten (legitimierenden) Dimension staatstheoretischer Souveränität – bewusst beschränkt.

IV. Souveränität – Macht – Schutz

Das Konzept von »Schutz« impliziert zum einen eine Machtasymmetrie zwischen dem Schützenden und dem Geschützten resp. Schutzbedürftigen, zum anderen ein »Wovor«. Zum Schützen ist derjenige verpflichtet, der

die Macht dazu hat[23]. Geschützt werden muss vor Schädlichem – nicht vor Nützlichem. Das Schädliche, vor dem der Einzelne im Zusammenhang ihn betreffender Daten geschützt werden muss, ist zweifellos ein Gebrauch dieser Daten, der dem Individuum nicht nur nichts nützt, sondern ihm womöglich schadet, also als *Missbrauch* zu kennzeichnen ist, der etwa zur Stigmatisierung, Diskriminierung oder Benachteiligung führt. Selbst wenn objektiver Schaden nicht eintreten sollte – bereits der nicht autorisierte Zugriff auf persönliche Daten wäre eine Schädigung des Selbstbestimmungsrechts durch Verletzung der Privatsphäre. Vor all diesen Schäden muss der »Souverän« (ob nun ein Nationalstaat oder ein supranationales Gebilde wie die EU) »seine« Bürgerinnen und Bürger durch geeignete gesetzliche, administrative, technische Maßnahmen (z.B. die digitale Infrastruktur betreffend) schützen.

Damit ist allerdings Selbstschädigung des Individuums grundsätzlich nicht ausgeschlossen: Die Achtung vor der Selbstbestimmung des Einzelnen gebietet es dem Staat, ihn – zumindest in der Regel – nicht daran zu hindern, persönliche Daten von sich aus preiszugeben, indem er z.B. googelt, Facebook oder Dating-Apps nutzt. Dass diese Dienste nicht aus Altruismus angeboten werden, sondern Geschäftsmodelle sind, in denen der Einzelne mit »seinen« Daten bezahlt, deren Analyse sowohl die Dienstleistung verbessern, aber auch (z.B. durch Werbeeinnahmen) Profite steigern und zu anderen Zwecken (z.B. der Steuerung von Menschen im Sinne privatwirtschaftlicher oder politischer Interessen) benutzt werden kann, sollte jedem Zeitgenossen klar sein. Noch stärker gilt dies für die Preisgabe des individuellen genetischen Codes, die erfolgt, indem ein Individuum z.B. eine Speichelprobe zu einer Genomanalyse an ein US-Unternehmen wie »23andMe« oder eine Blutprobe für einen Pränataltest an ein chinesisches

23 Diese Asymmetrie ist ein zentraler Punkt in Hans Jonas' »Versuch einer Ethik für die technologische Zivilisation«. Was er primär auf das Individuum bezieht, lässt sich mutatis mutandis auch »den Staat« beziehen: Sofern »das Schicksal Anderer […], durch Umstände oder Vereinbarung, in meine Hut [im Sinne von Obhut – Vf.] gekommen« ist, schließt »meine Kontrolle da*rüber* zugleich meine Verpflichtung da*für*« ein (Jonas 1979, S. 176, Hervorhebungen im Original). Dieses von Jonas individualethisch gedachte Prinzip würde verallgemeinert lauten: »Je größer die Macht des Handelnden, um so größer die Verantwortung für das von dieser Macht Abhängige.« Niggemeier 2002, S. 142. Zur »Macht« könnte wiederum *auch* die grundsätzliche Verfügungsgewalt (»Datensouveränität«) bzw. »das Recht jeder Person auf Schutz der sie betreffende Daten« (Art. 16 AEUV) gehören – siehe hier im Abschnitt VIII die Überlegung zu Datenteilungspflichten nach Jonas und Lévinas.

Unternehmen wie die BGI Group[24] sendet. In beiden Fällen verfügen dann Stellen, die nicht im deutschen oder EU-Hoheitsgebiet angesiedelt sind, über die genomischen Daten der einsendenden Individuen (und, zumindest teilweise, ihrer Blutsverwandten). Insbesondere in der KI-gestützten Analyse dieser Daten liegt großes Nutzen- wie Schadenspotenzial. Letzteres z.B. in der Entwicklung von Biowaffen, die aufgrund der Ausrichtung an bestimmten genetischen Merkmalen nur bestimmte Populationen schwer erkranken lassen könnten. Hier könnte der Schutzauftrag des Souveräns gegenüber *allen* Bürgerinnen und Bürgern[25] sogar eine gesetzliche Einschränkung der Selbstbestimmung[26] des *Einzelnen* rechtfertigen, vorausgesetzt eine solche Maßnahme könnte wirksam und verhältnismäßig den angestrebten Zweck erfüllen.

Alternativ oder komplementär dürfte die Schutzpflicht dem politischen Souverän aufgeben, geeignete Maßnahmen zu ergreifen, um die Menschen über das Schädigungspotenzial solcher Datenpreisgaben aufzuklären, sie gegebenenfalls durch verpflichtende Warnhinweise (ähnlich wie in der analogen Welt z.B. bei Tabakprodukten) zu erinnern und, so weit möglich, den Auf- und Ausbau vergleichbarer Dienstleistungen im eigenen Hoheitsgebiet zu fördern, die den dort geltenden Werten und Standards entsprechen. Allerdings ist darauf zu achten, dass das zulässige bzw. sogar gebotene informativ-edukatorische Handeln nicht in einen übergriffigen Paternalismus umschlägt.

---

24 Siehe hierzu z.B. die Zusammenfassung einer Reuters-Recherche: https://www.reuters.com/investigates/special-report/health-china-bgi-dna/ [2.8.2024].

25 Hier ist nicht nur an den Schutzauftrag in Bezug auf personenbezogene Daten aus Art. 16 AEUV zu denken, sondern an den Leben und Gesundheit umfassenden Schutzauftrag insbesondere aus Art. 2 GG. Art. 2 und 3 EU-GRCh statuieren ein »Recht auf Leben« wie »auf körperliche und geistige Unversehrtheit«.

26 Dieses potenzielle Spannungsverhältnis zwischen der Ausübung individueller Selbstbestimmung und staatlicher Souveränität macht deutlich, dass es zu kurz greift, Souveränität als »Fähigkeit einer juristischen oder natürlichen Person zur Selbstbestimmung über ihre Datengüter« (Otto/Burmann 2021, S. 284) zu verstehen. Damit versteht man weder das Besondere von Souveränität noch das von Selbstbestimmung. Letztere liegt im Beispielsfall in der individuellen Entscheidung, die Blut- oder Speichelprobe ins Nicht-EU-Ausland zu versenden – und damit das virtuelle »Datengut« des eigenen genetischen Codes EU-Externen zugänglich zu machen; erstere in der eventuellen politischen Entscheidung, durch geeignete Maßnahmen solchen Daten-Export zu verhindern.

Ethisch – und unter gewissen Einschränkungen juridisch[27] – relevant ist nicht nur das Tun von »Gutem« oder »Bösem«, sondern auch das (Unter-)Lassen oder Be- oder Verhindern von Gutem. Insofern ergibt sich aus der generellen (und der beispielhaft in Art. 16 AEUV spezifizierten) Schutzpflicht des Souveräns eine (wenn nicht juridische, so doch ethische) Pflicht, den Schutz vor potenziellem Schaden durch eine »Sache« (im weitesten Sinne) so zu gestalten, dass er potenziellen Nutzen durch eben die »Sache« möglichst gar nicht, auf jeden Fall aber nicht mehr als unbedingt nötig be- oder gar verhindert. Für die Prüfung der Verhältnismäßigkeit möglicher Schutzmaßnahmen sind sowohl deren Eingriffstiefe als auch die reale Wirksamkeit zur Erfüllung des Schutzzwecks und die Auswirkungen auf andere Schutzgüter – darunter so fundamentale wie Leben und Gesundheit der Menschen – abzuwägen.

V. Individuelle Daten(zugangs)souveränität – Metapher und Mantra

Vorstehende Überlegungen skizzieren, wie sich der klassische Souveränitätsbegriff nicht nur suggestiv-verheißungssemantisch[28] etwa in »Werbetexten« politischer[29] oder ökonomischer Zielsetzung benutzen, sondern in

27 *Strafbar* ist ein Nicht-Tun nur qua Unterlassungsdelikt nach § 13 StGB oder konkret z.B. nach § 138 (Nichtanzeige einer geplanten Straftat) oder § 323 c StGB (unterlassene Hilfeleistung); allerdings können insbesondere aus grundrechtlichen Schutzpflichten konkrete Handlungsaufträge erwachsen (Untermaßverbot). *Ethisch* ist jedes Nicht-Tun eines Guten, das zu tun *möglich* wäre, erörterungsbedürftig. Im Sinne Kants Praktischer Philosophie wäre ein solches Nicht-Tun möglichen Gutes als Pflichtverletzung anzusehen, denn – neben der »eigenen Vollkommenheit« – ist »fremde Glückseligkeit« der andere Zweck, den ein moralfähiges animal rationale wie der Mensch sich setzen *muss* (Kant 1981a [1797], S. 13 ff., zitiert nach der Originalpaginierung). Auch in einer *Angewandten* Ethik, wie der von Beauchamp/Childress (2013, S. 202–248), steht neben dem Nicht-Schaden das positive »Gebot« des Gutes-Tun (beneficence). Wäre die Reichweite dieser Theorie überdehnt, wenn man vermutet, dass dieses Gebot nicht nur für den einzelnen Arzt in der Behandlung eines Patienten, also auf der Mikroebene gilt, sondern auch für das (politische) Handeln der Ärzte als Gemeinschaft (in Deutschland etwa durch Ärztekammern) auf der Meso- und für den Gesetzgeber auf der Makroebene? Siehe Jonas (1979, S. 181): »Der wirkliche Staatsmann wird seinen Ruhm […] darin sehen, dass von ihm gesagt werden kann, er habe zum Besten derer gewirkt, über die er Macht hatte: *für* die er sie also hatte.«

28 Von »Versprechungssemantik« spricht Gehring (2022, S. 35).

29 Siehe z.B. die »Datenstrategie« der Bundesregierung (2021), der Gehring (2022, S. 33) »begrifflichen Wirrwarr« attestiert. So würden die Termini »Souveränität« und »souverän« in Verbindung

seinen drei Hauptbestimmungsmomenten *mutatis mutandis* tatsächlich auf die Welt des Digitalen einschließlich der Regelung von Datenzugängen anwenden lässt. Zugleich wird klarer, warum, hiervon unterschieden, die Anwendung des Wortes »Souveränität« auf Individuen (sofern nicht der absolutistische Herrscher gemeint ist) »nur« im metaphorischen Sinne zu verstehen ist. Diese Unterscheidung führt in praktischer Hinsicht zu unterschiedlichen Anforderungen bzw. Erwartungen zum einen an staatliches Handeln, zum anderen an das Individuum.

Sofern Souveränität im Zusammenhang des Digitalen »klassisch« gedacht wird, so verbleibt sie in der Sphäre des Staatlichen und dessen Schutzpflichten. Derselbe Akteur, der in der analogen Welt z.B. die Grenzen seines Territoriums und die Zugänge zu diesem schützt, wird in der digitalen Welt z.B. kritische Dateninfrastrukturen und Datenzugänge schützen – oder Akteuren in seinem Hoheitsgebiet (z.B. Krankenkassen) solchen Schutz gesetzlich aufgeben. »Souveränität« wird hier auf das neue Wirklichkeitsfeld »Digitalität« angewandt, also begrifflich, politisch und rechtlich übertragen – während es sich im Hinblick auf das Individuum um einen *metaphorischen* Gebrauch im Sinne poetischer Lizenz handelt.[30] Eine Metapher kann erhellend sein, aber auch zu Fehlschlüssen führen, ähnlich wie eine Analogie helfen kann, sich einen Sachverhalt fasslich zu machen, aber nicht als Beweis dafür missverstanden werden darf, dass die Sache selbst sich genauso verhält.[31]

Der metaphorische Gebrauch des Wortes »Souveränität« im Zusammenhang von Individuen in der digitalen Welt dampft dessen rechtsphilosophi-

---

mit den Wörtern Daten und Digitalisierung »inflationär, nämlich insgesamt 33 Mal« gebraucht und dabei »fast beliebig genutzt und auch verwechselt«.

30 Aristoteles, der die »Metapher« als erster definierte, tat dies in seiner *Poetik* (Kap. 21 / 1457b). Hier definiert er sie allgemein als »onómatos allotríou epiphorá«: als Beilegung eines fremden (im Sinne von: einem andern gehörigen) Namens. Von den dann unterschiedenen vier Arten von Metaphern funktioniere die vierte (die am stärksten dem modernen Verständnis des Wortes »Metapher« entspricht), »katà tò análogon«: gemäß der Analogie – »eine Beziehung, in der sich die zweite Größe zur ersten ähnlich verhält wie die vierte zur dritten«, z.B. »das Alter verhält sich zum Leben, wie der Abend zum Tag«, was den Dichtern erlaube, das Alter als Abend des Lebens anzusprechen oder den Abend als Alter des Tages (ebd.). Zu Funktion und Grenzen solcher Übertragungen bzw. Analogiebildungen siehe die nächste Anmerkung).

31 Formuliert in Anlehnung an Kants Caveat zu Analogien "im Aufsteigen vom Sinnlichen zum Übersinnlichen" (Kant 1981b [1793], Anmerkung S. 81 ff., zitiert nach der Originalpaginierung). Aus dem Umstand, dass "wir ein Schema zu einem Begriffe" brauchen, "um ihn uns verständlich zu machen«, dürfe man, so Kant, nicht »die Folge ziehen", dass ein so erschlossenes Prädikat »dem Gegenstande selbst, als sein Prädikat zukommen müsse« (ebd.).

sche, staats- bzw. demokratietheoretische sowie völkerrechtliche Bedeutung auf die davon wohl unterscheidbaren Konzepte »(informationelle) Selbstbestimmung« und »Kompetenz« im Umgang mit Daten ein[32] – beides sinnvolle Ziele, für die allerdings eigene Wörter zur Bezeichnung zur Verfügung stehen: Vor allem müssen sie aus Perspektive einer angewandten Ethik auf den Anwendungskontext bezogen und in diesem Bezug konkretisiert werden, weniger im Bezug auf semantische Halo-Effekte einer anderen Begrifflichkeit.

So könnte die Rede vom Einzelnen als Datensouverän nicht für nur einen selbstbestimmten, kompetenten Umgang mit Daten im Rahmen der jeweiligen Sachlogik (z.B. des Online-Bankings oder einer Elektronischen Patientenakte) stehen, sondern als Suggestion einer Alleinherrschaft über ihn betreffende Daten missverstanden werden, die es so nicht gibt und nicht geben kann. Ob es sie, kontrafaktisch gedacht, geben *sollte*, und wenn ja, in welchem konkreten Sinne[33], mag man fragen und zur Beantwortung die Analogie zur digitalen oder Datensouveränität im staatstheoretischen Sinne als Kontrastfolie nutzen, aber die Analogie selbst gibt keine zwingende Antwort, sie begründet keine Pflicht. Hier lohnt es sich, einen Schritt zurückzutreten und nach dem Verständnis des Wortes »Daten« und der mit ihm bezeichneten Phänomene zu fragen (also *vor* der Definition des Wortes z.B. zu informationswissenschaftlichen oder juristischen Zwecken).

VI. Was sind »Daten«?

Ob das Geburtsdatum und die attribuierte Geschlechtsidentität eines Neugeborenen beim Standesamt in einem Buch oder in einem Computer registriert werden – die Art der Speicherung ändert nichts am Informationsgehalt. Ebensowenig, ob Konten auf Papier oder elektronisch geführt werden. Oder Gesundheitsdaten auf Karteikarten oder in einer Elektronischen Patientenakte.

---

32 Gehring (2022, S. 41) merkt an, dass die »Datenstrategie der Bundesregierung einen Kompetenz-Ansatz verfolgt, welcher das Ziel des ›souverän‹-Werdens geradezu rührend eng an didaktische Vorstellungen von der Befähigung des Einzelnen knüpft.«

33 Wäre man nicht wieder auf den Staat als Souverän im nicht-metaphorischen Sinne verwiesen, der geeignete (gesetzliche, administrative, infrastrukturelle u.ä.) Rahmenbedingungen gewährleisten müsste, in denen dann der Einzelne selbstbestimmt in seinen jeweiligen Lebenszusammenhängen mit ihn betreffenden Daten umgehen kann?

Zweifellos bringt die elektronische Verarbeitung von Daten, ihre Zusammenführung und – womöglich KI-gestützte – Auswertung neue Informationsgehalte mit höherem Nutzen- und Schadenspotenzial mit sich als die papierne Verarbeitung. Wie mit diesem Potenzial umzugehen sei, ist eine eminent wichtige und gerade deshalb eigens zu erörternde Frage. Sie mit der Klärung der Frage nach den Lebenswirklichkeiten, die mit dem Wort »Daten« adressiert werden, zu vermischen, hilft im Verständnis weder des einen noch des anderen nicht weiter. Um zu diesen zurückzukehren:

Das Geburtsdatum eines Menschen wird nicht erst dadurch zum Datum, dass es elektronisch verarbeitet wird. Das gilt für alle Daten. Daten sind, wörtlich aus dem Lateinischen übersetzt, Gegebenes – also etwas, das mir oder anderen[34] durch mich oder andere gegeben wird. Das beginnt bei den Sinnesdaten, die neuronal verarbeitet werden, und endet nicht bei komplexen Programmen, die komplizierteste Satellitenlenkung oder – semantisch größtenteils verständliche, wenngleich inhaltlich nicht immer überzeugende – Spracherzeugung (Large Language Models) ermöglichen.

34 Ob Daten in diesem Sinne einem Computer, und sei es auch dem leistungsstärksten, *gegeben* sind, berührt die Frage des (Selbst-)Bewusstseins. Sofern man letzteres mit Kant als das Hervorbringen der »Vorstellung *Ich denke*« versteht, »die alle meine Vorstellungen [muss] begleiten können« (Kant 1981c [1787], S. 131 ff, zitiert nach der Originalpaginierung), so kann der Computer zwar »Daten« verarbeiten, aber »er« (oder »sie«, wenn man z.B. an den Film »Her« von Spike Jonze, 2013, denkt) *hat* sie nicht, weil es dieses atome »ich denke« nicht gibt, das alle *seine* (oder *ihre*) Vorstellungen muss begleiten *können*. Die Modalität hier ist entscheidend: Auch ein Mensch denkt nicht bei jeder Vorstellung, dass *er* sie hat, aber er *kann* zu jeder Zeit auf die Meta-Ebene des *gewussten* Vorstellens wechseln und von dort aus *seine* Vorstellungen (auch: Begriffe, Urteile, Schlüsse) als *seine* wissen, sie kritisch vergleichen, auf Konsistenz prüfen. Wer mit Large Language Models (LLM) »Gespräche« führt, stellt schnell fest, dass sie zwar Bewusstsein *simulieren* können – bis hin zu Aussagen wie »Es tut mir leid« (z.B. nach einer vom User durch Nachfragen aufgedeckten halluzinierten Quellenangabe) oder HAL's berühmten letzten Worten »Ich habe Angst« –, aber sie können nicht auf die kritische Meta-Ebene wechseln, sondern immer nur weiter, rein linear, Ketten von Zeichen bilden – wenn auch nach immer komplexeren Wahrscheinlichkeitsalgorithmen und auf immer breiterer Datenbasis. Diese Zeichen-Ketten können dann von einem realen Bewusstsein wahrgenommen und kognitiv verarbeitet, »verstanden« und z.B. als »schlüssig« oder als »nicht schlüssig« beurteilt werden, aber das sie produzierende Programm kann dies nicht. Dieser kategoriale »gap« wird nicht verschwinden, auch wenn die LLM »besser« trainiert werden und der Unterschied von immer weniger Menschen, zuletzt vielleicht von keinem mehr *bemerkt* wird. Er lässt sich aber *wissen*. Dem gegenüber verbleibt der Turing-Test für Künstliche Intelligenz auf einer behavioristischen Ebene.

Insofern lässt sich sagen: Leben ist Datenverarbeitung (nicht nur, aber auch) – bei den meisten Lebewesen[35] ohne Bewusstsein, bei Menschen kann dieses dazu kommen und eine Metaebene schaffen, die »Denken« genannt wird. Dieses konstituiert sich in Zeichen, die sich als Daten zweiter Ordnung verstehen lassen, insofern sie einerseits selbst »Gegebenes« *sind* (z.B. akustisch als gesprochenes Wort oder optisch als Schriftzeichen oder eben elektronisch als digitale Folge von Nullen und Einsen), andererseits anderes im weitesten Sinne »Gegebenes« (Dinge, Sachverhalte, Zusammenhänge) für mich oder andere bezeichnen *sollen*. Beide Arten von Daten haben notwendig einen doppelt relationalen Charakter: Sie betreffen einen oder mehrere und sind einem oder mehreren gegeben. Im Hinblick auf Daten erster Ordnung gilt dieser relationale Charakter für alle Lebewesen, im Hinblick auf Daten zweiter Ordnung, d.h. »Zeichen«, die etwas bedeuten (sollen), gilt er grundsätzlich für alle Menschen, auch wenn kein Mensch alle Daten-Zeichen (z.B. die Phoneme oder Grapheme einer unbekannten Sprache, binäre Zahlenfolgen, QR Codes usw.) versteht.

Jeder Mensch ist zu seinem Überleben darauf *angewiesen*, dass Daten über ihn von anderen Menschen »erhoben« und verarbeitet werden. Das beginnt mit der Mutter, die die Signale ihres Neugeborenen wahrnimmt, daraus z.B. auf Hunger oder Schmerzen schließt und entsprechend tätig wird. Die Frage ist nicht das Ob, sondern das Wie. Die Datenerhebung kann durch einfache Wahrnehmung erfolgen (z.B. die Aufnahme der Bestellung in einem Restaurant durch den Kellner) oder durch komplexe Verfahren (z.B. aufwendige medizinische Diagnostik). Wenn nun eine Person den Tisch im Restaurant unter Hinterlegung ihrer Kreditkartennummer reserviert hat – und später damit bezahlt –, wenn die Bestellung elektronisch aufgenommen und an die Küche weitergeleitet wird, so werden diese personenbezogenen Daten digitalisiert und damit grundsätzlich zusammenführbar und auswertbar. Damit werden sie auch *leichter* als bei analoger Durchführung der einzelnen Schritte anderweitig nutzbar – gegebenenfalls zum Nachteil der betroffenen Person. Die Digitalisierung von Daten erhöht solche Risiken, die grundsätzlich auch in der analogen Welt gegeben sind, beträchtlich; sie muss deshalb im

35 Ob man Computern, weil sie Daten verarbeiten und »Bewusstsein«, sogar »Gefühle« simulieren können, »Leben«, gar Persönlichkeit und Persönlichkeitsrechte zusprechen soll? Eher wäre ein weiteres Caveat angezeigt: Wenn jedes Leben (oder: Bewusstsein) Datenverarbeitung ist, folgt daraus nicht, dass jede Datenverarbeitung Leben (oder: Bewusstsein) ist. Alle Schmetterlinge sind Insekten, aber nicht alle Insekten Schmetterlinge.

Hinblick auf die staatliche Pflicht zum Schutz der Bürgerinnen und Bürger vor Datenmissbrauch eigens bedacht werden. Aber für das Verständnis und die Realisierung *dieser* Pflicht des politischen Souveräns ist es nicht notwendig, und angesichts der Sachlogik von »Daten« vielleicht sogar irreführend, das Konzept einer *individuellen* Daten-Souveränität aufzurufen. Selbst wenn man individuelle Souveränität auf Selbstbestimmung und digitale Kompetenz reduziert.

Selbstbestimmt handelte das Individuum darin, sich für den Besuch dieses bestimmten Restaurants zu entscheiden – im Rahmen dieser Entscheidung akzeptierend, dass man dort z.B. nur elektronisch, unter Hinterlegung seiner Kreditkartennummer reservieren und bezahlen kann. Auch die digitale Aufnahme und Verarbeitung der Bestellung wurde durch konkludentes Handeln akzeptiert. Einzeleinwilligungen zur zweckgemäßen Erhebung und Verarbeitung wären widersinnig. Ebenso die willkürliche Löschung der relevanten Daten. Im Gegenteil: Das Individuum erwartet, dass »seine« Daten (der Reservierungswunsch z.B. betreffend einen Tisch am Fenster oder das Weglassen einer Zutat, auf die es allergisch reagiert) verarbeitet werden. Und was Daten-Löschungen angeht, so erwartet das Individuum die Erfüllung der staatlichen Schutzpflicht durch Aufbewahrungspflichten, die dem abrechnenden Restaurant und dem von ihm in Anspruch genommenen Kreditinstitut auferlegt sind, damit z.B. im Falle einer zu hohen Abbuchung sein Vermögen wirksam geschützt werden kann (durch Reklamation, gegebenenfalls Anzeigenerstattung).

Der Mensch könnte nicht (über-)leben, ohne dass er Daten produziert und andere diese Daten wahrnehmen – oder gegebenenfalls die Produktion weiterer Daten z.B. durch Anordnung eines Röntgenbildes veranlassen – und sie verarbeiten, »verstehen«, auf sie reagieren. Individuelle »Souveränität« – wenn schon das Wort in diesem Zusammenhang benutzt werden soll – besteht nicht in den einzelnen Schritten der Datenerzeugung und -verarbeitung, sondern in der *Entscheidung*, dieses Restaurant oder jenen Arzt aufzusuchen.

VII. Zugänge zu (Gesundheits-)Daten[36] – Primär- und Sekundärnutzung

Beim Arztbesuch geht es um den Schutz von Leben und Gesundheit. Ein Mensch, der an Leib oder Seele leidet und – in »souveräner« Entscheidung – einen Arzt aufsucht, *bittet* diesen mit eben diesem Aufsuchen um optimale Hilfe. Ins Rechtlich-Ökonomische gewendet: er *beauftragt* ihn, solche Hilfe (gegen ein Honorar) zu leisten. Ins Relationale gewendet: Er vertraut sich diesem bestimmten Arzt an. »Souveränität«, wenn man das Wort partout auf einen Einzelnen anwenden will[37], liegt hier im *(An-)Erkennen* des eigenen Leidens sowie in dem *Entschluss*, die Hilfe eines in diesem Bereich als sachverständig(er) Anerkannten (»Expertenwissen«) in Anspruch zu nehmen und dafür ihm alle Informationen – an dieser Stelle gleichbedeutend mit »Daten« – zu geben, die für das selbst gesteckte Ziel einer Genesung *erforderlich* sind.

Wer einen Zweck will, muss auch die geeigneten Mittel wollen.[38] Dazu gehört im Hinblick auf die angestrebte Heilung die *Bereitschaft*, dem Arzt – über das allgemeine Datum hinaus, das ihm der Patient mit einer anfänglichen Aussage wie »Mir tut es hier weh« liefert – weitere Daten zu geben. Der Leidende muss dem Behandelnden »Zugang« zu allen von ihm als Fachmann für relevant erachteten Informationen eröffnen. Er muss gegebenenfalls auf intime Fragen antworten, intime Körperteile zeigen, intime Untersuchungsprozeduren ausführen lassen. Die Bereitschaft, sich im wörtlichen

36 Dem Sachgehalt nach lehnen sich die in den Absätzen VII und VIII folgenden Ausführungen stark an das Digitalisierungsgutachten des Sachverständigenrats Gesundheit und Pflege (2021) an, insbesondere an die Kapitel 3 (»Die fach-, einrichtungs- und sektorenübergreifende elektronische Patientenakte«, Tz. 163–320) und 5 (»Nutzung von Versorgungsdaten zu Forschungszwecken«, Tz. 445–552). Es würden den Rahmen dieses Beitrags sprengen, die geringfügigen Unterschiede zwischen den hiesigen Überlegungen aus der Perspektive einer Angewandten Ethik – siehe Abschnitt I – und denen des Sachverständigenrats nachzuzeichnen.

37 Dann allerdings in der bereits angesprochenen Begriffsumdeutung Gernot Böhmes (2008, S. 149), wonach der »souveräne Mensch« das Subjekt ist, »das anerkennt, dass es nicht Herr im eigenen Haus ist, das Subjekt, zu dem das Leiden ebenso gehört wie das Handeln.«

38 Damit ist nicht gesagt, dass der Zweck jedes denkbare Mittel »heiligt« im Sinne von »rechtfertigt«. Wenn ein Mensch eine Organtransplantation braucht, um zu überleben, muss er (wenn er weiterleben will) auch die entsprechende Operation wollen. Er darf aber weder den Tod eines anderen, als Spender geeigneten Menschen *wollen* (allenfalls generisch *wünschen*), noch gar ihn herbeiführen – oder den anderen mit Geld (womöglich unter Ausnutzung einer wirtschaftlichen Notlage) oder anderen Mitteln drängen, ihm ein Organ »freiwillig« zu spenden. Die *Geeignetheit* der Mittel ist zu messen an ihrer Vereinbarkeit mit anderen »Werten« (ethisch gesprochen) bzw. mit geltenden Gesetzen (juridisch gesehen).

und im übertragenen Sinne zu entblößen, ist untrennbar verbunden mit der *Erwartung*, dass der Arzt die erhobenen Daten in seinem Sachverstand zusammenführt und auswertet und sie so aufbewahrt, wie es für eine Behandlung lege artis erforderlich ist. Zugleich erwartet der Patient, dass der Arzt die ihm anvertrauten Daten bestmöglich vor Kenntnisnahme bzw. Zugriff durch Unbefugte und vor Missbrauch schützt. Das Arztgeheimnis ist Datenschutz avant la lettre.

Indem also ein Individuum sich entscheidet, einen Arzt aufzusuchen, ist dieser *autorisiert* – und *verpflichtet* –, *alle* Daten zu erheben und zu verarbeiten, die seiner Fachkenntnis nach nötig sind, um eine Diagnose zu stellen, Therapie-Optionen zu ermitteln und mit dem Patienten zu besprechen sowie die dann vom spezifisch aufgeklärten Patienten gewählte durchzuführen. Um einem häufig anzutreffenden Missverständnis entgegenzutreten: Das zuletzt anklingende Konzept der spezifischen, informierten, freiwilligen Einwilligung ist, in dieser lebensweltlichen Perspektive, auf die *Behandlung* als Ganzes, *einschließlich* der in diesem Zusammenhang erfolgenden Datenerhebung und -verarbeitung, zu beziehen. Die Inklusion von Datenerhebung und -verarbeitung in die Einwilligung ist sachlogisch notwendig – und sogar gefordert –, um *lege artis* zu diagnostizieren und zu therapieren. Der betreffende Mensch hat sie mit-beauftragt, als er den Arzt aufsuchte. Dieser soll ihn zwar in verständlicher Sprache auch über die von ihm vorgesehene Erhebung und Verarbeitung medizinisch relevanter Daten, vulgo Diagnostik, aufklären, aber als medizinischer Laie kann der Patient letztendlich nicht beurteilen, welche spezifischen Daten der von ihm beauftragte Arzt für sein professionelles Handeln benötigt. Er muss insoweit dem von ihm aufgesuchten Arzt *vertrauen*.

Eine explizite Einwilligung wäre nur erforderlich, wenn es sich um *invasive* Diagnostik handeln würde, die ein *höheres Risiko* mit sich bringt als das minimale z.B. einer Blutabnahme. Aber in solchen Fällen bezieht sich die Einwilligung auf die *Durchführung* der nicht risikofreien diagnostischen Maßnahme als solcher, nicht in die Erhebung und Verarbeitung der so gewonnenen Daten, denn diese sind das Ziel der zur Rede stehenden Diagnostik. Es wäre unsinnig, anzunehmen, dass der Patient das Risiko einer speziellen Datenerhebung auf sich nehmen, aber die Auswertung durch den Arzt nicht zulassen wollen würde. Allenfalls ließe sich kasuistisch konstruieren, dass ein Patient im Warten auf das Ergebnis Angst vor demselben bekommt und unter Hinweis auf sein Recht auf Nicht-Wissen fordert, dass ihm das Ergebnis (die Diagnose) nicht eröffnet wird. Während ihm dies zuzugestehen

wäre, ist es normativ doch fraglich, ob für solche seltenen Fälle der Patient die Möglichkeit haben sollte, die Eintragung des Ergebnisses in die Elektronische Patientenakte zu untersagen (was man »Befüllungs-Opt-out« nennen könnte). Eine Löschung der Daten im IT-System des Leistungserbringers wird er ohnehin nicht erlangen können, da dem gesetzliche Vorschriften (Dokumentations- und Aufbewahrungspflichten) entgegenstehen.

Da die Untersuchung solidarisch finanziert wurde, lässt sich zudem argumentieren, dass die Solidargemeinschaft ein eigenes Interesse an dem diagnostischen Befund hat, dessen Zustandekommen sie finanziert hat: Zusammen mit anderen Befunden könnte er, wissenschaftlich ausgewertet, zur früheren Erkennung und besseren Behandlung von vergleichbaren Erkrankungen anderer Mitglieder der Solidargemeinschaft beitragen.[39] Dieses »Gemeinwohlinteresse« wäre durch ein – über Abrechnungs- und Kontrollinteressen hinausgehendes – Datennutzungsrecht der Solidargemeinschaft an Daten aus von ihr finanzierter Diagnostik und Therapie zu realisieren.[40] Diese Daten sollten, pseudonymisiert, für die Sekundärnutzung zu gemeinwohldienlichen Zwecken (insbesondere der wissenschaftlichen Auswertung) zugänglich sein – unabhängig davon, ob der Patient sie zur Kenntnis genommen oder vor sich selbst weggeschlossen hat. Die Sekundärnutzung müsste gesetzlich durch eine Befugnisnorm, begleitet von wirksamen Kontrollmechanismen und empfindlicher Strafandrohung bei unbefugtem Zugriff auf oder Missbrauch von Daten, realisiert werden.

Die Solidargemeinschaft ist zugleich dem aufgeklärten Selbstinteresse des Individuums und seinem Anspruch auf »Daten(zugangs)souveränität« (wenn man das Wort auf den Einzelnen anwenden will) über die Lebenszeit hinweg verpflichtet. Dies würde dafür sprechen, das Untersuchungsergebnis so aufzubewahren, dass das Individuum, wenn es seine Meinung ändert, sich Zugang zu der Diagnose verschaffen kann. Hier könnte die Möglichkeit einer »Verschattung« oder »Sperrung« von bestimmten Daten in der ePA genutzt werden, wie sie der Sachverständigenrat Gesundheit & Pflege als Opt-out-Option für den Patienten vorgeschlagen hat.[41] Es sollte technisch machbar und rechtlich regelbar sein, dass ein Arzt auf Wunsch des Patienten ei-

39 Insofern ist das in Anmerkung 19 aufgerufene »bonum commune« nicht als metaphysische Entität zu verstehen, sondern als Ober- und Sammelbegriff für das Wohl aller einzelnen in einer Rechts- und Solidargemeinschaft Zusammenhaltenden.

40 Die Abrechnungs- und Kontrollinteressen der Solidargemeinschaft sind in Deutschland durch § 75 SGB X bereits realisiert – siehe auch Anmerkung 55.

41 Siehe Sachverständigenrat 2021, Tz 217 ff.

nen separaten Ordner anlegt und in diesem den Patienten betreffende Daten speichert, von denen dieser derzeit (im Sinne seines Rechts auf Nicht-Wissen) keine Kenntnis erlangen will. So wäre ein späterer Zugriff durch ihn (oder einen von ihm dann autorisierten Leistungserbringer) möglich. Zugleich hätte der Arzt seine Befüllungspflicht erfüllt, von der es keine Ausnahme geben sollte:

Der Patient *erwartet, ja fordert* – Einwilligung ist insofern das falsche Paradigma –, dass all ihn betreffenden, medizinisch relevanten Daten zu seinem Wohl (z.B. zur Verlaufs-, Ergebnis-, Qualitätskontrolle, notfalls auch zur Klärung von Haftungsfragen) erhoben und *vollständig* in seiner Patientenakte hinterlegt werden und im Weiteren ihm und anderen von ihm Autorisierten zugänglich sind. Löschungen sollten deshalb für alle Beteiligten rechtlich verboten und technisch verhindert werden – zum Schutz des Patienten und seiner medizinischen und gegebenenfalls rechtlichen Interessen, aber auch der Interessen des Leistungserbringers (so wird in der Terminologie des SGB V der Arzt, das Krankenhaus usw. genannt) und des Leistungsträgers (die Krankenkasse) und, im Hinblick auf die Sekundärnutzbarkeit (siehe unten): der Rechts- und Solidargemeinschaft.

Neben einem Schutz vor Löschung durch andere impliziert dies auch einen Schutz vor (versehentlicher oder willentlicher) Löschung von Gesundheitsdaten in der ePA durch den Patienten selbst. Auch solche Löschung liefe seinem aufgeklärten Selbstinteresse zuwider. Insofern könnte die einschlägige Empfehlung des Sachverständigenrats in seinem Digitalisierungsgutachten (2021) als »schwacher Paternalismus« bezeichnet werden. Schwach ist dieser Paternalismus, insofern mit der Möglichkeit, die ePA für sich ganz abzulehnen (die primäre Opt-out-Option, deren Ermöglichung der Sachverständigenrat empfiehlt), die Möglichkeit gegeben ist, sich der »Logik« der ePA zu entziehen. Dass aber die ePA in sich kein Befüllungs- und Löschungs-Opt-out vorsehen sollte, lässt sich als durch die *Pflicht* geboten verstehen, die durch gesetzlichen Zwang erlangten Finanzmittel (»Krankenkassenbeiträge«) so effizient wie möglich einzusetzen, denn diese Pflicht gilt umfassend: nicht nur für Behandlungs-, sondern auch für Infrastrukturmaßnahmen wie den Aufbau und das Betreiben einer ePA-basierten Gesundheitsversorgung.

Schließlich dürfte die Schaffung von Befülllungs- und Löschungs-Opt-out-Möglichkeiten bei nicht wenigen die irrige Vorstellung erwecken oder fördern, es seien mit der Verhinderung oder Löschung bestimmter Gesundheitsdaten in der eigenen ePA diese Daten digital nicht mehr vorhanden.

Das trifft aber nicht zu. Sie *bleiben* im Informationssystem des Leistungserbringers (des Arztes, Krankenhauses, Labors) wie des Leistungsträgers (bei letzterem zwar »nur« die abrechnungsrelevanten, aber auch diese können sehr persönliche Informationen über einen Menschen enthalten – z.B. »verrät« das Abrechnungsdatum einer regelmäßigen Verschreibung von Retrovir den HIV-Status des Versicherten). Insofern wäre es Augenwischerei, ja ein desinformatives Tun, das die Menschen nicht zu aufgeklärter Selbstbestimmung im Umgang mit ihren Daten befähigt, sondern sie verdummt, wenn man den Eindruck vermittelte, durch eine untersagte Befüllung oder eine Löschung wäre ein sensibles Gesundheitsdatum digital »aus der Welt«.

Nur der Versicherte verlöre, wenn er Daten in der ePA löschen oder dem Leistungserbringer bereits ihre Eintragung untersagen könnte, den Überblick, welche ihn betreffende Gesundheitsdaten es in der digitalen Welt »gibt« (womöglich faktisch schlecht vor unbefugten Zugriffen geschützt, aber seinem befugten Zugang entzogen). Die so entstehende Unvollständigkeit der Datensätze der ePA ist nicht nur – neben irreführender oder zumindest missverständlicher »Aufklärung« über die Begrenztheit solchen Löschens – eine eklatante Schwächung der sonst gerne beschworenen »Datensouveränität«. Diese Unvollständigkeit kann im akuten Krankheitsfall (wenn z.B. wichtige Befunde, eventuell auch Fehldiagnosen und daraufhin erfolgte Fehlbehandlungen nicht so schnell wie nötig zugänglich sind, weil aus der ePA gelöscht) ernste Folgen für Leben und Gesundheit des Betroffenen haben.

In Dänemark – wo die EU-Verträge, die Grundrechtecharta und die DSGVO wie in Deutschland gelten – ist es weder dem Arzt noch dem Patienten möglich, zumindest nicht erlaubt, Gesundheitsdaten aus der elektronischen Patientenakte zu löschen (was man analog zum o.g. Befüllungs-Opt-out Löschungs-Opt-out nennen könnte). Auch eine bestätigte Fehldiagnose darf nicht gelöscht, sondern nur mit einem entsprechenden Kommentar versehen werden. Dies gilt selbst für den Fall, dass ein Arzt versehentlich ein Gesundheitsdatum in die elektronische Akte eines anderen Patienten eingetragen hat! Auf der offiziellen Webseite des dänischen Gesundheitssystems (www.sundhed.dk) werden Ärztinnen und Ärzte wie folgt über ihre Rechtspflichten belehrt:

»Informationen in der Krankenakte dürfen nicht gelöscht oder unleserlich gemacht werden. Das gilt auch dann, wenn die Informationen offensichtlich falsch sind, zum Beispiel wenn Sie versehentlich etwas über einen Patienten in die falsche Patientenakte geschrieben haben. Stellt sich im Nachhinein heraus, dass eine Information falsch ist, darf sie nur

durch einen korrigierenden Zusatz berichtigt werden. Berichtigungen oder Ergänzungen dürfen also nur so vorgenommen werden, dass der ursprüngliche Text im Datensatz erhalten bleibt.«[42]

Unabhängig davon, wie die dänischen Regelungen im Rahmen der eingefahrenen deutschen Datenschutznarrative juristisch bewertet würden – aus ethischer Sicht spricht vieles für die Ausgestaltung, wie sie in Dänemark und anderen EU-Mitgliedstaaten praktiziert wird, unter der Bedingung, dass Patienten die Möglichkeit gegeben wird, Inhalte auf der ePA wegzuschließen (und sich und anderen wieder zugänglich zu machen). Denn das Schutzgut einer vor allem aus medizinischen, aber auch aus abrechnungs- und haftungsrechtlichen Gründen möglichst umfassenden *Nachvollziehbarkeit* von in Anspruch genommener Gesundheitsversorgung (einschließlich eventueller Fehldiagnosen und Fehlbehandlungen) sowie das Schutzgut patienten- oder gemeinwohldienlicher *Forschung* durch Sekundärnutzbarkeit einer umfassenden Datenbasis – mit den kuratierten, Forschenden auf Antrag streng kontrolliert und pseudonymisiert zugänglich gemachten Daten möglichst aller, die Gesundheitsversorgung erhalten haben –, wiegen in der Abwägung mit formaljuristischen Einwilligungskonstrukten schwer, zumal diese aus einer Abwehrperspektive gedacht sind, die für den Sachzusammenhang *gewollter*[43] Gesundheitsversorgung *erst in zweiter Linie* (im Hinblick auf Datenmissbrauch) einschlägig ist. *In erster Linie* ist hier »Schutz« nicht negativ im Sinne von Abwehr, sondern positiv im Sinne des Schutzes nutzenstiftender Möglichkeiten zu denken[44]: der Er-

42 Siehe https://stps.dk/sundhedsfaglig/ansvar-og-retningslinjer/sundhedsfaglig-vejledning/journalfoering/faq [27.1.2024; ins Deutsche übersetzt mit DeepL]. Antwort auf die Frage »Må jeg slette oplysninger fra en patientjournal?« (»Kann ich Informationen aus einer Patientenakte löschen?«). Der Verfasser dankt Prof. Mickael Beck, Staatswissenschaftliches Institut der Süddänischen Universität (SDU, Odense), für den Hinweis auf die hier zitierte Quelle.

43 Dieses vom (Rechts-)Subjekt ausgehende Wollen, also das Setzen *eigener* Zwecke, das damit auch die sachlogisch notwendigen Mittel will – etwa die Datenverarbeitung im Rahmen der Gesundheitsversorgung, oder die im Rahmen eines digitalen Bankkontos –, ist *wesentlich* zu unterscheiden von dem Wollen *anderer*, die mich betreffende Daten zu *ihren* Zwecken (Interessen) erlangen wollen. Dabei wäre zu unterscheiden zwischen a) dem Interesse des Rechtstaates, dessen Bürger ich bin und der zu seinem Funktionieren gesetzlich bestimmte Daten braucht, b) dem Interesse anderer Staaten (insbesondere deren Geheimdiensten) oder privaten Partikularinteressen – c) kommerzieller oder d) krimineller Art – an mich betreffenden Daten.

44 Es wäre interessant, begriffsgeschichtlich zu rekonstruieren, inwiefern der Umstand, dass das deutsche Datenschutzverständnis in seinen Grundzügen und in seiner bisherigen Differenzierung von dem Urteil des Bundesverfassungsgerichts vom 15.12.1983 zum damaligen Volkszählungsvorhaben der Bundesregierung (und aller Länder bis auf Hamburg) geprägt worden ist,

möglichung positiver »Werte« wie Leben, Gesundheit, damit ermöglichter Selbstbestimmung und der Realisierung solcher Persönlichkeitsrechte wie dem auf vernünftigen Umgang mit und Zugang zu den mich betreffenden (Gesundheits-)Daten.

Insofern das Individuum eine *solidarische Krankenversicherung* zur Finanzierung der Behandlung in Anspruch nimmt, gehört zu diesem lebensweltlichen Zusammenhang auch (ohne dass es dazu expliziter Einwilligung bedarf – diese ist mit der Inanspruchnahme konkludent gegeben), dass solche Finanzierung nur aufgrund namentlicher Datenverarbeitung möglich ist: Der Arzt muss ad personam abrechnen. Ebenso die Apotheke, in der der Patient ein ihm verschriebenes Arzneimittel abholt. Selbst im digital rückständigen Deutschland wurden diese Daten schon vor der Einführung einer Elektronischen Patientenakte und des E-Rezeptes digital verarbeitet. Dies erfolgt aufgrund gesetzlicher Regelungen. Weder waren und sind in diesem Zusammenhang Einwilligungen des einzelnen Patienten nötig noch sind Daten-Löschungen durch den betroffenen Patienten möglich. Die sogenannten *Abrechnungsdaten* werden im Computersystem der Krankenkasse des Patienten zusammengeführt und dort gemäß den gesetzlichen Aufbewahrungspflichten gespeichert. Dort werden sie zur Abwicklung, gegebenenfalls auch zur Kontrolle der Abrechnungen genutzt. Von den Krankenkassen werden zudem die Abrechnungsdaten zusammen mit den Diagnosen (nach der deutschen Fassung der von der WHO herausgegebenen Internationalen Klassifikation der Krankheiten – ICD – verschlüsselt) pseudonymisiert an das nationale Forschungsdatenzentrum (FDZ) weitergegeben, durch das wiederum Forschende auf Antrag Zugang zu Datensätzen zur Sekundärnutzung im Hinblick auf bestimmte Forschungsfragen erhalten können. Nur die sogenannten *Behandlungs- oder Versorgungsdaten* verbleiben bis dato (2024) – allerdings schon digitalisiert – im Praxisverwaltungssystem (PVS) des Arztes[45] oder im Krankenhausinformationssystem

dazu geführt hat, dass in Deutschland bis heute Datenschutz ohne Rücksicht auf den lebensweltlichen Kontext *primär* als Schutz vor Datenmissbrauch und nicht, wie hier vorgeschlagen, in individuell gewollten Zusammenhängen (wie der Gesundheitsversorgung, dem eBanking u.ä.) primär als Schutz der positiven Möglichkeiten aus Datennutzung und, hiervon abgeleitet, diese bewahrend und absichernd, erst *sekundär* als Schutz vor Datenmissbrauch gedacht und gestaltet wird.

45 Die Karteikarten in Arztpraxen sterben aus. Auch die in diesen gespeicherten Daten waren nicht vor Missbrauch gefeit. Der Schaden durch Missbrauch wurde aber immer als geringer gewertet als der Schaden, der zu befürchten wäre, wenn Ärzte Behandlungsverläufe nicht oder nicht voll-

(KIS) der Einrichtung, in der der Patient stationär behandelt wurde. Es gelten Dokumentations- und Aufbewahrungspflichten. Der Patient hat ein Anrecht auf Kopien dieser beim Leistungserbringer gespeicherten Daten (nicht auf ihre Löschung), allerdings stehen sie ihm bislang nicht gesammelt zur Verfügung. Eine *vollständige* Elektronische Patientenakte könnte hier individuelle »Souveränität« im metaphorischen Sinne durch den jederzeitigen und umfassenden Zugang zu allen das Individuum betreffenden Gesundheitsdaten tatsächlich *stärken*.

VIII. Datenschutz, der die Daten wirksam schützt und ihre verantwortliche Nutzung ermöglicht

Vorstehende Darstellung stellt den sehr komplizierten, zudem in legislativer Entwicklung befindlichen Regelungsstand der Datenverarbeitung und -zugänge im deutschen Gesundheitsversorgungssystem nur näherungsweise dar.[46] Wichtig für die Weiterentwicklung des Rechtsrahmens wäre die Einsicht, dass in den skizzierten Realzusammenhängen – vom Arztbesuch über die Abrechnung bis zur Sekundärnutzung – die Konzepte von individueller Souveränität und Einzeleinwilligungen (z.B. was die Befüllung mit oder Löschung von Inhalten in der ePA betrifft) für den Umgang mit und Zugang zu Gesundheitsdaten wenig zielführend sind. Denn die mit diesen Wörtern verbundene *Anliegen* sind in dem vorgängigen, die Datenverarbeitung und -speicherung auslösenden *Entschluss* des Einzelnen, zu seinem Gesundheitsproblem einen Arzt zu konsultieren und die Solidargemeinschaft dafür aufkommen zu lassen, *erfüllt*. Dies gilt im Hinblick auf die Datenverarbeitung im Zusammenhang der Konsultation (Anamnese, Diagnostik) und sich eventuell anschließender Therapie sowie der Kostentragung – *nicht*, wie schon angesprochen, im Hinblick auf eine eventuelle Behandlung, in die als solche separat eingewilligt werden muss. Mit der Einwilligung in

ständig dokumentieren und sie für sich und andere Leistungserbringer (im Streitfall auch für gerichtliche Gutachter) nicht mehr nachvollziehbar machen würden.

46 Zur Veranschaulichung siehe die einschlägigen Bestimmungen im SGB V (z.B. § 295 SGB V), deren Grad an Differenzierung mit einiger Wahrscheinlichkeit sowohl den promovierten Versicherungsjuristen Franz Kafka als auch Niklas Luhmann, der gleichfalls als Jurist (in einer Landesbehörde) startete und dann über die Verwaltungswissenschaft zur Soziologie und Entwicklung seiner Systemtheorie kam, literarisch oder philosophisch-analytisch inspiriert hätte.

die konkrete Behandlung ist aber wiederum die Einwilligung in die damit verbundene medizinisch notwendige bzw. abrechnungstechnisch oder gegebenenfalls rechtlich geforderte Datenverarbeitung (z.B. dem Arzt oder Krankenhaus auferlegte[47] Dokumentations- und Aufbewahrungspflichten) gegeben. Es wäre sachlogisch und ethisch-normativ unsinnig, von dieser vom Individuum in diesem Kontext *gegebenen Einwilligung* (z.B. zu einem operativen Eingriff), die als Ausdruck individueller »Souveränität« angesprochen werden mag, die zu der mit dem Eingriff notwendig verbundenen Datenverarbeitung (z.B. Erstellung und Speicherung eines OP-Berichts) abzuspalten und zu dieser weitere einzelne Einwilligungen zu verlangen. Dabei garantieren solche formaljuristischen Aufsplitterungen, die gerne mit dem Epitheton »feingranular« versehen werden, keinen zusätzlichen oder gar besonders »strengen« Datenschutz – anders als insbesondere im deutschsprachigen Diskurs insinuiert wird. Im Gegenteil: Sie sind oft unnütz oder sogar schädlich (verglichen etwa mit den dänischen Regelungen in diesem Bereich).

Unnütz sind sie, weil es die Gesundheitsdaten eines Patienten nicht schützt, wenn Einwilligungserklärungen, die oft seitenlang und für viele kaum bis nicht verständlich formuliert sind, zumeist ungelesen unterschrieben werden und dann millionenfach in Aktenschränken von Arztpraxen oder Krankenhäusern vergilben. Der Patient unterschreibt, weil er die Behandlung und damit auch die zu diesem Zweck gehörenden Mittel *will*. Dass er in der Regel »blind« unterschreibt, als sträflichen, zumindest tadelnswerten Verzicht auf Souveränitätsausübung zu kritisieren, wäre verfehlt. Denn damit würden auf der Sachebene das ureigene Interesse des Patienten an seiner Gesundheit (bzw. Genesung) sowie der Behandlungskontext und auf der normativen Ebene die Einwilligung ignoriert, die der Patient damit gegeben hat, dass er, selbstbestimmt, einen Arzt oder ein Krankenhaus aufsuchte und um Hilfe bat.

Da nicht alle Menschen medizinisches und juristisches Expertenwissen haben *können*, muss der Gesetzgeber[48] die Rahmenbedingungen der Gesundheitsversorgung so gestalten, dass das medizinisch Notwendige

47 Die geltende Rechtsordnung bietet mit dem Gendiagnostikgesetz (GenDG) ein Analogon (siehe die Strafvorschriften in § 25 GenDG), zumindest eine Anregung zur Ausgestaltung entsprechender Schutzvorschriften.

48 – als eine der drei Realisierungsformen (neben Exekutive und Jurisdiktion) jener Souveränität, die letztlich vom Volke ausgeht – siehe hier Abschnitt II.

erfolgt und die unter dieser Bedingung (der medizinischen Notwendigkeit) im Versorgungszusammenhang erhobenen Daten wirksam vor Missbrauch geschützt sind und zugleich für die Nutzung zum Wohle des Patienten[49] zugänglich sind.

Tatsächlich sind Gesundheitsdaten, wie in diesem Kontext gerne gesagt wird, »besonders sensibel« und bedürfen besonderen Schutzes. Echter Schutz wird aber dadurch gewährleistet, dass der Gesetzgeber zum einen festlegt, dass nur Datenerhebungen, -verarbeitungen und -zugänge zulässig sind, die für eine solidarisch finanzierte Gesundheitsversorgung (und daran anknüpfende Sekundärnutzung – s.u.) medizinisch sowie aus Abrechnungs- und Haftungsgründen *notwendig* sind (ex negativo: und welche nicht), und zum anderen festlegt, welche informationstechnischen, organisatorischen und sonstigen Maßnahmen getroffen werden müssen, um die erhobenen Daten vor *unbefugten* Zugriffen und vor Missbrauch zu sichern. Drittens muss der Gesetzgeber die real-wirksame (nicht rein formal-juristische) Einhaltung vorstehender Bestimmungen kontrollieren (lassen)[50] und sanktionieren, wenn sie nicht eingehalten werden, und noch schärfer sanktionieren, wenn Unbefugte sich trotzdem Zugang zu Gesundheitsdaten verschaffen und sie für eigene Zwecke missbrauchen.

Schädlich sind weitere Aufsplittungen der initialen Einwilligung, wenn sie die sachangemessene Datennutzung (z.B. für bestmögliche Gesundheitsversorgung – ob einzel- oder gruppennützig) ver- oder zumindest behindern, z.B. eine gute Behandlung erschweren, weil aufgrund unterschiedlicher Datenzugangs- und Einwilligungsregimes nach dem Umzug

49 »verstanden als das Wohl« des Einzelnen sowie »aller aktuellen und aller zukünftigen Patientinnen und Patienten« (Sachverständigenrat 2021, Tz. 31), also individual- wie sozialethisch.

50 Die Aufgaben der 18 Datenschutzbehörden, die Deutschland sich leistet (eine auf Bundes-, 17 auf Landesebene – der Freistaat Bayern hat zwei –; die EU-Datenschutzgrundverordnung fordert eine pro Mitgliedstaat), könnten entsprechend umdefiniert und die Personalausstattung entsprechend geändert werden – weg von formal-juristischen Prüfungen z.B. von Einwilligungsformularen hin zu real-wirksamen Kontrollen. Dazu würde gehören, dass sie als Anlauf-, also Ombudsstellen fungieren, an die Datenmissbrauch befürchtende Bürgerinnen und Bürger sich wenden können. Diese Stellen sollten bei Plausibilität der Befürchtung oder auch von sich aus stichprobenartig informationstechnisch und ablauforganisatorisch prüfen, ob die Verarbeitung von und die Zugänge zu Daten sachangemessen geschützt sind. Auch könnten sie als Beratungs- und evtl. als Zertifizierungsstellen für öffentliche und private Akteure dienen, die – z.B. als Ärzte – mit »sensiblen« Daten umgehen und nach Umsetzung der gesetzlichen Bestimmungen und diesbezüglicher Prüfung auf die Wirksamkeit des Schutzes (im Sinne von Datensicherheit) ebendies bescheinigt kommen.

eines Patienten von Bundesland A nach Bundesland B relevante Gesundheitsdaten des Patienten nicht (mehr) zugänglich sind bzw. in aufwendigen Einzelschritten (oft – groteskerweise – in wenig datenschützenden Formaten wie Fax oder Mail) zusammengesucht werden müssen – was oft nicht vollständig oder nicht rechtzeitig gelingt.

Zugänge zu den Gesundheitsdaten eines Patienten sollen primär zu dessen Nutzen gewährt und genutzt werden, sekundär aber auch zum Nutzen von Patienten mit der gleichen Erkrankung (etwa zur gruppennützigen Forschung) und zum Nutzen aller Patienten (z.B. zur Prävention und Prophylaxe einer Erkrankung, zu Public-Health-Zwecken oder auch zur Gesundheitssystemsteuerung[51]). Diese Sekundärnutzung für gruppen- oder allgemein patientenwohldienliche Zwecken lässt sich ethisch nicht nur als zulässig, sondern als *geboten* ansehen[52], denn die Gesundheitsdaten eines Einzelnen, sofern ihre Erhebung von der Solidargemeinschaft finanziert wurde, sollten anderen Einzelnen in dieser Versichertengemeinschaft oder der Solidargemeinschaft insgesamt (z.B. im Rahmen einer Pandemie) zu Gute kommen – unter der unerlässlichen Bedingung, dass der Einzelne vor Daten-

51 Diese Zwecke dienen dem Wohl des und der einzelnen wie der Gemeinschaft, so dass sie – unter Bedingung ihrer Nutzen wie Schutz wirksam sichernden Umsetzung – von allen Mitgliedern dieser Gemeinschaft mitgetragen werden sollten. Insofern ist es ethisch nachvollziehbar, dass Art. 9 Abs. 2 litt. h) und i) der EU-Datenschutzgrundverordnung erlaubt, die faktische Einzel-Einwilligung jedes und jeder einzelnen durch eine gesetzliche Befugnisnorm auf EU- oder nationaler Ebene zu substituieren, sofern »h) die Verarbeitung […] für Zwecke der Gesundheitsvorsorge […], für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich […] erforderlich« oder »i) die Verarbeitung […] aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten […] erforderlich« ist. Zur Frage, ob und auf welche Weise die Nutzung dieser Möglichkeiten ethisch geboten ist, siehe die nachfolgenden Ausführungen im Haupttext.

52 Insofern wäre es nicht nur ein *Recht* (im juridischen Sinne), sondern eine *Pflicht* (im ethischen Sinne) der Rechts- und Solidargemeinschaft (wenn anders solche Entitäten *ethisch* verpflichtet sein können), Gesundheitsdaten, deren Gewinnung sie finanziert hat, vor individuellen Löschungen (ob durch den Patienten, Leistungserbringer oder Leistungsträger) zu schützen und sie sekundär für das Wohl anderer Mitglieder eben dieser Rechts- und Solidargemeinschaft (und kooperierender anderer Rechts- und Solidargemeinschaften) streng kontrolliert nutzbar zu machen: für gesetzlich definierte Zwecke, unter wirksamen Überwachungsmechanismen sowie empfindlichen Sanktionen von Verstößen – und Befüllungs- und Löschungs-Opt-outs in der Elektronischen Patientenakte *nicht* zuzulassen (wie dies z.B. in dänischen Gesetzen geregelt ist).

missbrauch, Stigmatisierung, Diskriminierung oder Benachteiligung *wirksam* geschützt wird.

Mit der Inanspruchnahme solidarischer Finanzierung einer Gesundheitsversorgung lässt sich zudem die *Einwilligung* zur Sekundärnutzung der im Rahmen dieser Gesundheitsversorgung erhobenen Daten als *durch konkludentes Handeln gegeben* ansehen.[53] Insofern spricht aus ethischer Sicht sehr viel für eine entsprechende gesetzliche Befugnisnorm, die (wie in anderen EU-Mitgliedstaaten) die Sekundärnutzung von Gesundheitsdaten ohne Einzeleinwilligung erlaubt – sofern, es sei nochmals betont, ein *wirksamer* Schutz vor Missbrauch bestmöglich gewährleistet ist.

Anders verhält es sich, wenn die Gesundheitsdaten durch private Finanzierung zustande gekommen sind, z.B. ein »User« eine nicht von seiner Krankenversicherung finanzierte GesundheitsApp auf *eigene* Kosten gekauft hat und diese z.B. *seine* Blutdruckwerte in Verbindung mit Uhrzeiten und körperlicher Bewegung erfasst. Die Gewährung des Zugangs zu *diesen* Daten ist am ehesten als »Datenspende« zu bezeichnen und könnte als Ausdruck individueller Datensouveränität adressiert werden.[54] Allerdings ist das Wort Datenspende wiederum nur metaphorisch zu verstehen, denn das in der analogen Welt entwickelte Konzept von »Spende« impliziert, dass ich etwas zum Nutzen eines anderen weg-gebe und dann selbst nicht mehr habe – z.B. Geld, Kleidung, Blut oder eine Niere. Wenn ich mich entscheide,

53 Dieser Grundgedanke inkludiert die »privat« Versicherten. Diese bilden zum einen auch, wenngleich kleinere Solidargemeinschaften (vom partikularen Profitinteresse ihrer Anteilseigner kann in diesem Zusammenhang abgesehen werden). Zum anderen partizipieren sie an Gesundheitssystemstrukturen, die durch die große Zahl der gesetzlich Versicherten und über den Bundeszuschuss auch durch sie selbst (durch die privat Versicherten als Steuerzahlende) finanziert werden. Ethisch-normativ wären ihre Gesundheitsdaten genauso wie die gesetzlich Versicherter zu nutzen, auch wenn dies juristisch schwer umsetzbar sein mag.

54 Der Ausdruck »Datenspende« fand insbesondere durch die Ethikrat-Stellungnahme »Big Data und Gesundheit« von 2017 (S. 266 f.) Eingang in Diskurse über Daten und Digitalisierung. Er wurde aufgegriffen und weiter entwickelt (siehe beispielhaft Strech u.a. 2020 und Hummel u.a. 2021). Insofern seine Verwendung zu einem Umdenken im Umgang mit Daten beiträgt, dürfte sie in pragmatischer Absicht ähnlich akzeptabel sein wie die analogische Rede von individueller Datensouveränität. In beiden Fällen gilt aber das Caveat, dass aus Analogien *nie sicher* geschlossen werden kann, sondern sie eher zu Fehlschlüssen verleiten. Wenn der Ethikrat (2017, S. 266) z.B. fordert, dass »am Einwilligungsmodell grundsätzlich festzuhalten ist«, so wäre aufgrund des hier Ausgeführten z.B. für den Gesundheitsbereich zu differenzieren, dass die Einwilligung sowohl in Primär- als auch Sekundärnutzung allfälliger Gesundheitsdaten »grundsätzlich« in der – selbstbestimmten – Inanspruchnahme solidarisch finanzierter Gesundheitsversorgung bereits erfolgt ist.

Gesundheitsdaten aus einer privat finanzierten GesundheitsApp für ein bestimmtes Forschungsprojekt oder auch einem dafür angelegten Datenpool beim nationalen Forschungsdatenzentrum zur Verfügung zu stellen[55], dann bleiben diese Daten mir erhalten.

Auf jeden Fall ist das Wort Datenspende nicht angebracht zur Bezeichnung der Sekundärnutzung von durch solidarische Finanzierung gewonnenen Gesundheitsdaten, denn es ist konstitutiv für eine Solidargemeinschaft, dass jeder sich verpflichtet bzw. gesetzlich verpflichtet wird, nach seinen Möglichkeiten zu ihrem Funktionieren beizutragen. Dieser Beitrag wird in Bezug auf die Krankenversicherung in der Öffentlichkeit vor allem als finanzieller verstanden, aber es war schon bislang so, dass auch *Daten* aus der solidarisch finanzierten Gesundheitsversorgung als Beitrag zum Funktionieren des Solidarsystems genutzt werden, namentlich die Abrechnungsdaten, die auf Basis einer gesetzlichen Befugnisnorm ohne Einzel-Einwilligung auf Antrag für wohl definierte Forschungszwecke zugänglich gemacht werden.[56]

So hätte der Sachverständigenrat Gesundheit und Pflege sein Gutachten zur Entwicklung des Krankengelds (2015) so nicht schreiben können, wenn ihm nicht retrospektive, mehrere Jahre umfassende Analysen der pseudonymisierten Krankschreibungen einschließlich ICD-codierter Diagnosen von Millionen gesetzlich Krankenversicherter vorgelegen hätten.[57] Für die *Gesundheitssystemsteuerung* sind solche Analysemöglichkeiten sehr hilfreich, um z.B. im Fall des erwähnten Gutachtens datengestützte Empfehlungen geben zu können, mit welchen Maßnahmen der Anstieg längerer Arbeitsunfähigkeit (ab dem 43. Krankheitstag wird von den Krankenkassen Krankengeld gezahlt, zuvor erfolgt bei abhängig Beschäftigten Lohnfortzahlung im Krankheitsfall durch den Arbeitgeber) gebremst werden kann – was wiederum der Lebensqualität des einzelnen dient wie die Solidargemeinschaft vor vermeidbaren Kosten schützt. Um die *Qualität* der *Gesundheitsversorgung* zu verbessern, wäre es wichtig, auch die Behandlungsdaten analysieren zu kön-

55 Als pseudonymisierter oder anonymisierter Datensatz, der mit einigen für die Auswertung wichtigen Basisdaten wie Alter, Geschlecht, Gewicht, evtl. auch Vorerkrankungen oder besonderen Konditionen (z.B. Long-COVID-Diagnose seit Monat/Jahr) zur Verfügung gestellt wird.

56 Zentral ist hier die Befugnisnorm aus § 75 SGB X, der die die Übermittlung von Sozialdaten für Forschung und Planung (z.B. Steuerung des Gesundheitsversorgungssystems) regelt – *ohne* Einwilligungserfordernis.

57 Zu den »Datengrundlagen des Gutachtens« siehe Kapitel 4, Sachverständigenrat Gesundheit & Pflege 2015, S. 55–64. Dort auch (auf S. 63) »Vorschläge des Rates zur Verbesserung der Datengrundlage«.

nen. Diese sind in Arztpraxen, Krankenhäusern und Laboren vorhanden, aber sie können in Deutschland nicht zusammengeführt und Forschenden – kuratiert und kontrolliert – nicht zugänglich gemacht werden.

In der Grundlagenforschung, in der es oft mehr auf Qualität als auf Quantität (Big Data) ankommt, konnten deutsche Forscher in der SARS-CoV-2-Pandemie Bahnbrechendes beitragen – so zur schnellen Identifikation des Virus und zur zügigen Entwicklung eines Testverfahrens wie dann eines neuartigen Impfstoffs (mit der mRNA-Technik). Aber wenn eine schwere Nebenwirkung eines Arzneimittels oder eines Impfstoffs sehr selten ist (etwa nur bei jedem 50.000ten Patienten oder Impfling auftritt), dann kann sie in Zulassungsstudien mit z.B. 40.000 Probanden (von denen etwa die Hälfte das Placebo erhält) nicht systematisch, sondern nur zufällig festgestellt werden. Nur wenn die Gesundheitsdaten von Millionen Patienten und Geimpften zusammengeführt und pseudonymisiert für spezifische Forschungsfragen zugänglich sind, lassen sich extrem seltene »adverse effects« durch systematische (gegebenenfalls KI-gestützte) Analyse der verknüpften Daten herausfinden und spezifizieren (z.B. ein gering, aber doch noch signifikant erhöhtes Risiko einer Hirnvenenthrombose bei Impflingen weiblichen Geschlechts unter 65 Jahren).[58]

Diese grundsätzliche, kontrollierte Zugänglichkeit von Behandlungsdaten ohne Einzel-Einwilligung wäre kategorial nichts völlig Neues. Dass Behandlungsdaten wissenschaftlich aufgearbeitet und unter Experten diskutiert werden, gehört zum Kern einer empirischen Wissenschaft wie der Medizin. Dies kann in Fallstudien oder in der Auswertung der Daten größerer Kohorten geschehen. Wissen und Einwilligung des einzelnen Patienten sind insoweit nur gefordert, wenn ihn die wissenschaftliche Aufarbeitung oder Präsentation (z.B. bei einem Kongress) als Person *aktual* erkennbar, also identifizierbar machen würde. Das Argument, dass die heutigen Möglichkeiten der Datenverarbeitung durch umfassende Verknüpfung (Datenlinkage), Big Data, Genomanalysen, KI usw. jeden als Person *potenziell* erkennbar, also re-identifizierbar machen und insofern die explizite Einwil-

58 Anlässlich der Vorstellung seines Gutachtens zur Resilienzstärkung des Gesundheitssystems stellte der Sachverständigenrat Gesundheit und Pflege im Januar 2023 fest: »In der SARS-CoV-2-Pandemie war Deutschland weitgehend im Blindflug unterwegs. Bei den Verläufen und Folgen von Infektionen, Behandlungen und Impfungen mussten wir uns häufig auf wesentlich bessere Daten z.B. aus Dänemark oder Israel verlassen.« So das Ratsmitglied Prof. Petra Thürmann in der begleitenden Pressemitteilung – siehe https://www.svr-gesundheit.de/fileadmin/Gutachten/Gutachten_2023/SVR_Gutachten_2023_Pressemitteilung_19012023.pdf [4.8.2024].

ligung jedes einzuholen ist, vernachlässigt nicht nur den modalen Unterschied zwischen Möglichkeit und Wirklichkeit. Vor allem ist das Argument abzuwägen mit dem vielfältigen Nutzen, den eben die *verantwortliche* Nutzung der genannten Möglichkeiten hervorbringen kann,[59] und mit den realisierbaren (wenn wirklich gewollten) Möglichkeiten, unbefugte Zugriffe und Datenmissbrauch informationstechnisch zu verhindern, die Zugänge bzw. Zugriffe streng zu kontrollieren[60] und Verstöße ebenso wie damit zusammenhängende Stigmatisierung, Diskriminierung oder benachteiligung hart zu sanktionieren.

Dem eigenständigen Recht der Rechts- und Solidargemeinschaft auf verantwortliche Sekundärnutzung könnte eine (»individualethische«) Pflicht korrespondieren, eben diese Sekundärnutzung nicht nur zu akzeptieren, sondern zu *wollen*[61]: kantianisch z.B. im Sinne der Pflicht, zu anderer

59 Siehe Sachverständigenrat 2021, Tz 15: »Für den Nutzen des Patienten bzw. der Patientin wird […] entscheidend sein, dass die Daten aus seiner bzw. ihrer wie aus der Behandlung aller anderen für die Gesundheitsforschung genutzt werden können. Eine enge Verzahnung zwischen Versorgung und Forschung erhöht die Chancen differenzierter Diagnostik und zielgenauer Therapie auf dem jeweiligen Stand der Wissenschaft. Um diesen individuellen und kollektiven Nutzen zu ermöglichen, sollte geprüft werden, ob für Versorgungsdaten auf Basis von Artikel 9 Abs. 2 Datenschutz-Grundverordnung (DSGVO) eine gesetzliche Befugnisnorm zur Verarbeitung ohne Zustimmungserfordernis geschaffen werden kann. Für die Nutzung der Abrechnungsdaten der gesetzlichen Krankenkassen nach §§ 303a bis f SGB V gibt es bereits eine entsprechende Regelung. Die Behandlungsdaten, die im Rahmen solidarisch finanzierter Gesundheitsversorgung erhoben und ohnehin dokumentiert werden, sollten über die ePA pseudonymisiert an eine zentrale ›Sammelstelle‹ (Forschungsdatenzentrum (FDZ)) weitergeleitet werden, die diese Daten treuhänderisch verwaltet, sichert und für Forschungszwecke kuratiert zur Verfügung stellt.«

60 In anderen EU-Mitgliedstaaten wie Dänemark und Estland wird jeder Zugriff auf Gesundheitsdaten ad personam und unlöschbar protokolliert. So kann der Patient nachvollziehen, welcher Leistungserbringer (*namentlich* – nicht etwa »Arztpraxis X« oder »Station 5B«) wann in seine Patientenakte Einblick genommen hat, er kann diesen darauf ansprechen und wenn keine guten Gründe für die Einblicknahme vorgebracht werden (z.B. der Arzt nachweislich nicht konsultativ in die Behandlung involviert wurde), diesen rechtlich belangen. Die Rechtsfolgen sind empfindlich (bis hin zum Verlust der Approbation auf Lebenszeit).

61 So wie der Steuerpflichtige in einem Rechtsstaat grundsätzlich »seine« Steuern (als Beitrag zum Gemeinwesen) zahlen *wollen* muss. Es spricht vieles dafür, dass die Digitalisierung als eine der Einführung des Geldes (anstelle von Tauschobjekten) vergleichbare kulturgeschichtliche Disruption anzusehen ist. Digitalisierte Daten wären dann – wie Steuern – als Beitrag zum Gemeinwesen zu erheben und zu nutzen. Und ähnlich wie bei den Steuern wäre auch im Rahmen der Digitalisierung »der Staat« (im weitesten Sinne: auch etwa in Form delegierter Aufgaben wie der Gesundheitsversorgung der Bevölkerung) verantwortlich, durch geeignete Maßnahmen dafür zu sorgen, dass das Erhobene zu rechtmäßigen Zwecken gebraucht und der Missbrauch verhindert bzw. im Übertretungsfall bestraft wird. Niemand würde sich dazu verstehen, den potenziellen

»Glückseligkeit« (wozu man Leben und Gesundheit wird zählen dürfen) beizutragen[62]; ebenso in Weiterentwicklung des asymmetrischen Verantwortungsbegriffs Hans Jonas', wonach der der Daten »mächtigere« (zu dem ihn betreffende Behandlungsdaten z.B. zum Verlauf einer onkologischen Therapie vorliegen) dem Daten»schwächeren« (der eine vergleichbare Krebserkrankung hat und für deren bestmögliche Behandlung die Daten aus bisherigen Therapieverläufen analysierbar und mit den individuellen Parametern des Patienten abgleichbar sein müssten) durch Datenteilung zu helfen verantwortlich ist[63]; und schließlich etwa im weiterentwickelten Sinne Levinas', insofern das *Antlitz* des an Krebs Erkrankten, das mich und jeden, der eine solidarisch finanzierte Behandlung eines ähnlichen Krebsleidens erhalten hat, in die Pflicht nimmt, ihm die Behandlungsdaten (im Rahmen kontrollierter wissenschaftlicher Auswertung) potenziell *zu Gute kommen zu lassen*: das »Antlitz, in dem der Andere mich anruft und mir durch seine Nacktheit, seine Not, eine Anordnung zu verstehen gibt. Seine Gegenwart ist Aufforderung zu Antwort.«[64] Diese Antwort gibt der barmherzige Samariter als einzelner. Als einzelne, die zugleich Mitglieder einer Rechts- und Solidargemeinschaft sind, *sollten* wir alle sie geben, indem wir die (rechtlich ohnehin ermöglichbare – und zu ermöglichende) Sekundärnutzung von Behandlungsdaten auch *wollen* – und für sie eintreten.

IX. Ausblick in pragmatischer Hinsicht

Dass Maßnahmen wie die vorstehend skizzierten zum *wirksamen* Schutz vor Datenmissbrauch und zur Ermöglichung verantwortlicher Datennutzung bestmöglich realisiert werden, dürfte nicht wenig davon abhängen, dass von der deutschen Autosuggestion Abschied genommen wird, der zufolge unser Datenschutzverständnis das strengste der Welt sei. Es ist vielleicht das einseitigste, da es, wie im Verlauf dieser Überlegungen angemerkt, vor allem aus der Konstellation »Individuum gegen den in seinem Informati-

---

Missbrauch von Steuermitteln als Argument gegen staatliche Steuererhebung als solche zu verwenden. Dies gilt mutatis mutandis für die gesetzlich definierte Erhebung, Verarbeitung und Sekundärnutzung von Daten (einschließlich der besonders schützenswerten Gesundheitsdaten).

62 Siehe Kant 1981a [1797], S. 16.

63 Siehe hier Anmerkung 22.

64 Levinas 1983, S. 224.

onsbegehren übergriffigen Staat« gedacht ist und insofern primär Schutz als Abwehr und Einzel-Einwilligungen als wichtigste Gegenmaßnahme gegen solche Übergriffe versteht.

Aber das Individuum ist nicht nur schutzbedürftiges *Objekt* staatlichen, feindlichen, kommerziellen oder kriminellen Datenbegehrens (und eines oft wirkungslosen Schutzes davor), es ist auch selbst entscheidendes, lebendes, akut oder chronisch leidendes *Subjekt*, das auf Datennutzung in seinem Sinne, zu seinem Wohl angewiesen ist. Dieses Subjekt bedarf auch des Schutzes: des Schutzes der Möglichkeit, dass mit es betreffenden Daten im Sinne seiner selbst gesetzten Zwecke (z.B. Genesung) bestmöglich umgegangen wird. Dazu muss die Rechts- und Solidargemeinschaft entsprechende Rahmenbedingungen schaffen, die in zentralen Merkmalen vorstehend angesprochen wurden. Hierzu gehört im Gesundheitsbereich idealiter eine vollständige, bestmöglich geschützte, in Echtzeit befüllte und synchronisierte Elektronische Patientenakte, die für den Patienten wie für den von ihm aufgesuchten (= beauftragten!) Leistungserbringer leicht nutzbar ist und deren Funktionalität (über informationstechnische Spezifikationen) umfassende Primär- und Sekundärnutzung der Gesundheitsdaten ermöglicht. Um der Vollständigkeit willen wären keine Löschungs-, sondern die skizzierten Verschattungsoptionen vorzusehen. Nur so würde dem Patienten *Souveränität* (im metaphorischen Sinne) betreffend den *Zugang* zu »seinen« Gesundheitsdaten überhaupt erst ermöglicht.

Die Finanzwelt ist hier schon weiter als das Gesundheitssystem: Banken stellen »ethical hacker« ein. Deren Arbeit besteht in sog. Penetrationstests: Sie versuchen, Schwachstellen in der IT-Struktur des Unternehmens zu finden und damit Cyberattacken zu verhindern. Damit schützen sie nicht nur die Bank selbst vor schweren Schäden, sondern auch die Kunden der Bank. Auch und erst recht für die Datennutzung und die Datensicherheit im Gesundheitswesen wäre es sinnvoller, statt zusätzlicher Juristen, die das Einwilligungs(un)wesen nutzlos weiter ausdifferenzieren, gleichfalls »ethical hacker« einzustellen. Diese könnten mit Penetrationstests an allen einschlägigen Stellen der Gesundheitsversorgung (der Leistungserbringung wie der Kostentragung) dazu beitragen, dass die in diesem Kontext anfallenden Daten (Behandlungs- wie Abrechnungsdaten) jederzeit für Betroffene und Befugte zugänglich und vor unbefugten Zugriffen und Missbrauch bestmöglich geschützt sind. Zweifelsohne eine unendliche Aufgabe, aber einer, die immer neu zu erfüllen, der Mühe wert wäre, weil sie Leben, Gesundheit

und eine *hiermit* kompatible informationelle Selbstbestimmung oder, wie der Ethikrat formulierte, informationelle Freiheitsgestaltung schützt.

Diese Kompatibilität mit dem Schutz von Leben und Gesundheit scheint nicht nur ratsam oder klug, ihre Realisierung ließe sich mit Kant sowohl als eine der »*Pflichten* gegen sich selbst«[65] als auch als eine der »Pflichten gegen andere«[66] verstehen, da Selbstbestimmung ohne Leben[67] und zur Selbstbestimmung zumindest *hinreichende* physische und psychische Gesundheit hinfällig wäre. In diesem Sinne wäre es sogar jedem Individuum aus sich heraus *geboten*, dass es mit den anderen, von denen gemeinsam als »Volk« alle Staatsgewalt ausgeht, darauf hinarbeitet, die Rahmenbedingungen in Deutschland, was den Umgang mit und Zugang zu Daten betrifft, in den Bahnen der Gewaltenteilung weiterzuentwickeln. Ziel sollte sein, die Möglichkeiten sowohl verantwortlicher, kontrollierter einzel-, gruppen- und gemeinwohlnütziger Datennutzung als auch tatsächlich wirksamen Datenschutz (im Sinne von Datensicherheit) besser zu realisieren als durch die in Deutschland bislang vorrangig verfolgte Abspaltung formaljuristischer Einzel-Einwilligungen von der Selbstbestimmung des Individuums in lebensweltlichen Zusammenhängen wie dem solidarisch finanzierter Gesundheitsversorgung.

Literatur

Aristoteles: *Poetik*, Griechisch/Deutsch, übersetzt und herausgegeben von Manfred Fuhrmann, Stuttgart 1982.

Augsberg, Steffen/Gehring, Petra (2022): Datensouveränität als Diskursgegenstand: Ambiguität als Chance?, in: Augsberg, Steffen/Gehring, Petra (Hg.): *Datensouveränität. Positionen zur* Debatte, Frankfurt am Main, S. 7–17.

Beauchamp, Tom L./Childress, James F. (2013): *Principles of Biomedical Ethics*, New York/Oxford.

Blumenberg, Hans (2013): *Paradigmen zu einer Metaphorologie*, Frankfurt am Main.

Böhme, Gernot (2008): *Ethik leiblicher Existenz*, Frankfurt am Main.

65 Kant 1981a [1797], S. 63 ff.

66 Ebd., S. 116 ff.

67 Das Leben wird vom BVerfG (BVerfGE 39, 1, 42) als »die vitale Basis der Menschenwürde und die Voraussetzung aller anderen Grundrechte« bezeichnet.

Bundesregierung (2021): *Datenstrategie der Bundesregierung*, https://www.publikationen-bundesregierung.de/resource/blob/2277952/1845634/1a4 f7ea800bb838562e16fdfe4ffb354/datenstrategie-der-bundesregierung-download-bpa-data.pdf?download=1 [21.5.2024].

Fischer-Bollin, Peter (2021): »Souveränität der EU«. Äußere und innere Gefahren eines unerfüllbaren Versprechens, in: *Auslandsinformationen der Konrad-Adenauer-Stiftung*, https://www.kas.de/de/web/auslandsinformationen/artikel/detail/-/content/souveraenitaet-der-eu#SnippetTab [7.1.2024].

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

Gehring, Petra (2024): *Biegsame Expertise. Geschichte der Bioethik in Deutschland*, Frankfurt am Main [im Erscheinen].

Gehring, Petra (2022): Datensouveränität versus Digitale Souveränität: Wegweiser aus dem konzeptionellen Durcheinander, in: Augsberg, Steffen/Gehring, Petra: *Datensouveränität. Positionen zur Debatte*, Frankfurt am Main, S. 19–44.

Gehring, Petra (2006): *Was ist Biomacht? Vom zweifelhaften Mehrwert des Lebens*, Frankfurt am Main/New York.

Hegel, Georg Wilhelm Friedrich (1975 [1830]): *Enzyklopädie der philosophischen Wissenschaften*, in: ders.: *Werke*, Band 10, Frankfurt am Main.

Hummel, Patrik/Braun, Matthias/Augsberg, Steffen/von Ulmenstein, Ulrich/Dabrock, Peter (2021): *Datensouveränität: Governance-Ansätze für den Gesundheitsbereich*, Heidelberg/New York, https://link.springer.com/book/10.1007/978-3-658-33755-1 [21.5.2024].

Jonas, Hans (1979): *Das Prinzip Verantwortung. Eine Ethik für die technologische Zivilisation*, Frankfurt am Main.

Kant, Immanuel (1981a [1797]): Metaphysik der Sitten, in: ders.: *Werke in zehn Bänden*, herausgegeben von Wilhelm Weischeidel, Band 7, Darmstadt.

Kant, Immanuel (1981b [1793]): Die Religion innerhalb der Grenzen der bloßen Vernunft, in: ders.: *Werke in zehn Bänden*, herausgegeben von Wilhelm Weischeidel, Band 7, Darmstadt.

Kant, Immanuel (1981c [1787]): Kritik der reinen Vernunft, in: ders.: *Werke in zehn Bänden*, herausgegeben von Wilhelm Weischeidel, Band 3, Darmstadt.

Koalitionsvertrag (2021): *Mehr Fortschritt wagen. Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit*, https://www.bundesregierung.de/resource/blob/974430/1989762/9069d8019dabe546c2449dda2d838453/2021-12-08-koalitionsvertrag-data.pdf?download=1 [20.5.2024].

Lévinas, Emmanuel (1983): *Die Spur des Anderen. Untersuchungen zur Phänomenologie und Sozialphilosophie*, Freiburg/München.

Niggemeier, Frank (2002): *Pflicht zur Behutsamkeit? Hans Jonas' naturphilosophische Ethik für die technologische Zivilisation*, Würzburg.

Otto, Boris/Burmann, Anja (2021): Europäische Dateninfrastrukturen. Ansätze und Werkzeuge zur Nutzung von Daten zum Wohl von Individuum und Gemeinschaft, in: *Informatik Spektrum* 44, Heft 4, S. 283–291.

Person, Christian/Schütrumpf, Moritz (2022): Datensouveränität durch Dateninfrastrukturen: Das Leuchtturmprojekt Gaia-X, in: Augsberg, Steffen/Gehring, Petra: *Datensouveränität. Positionen zur Debatte*, Frankfurt am Main, S. 177–198.

Sachverständigenrat zur Begutachtung der Entwicklung im Gesundheitswesen (2023): *Gesundheitssystem für Krisen weiterhin nicht gut gewappnet*, https://www.svr-gesundheit.de/fileadmin/Gutachten/Gutachten_2023/SVR_Gutachten_2023_Pressemitteilung_19012023.pdf [4.8.2024].

Sachverständigenrat zur Begutachtung der Entwicklung im Gesundheitswesen (2021): *Digitalisierung für Gesundheit. Ziele und Rahmenbedingungen eines dynamisch lernenden Gesundheitssystems*, https://www.svr-gesundheit.de/fileadmin/Gutachten/Gutachten_2023/Gesamtgutachten_ePDF_Final.pdf [21.5.2024].

Sachverständigenrat zur Begutachtung der Entwicklung im Gesundheitswesen (2015): *Krankengeld – Entwicklung, Ursachen und Steuerungsmöglichkeiten*, https://www.svr-gesundheit.de/fileadmin/Gutachten/Sondergutachten_2015/Krankengeld_Druckfassung.pdf [15.5.2024].

Strech, Daniel/Kielmansegg, Sebastian Graf von/Zenker, Sven/Krawczak, Michael/Semler, Sebastian C. (2020): *»Datenspende« – Bedarf für die Forschung, ethische Bewertung, rechtliche, informationstechnologische und organisatorische Rahmenbedingungen*, wissenschaftliches Gutachten erstellt für das Bundesministerium für Gesundheit, https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/5_Publikationen/Ministerium/Berichte/Gutachten_Datenspende.pdf [21.5.2024].

von der Leyen, Ursula (2019a): A Union that strives for more. My agenda for Europe, https://commission.europa.eu/system/files/2020-04/political-guidelines-next-commission_en_0.pdf [5.5.2024].

von der Leyen, Ursula (2019b): *Eine Union, die mehr erreichen will. Meine Agenda für Europa*, political-guidelines-next-commission_de.pdf (europa.eu) [5.5.2024].

Welzel, Hans (1980): *Naturrecht und materiale Gerechtigkeit*, Göttingen.

Digitale Zwillinge in der Medizin: Datenessenzialismus, digitale Vulnerabilität und Gerechtigkeit

Philipp Kellmeyer

I. Einführung: *Homo geminus digitalis*

Durch die zunehmend feinere datenbasierte Charakterisierung der Merkmale und Verhaltensweisen eines Individuums, im internationalen Gebrauch als *digital phenotyping* bezeichnet, können mittlerweile sehr komplexe digitale Replikate dieser aggregierten digitalen Merkmale und Eigenschaften geschaffen werden, die als *digitaler Zwilling* bezeichnet werden.[1] In der medizinischen Forschung und Versorgung verspricht dieser Ansatz individuelle Krankheitszustände und -verläufe und darauf basierend personalisierte Diagnose-, Therapie- und Präventionsmaßnahmen *in silico* modellieren zu können. Da wir an der Schwelle zu dieser technologischen Entwicklung stehen, ist es unerlässlich, sich mit den vielschichtigen ethischen, rechtlichen und gesellschaftlichen Aspekten rund um digitale Zwillinge für gesundheits- und krankheitsbezogene Anwendungen zu befassen. Dieser Beitrag untersucht einige der komplexen anthropologischen normativen und gesellschaftlichen Herausforderungen digitaler Zwillingstechnologie im Hinblick auf gesundheitsbezogene Anwendungen aus einer dezidiert multidisziplinären Perspektive, um eine Engführung und Reduktion auf eine (bio)ethische Analyse von vorneherein zu vermeiden. Durch die Auseinandersetzung mit struktureller Ungerechtigkeit, Vulnerabilität als anthropologischer Dimension, den reduktionistischen Tendenzen des Datenessenzialismus und der nuancierten Kritik an der Phänotypisierung werden zunächst wichtige Spannungen identifiziert und beleuchtet. Dann wird mit Konzepten aus der Partizipationsforschung ein Modell für die

1 Barricelli/Fogli 2024; Venkatesh/Brito/Boulos 2024; Fagherazzi 2020.

verantwortungsvolle Entwicklung und Implementierung von digitalen Zwillingstechnologien entwickelt.

Besonderes Augenmerk wird dabei auf das Potenzial von Formen intensiver Partizipation in Forschung und Entwicklung[2] gelegt, moralische und ethische Spannungen bereits auf der Ebene der Technikentwicklung begegnen zu können und eine verantwortliche Innovationskultur im Bereich der digitalen Gesundheit zu fördern. Durch eine aktive Rolle von Interessensgruppen und Betroffenen – dem internationalen Sprachgebrauch folgend als *Stakeholder* bezeichnet – können Modelle für einen gerechteren Zugang zu Gesundheitstechnologien wie digitale Zwillinge entwickelt werden, die nicht nur technologisch fortschrittlich, sondern auch ethisch fundiert und sozial verantwortlich sind. Die Einbeziehung verschiedener Stakeholder in die Gestaltung, Implementierung und regulatorischen Steuerung von digitalen Zwillingen kann somit eine wichtige Komponente in der normativen Einbettung und Governance sein. Komplementär sind zur ethischen und rechtlichen Steuerung, im Sinne von effektiver Regulierung und Good Governance, natürlich auch rechtlich verbindliche Rahmenbedingungen für die Nutzung digitaler Zwillinge im Gesundheitswesen zu schaffen, welche beispielsweise im Beitrag von *Gruber und Zihlmann* in diesem Band dargelegt werden und als komplementär zu betrachten sind.

In den folgenden Abschnitten werden einzelne ethische Überlegungen entwickelt und Empfehlungen für eine verantwortungsvolle Entwicklung von digitalen Zwillingstechnologien im Gesundheitswesen vorgeschlagen.

II. Gesundheitsbezogene Anwendungsbereiche Digitaler Zwillinge

Um die vielseitigen Einsatzmöglichkeiten Digitaler Zwillinge in der biomedizinischen Forschung und medizinischen Versorgung ausschöpfen zu können, müssten zunächst die geeigneten technischen Voraussetzungen geschaffen werden.

Die klinische Nutzung digitaler Zwillinge erfordert beispielsweise die Integration und Verarbeitung großer Mengen heterogener Daten, neben Personendaten zu Alter, Geschlecht, insbesondere klinische Daten wie Geno-

2 Kellmeyer 2024.

mik, Daten aus Real-Time Monitoring (z.B. auf Intensivstationen), Daten aus elektronischen Patientenakten, Bildgebungsdaten und Daten aus vielen weiteren Quellen, in ebenfalls heterogenen IT-Ökosystemen (z.B. Kliniken, ambulante Versorgung, gegebenenfalls Versicherungen).

Die Herausforderungen im Hinblick auf Datenschutz, Interoperabilität und Datenintegration sind dabei immens. In Deutschland, wie in anderen Ländern, arbeiten daher mit Nachdruck große, standortübergreifende Medizininformatik-Initiativen und -konsortien an einer skalierbaren und datenschutzkonformen Integration klinischer Daten.[3]

Aktuelle Forschungsprojekte und Konzepte in der translationalen Forschung zeigen jedoch bereits das Potenzial Digitaler Zwillinge für die klinische Forschung und medizinische Versorgung. Hier einige Beispiele aktueller Anwendungen:

Krebserkrankungen: Digitale Zwillinge in der Krebsbehandlung ermöglichen es beispielsweise, virtuelle Simulationen durchzuführen, um die Reaktion eines Patienten auf verschiedene Krebstherapien vorherzusagen. Beispielsweise kann ein digitaler Zwilling genutzt werden, um die Wirksamkeit verschiedener Chemotherapie-Regime auf einen spezifischen Tumor zu simulieren, basierend auf der genetischen Konstitution und dem bisherigen Ansprechen des Patienten auf Behandlungen. Dies hilft, die Therapie zu personalisieren und Nebenwirkungen zu minimieren.[4]

Herz-Kreislauf-Erkrankungen: Bei Patienten mit Herzinsuffizienz kann der digitale Zwilling genutzt werden, um das Risiko von Ereignissen wie Herzinfarkten zu prognostizieren. Durch die Simulation verschiedener Szenarien und Behandlungsstrategien kann das Modell dabei helfen, die effektivste Medikation und Dosierung zu bestimmen und die Lebensqualität des Patienten zu verbessern.[5]

Diabetesmanagement: Ein digitaler Zwilling eines Diabetes-Patienten könnte kontinuierlich dessen Blutzuckerwerte simulieren und vorhersagen, wie verschiedene Faktoren wie Ernährung, körperliche Aktivität und Medikation den Blutzuckerspiegel beeinflussen. Dies würde eine sehr individuelle Anpassung des Behandlungsplans ermöglichen und helfen, gefährliche Schwankungen des Blutzuckerspiegels zu vermeiden.[6]

---

3 Albashiti u.a. 2024; Schepers/Fleck/Schaaf 2022.
4 Hernandez-Boussard u.a. 2021; Sager 2023.
5 Viola u.a. 2023; Coorey u.a. 2022.
6 Shamanna u.a. 2020 und 2021.

Prävention: Digitale Zwillinge können auch präventiv eingesetzt werden, um das Risiko für die Entwicklung chronischer Krankheiten basierend auf genetischen, umweltbedingten und Lebensstil-Faktoren zu bewerten. So könnten beispielsweise Ernährungs- und Bewegungspläne personalisiert und präventive Maßnahmen wie Impfungen oder regelmäßige Untersuchungen gezielt empfohlen werden.[7]

Durch die geplante Entwicklung eines Europäischen Gesundheitsdatenraums[8] und der damit verbesserten Datenintegration über Ländergrenzen hinweg könnten zukünftig die Vorteile digitaler Zwillinge noch umfassender genutzt werden. Durch den Zugriff auf umfangreiche, grenzüberschreitende Gesundheitsdaten könnten digitale Zwillinge präziser und umfassender in der klinischen Praxis implementiert werden, was die Patientenversorgung erheblich verbessern und die medizinische Forschung vorantreiben würde.

III. Konzeptuelle und ethische Aspekte digitaler Zwillinge

1. Konzeptuelle Aspekte der ethischen Debatte um Digitaler Zwillinge

Bei der ethischen Analyse der digitalen Zwillingstechnologien im Gesundheitswesen stützt sich unsere Diskussion zum Einen auf grundlegende medizinethische Prinzipien, die seit langem die biomedizinische Ethik in Deutschland und vielen anderen Ländern leiten, wobei in diesem Beitrag vor allem die Autonomie und die Gerechtigkeit – dem Verständnis von *Beauchamp* und *Childress* folgend – im Zentrum der Überlegungen stehen.[9] Darüber hinaus integrieren wir den Begriff der Vulnerabilität, wie er von

7 Milne-Ives u.a. 2022.

8 Lucas/Haugo 2024; Molnár-Gábor u.a. 2022.

9 Beauchamp/Childress 2001. Natürlich bewegen sich ethische Debatten in den allermeisten Kontexten und Gesellschaften stets im Spannungsfeld und im vollen Bewusstsein eines breit gefächerten moralischen und ethischen Pluralismus, sowohl was individuelle moralische Intuitionen angeht, als auch systematische Ethiktheorien und deren Anwendung. Dennoch lässt sich sagen, dass insbesondere im Bereich der biomedizinischen Ethik die Prinzipienethik nach Beauchamp and Childress starken Einfluss auf die Forschungsethik und Ethik im Gesundheitswesen hat. Da in den neueren Bereichsethiken für digitale Technologien (Roboterethik, KI-Ethik und Digitalethik) durchaus ein größerer Einfluss utilitaristischer Ethiken zu verzeichnen ist, wird es spannend zu beobachten sein, ob und inwieweit an der Schnittstelle zwischen Biomedizin und digitalen Technologie, in Zukunft vermehrt Werte- und Theoriekollision zu verzeichnen sein werden.

Catriona MacKenzie[10] umfassend konzeptualisiert wurde und zuletzt im Hinblick auf digitale Technologien als *digitale Vulnerabilität* aufgegriffen und entwickelt wurde[11], in unsere ethische Analyse.

Am Anfang der konzeptuellen Überlegungen möchten wir jedoch kurz den Blick auf den Begriff der Phänotypisierung und den damit konstruierten digitalen Identitäten lenken.

Phänotypisierung und digitale Identität

Der Phänotyp in der Biologie bezieht sich auf die beobachtbaren Merkmale oder Eigenschaften eines Organismus und die Phänotypisierung bezeichnet die Bestimmung dieser Merkmale, beispielsweise durch biometrische Messungen oder Verhaltensbeobachtungen. Diese Merkmale können anatomisch, biochemisch, physiologisch oder verhaltensbezogen sein und ergeben sich aus der Wechselwirkung des Organismus und der Umwelt. Die Phänotypisierung ist von entscheidender Bedeutung für das Verständnis der Vielfalt von Arten, einschließlich menschlicher Populationen, und für die Untersuchung, wie verschiedene genetische und Umweltfaktoren zu physischen und Verhaltensmerkmalen beitragen.

Die digitale Phänotypisierung im Kontext der digitalen Technologien erweitert dieses Konzept auf den digitalen Bereich. Es beinhaltet die Verwendung von Daten, die von digitalen Geräten wie Smartphones und Wearables erfasst werden, um den menschlichen Phänotyp auf individueller Ebene in situ zu quantifizieren.[12] Diese Daten können Aktivitäten in »sozialen« Medien, GPS-Standorte, Nutzungsmuster von Geräten und sogar Interaktionsdynamiken mit digitalen Plattformen umfassen. In der Forschung und bei Interventionen im Kontext der psychischen Gesundheit kann eine solche digitale Phänotypisierung zur Überwachung von Verhaltensweisen und Symptomen in Echtzeit eingesetzt werden, um ein dynamisches, umfassendes Bild des psychischen Zustands einer Person und ihrer Interaktionen mit der Umwelt zu erhalten.[13] Im Bereich der psychischen Gesundheit verspricht dieser Ansatz, neue Behandlungsoptionen für psychische Erkrankungen zu

10 Mackenzie/Rogers/Dodds 2013.
11 Kellmeyer 2020; Herzog/Kellmeyer/Wild 2022.
12 Dlima u.a. 2022; Insel 2017.
13 Birk/Samuel 2022.

schaffen, indem personalisierte, zeitnahe und kontextspezifische Interventionen ermöglicht werden.

Die digitale Phänotypisierung birgt zwar ein erhebliches Potenzial, doch müssen wesentliche konzeptionell-analoge Unstimmigkeiten zwischen der traditionellen biologischen Phänotypisierung und der digitalen Phänotypisierung beseitigt werden. Obwohl sie von Umweltfaktoren beeinflusst werden, basieren biologische Phänotypen in erster Linie auf beobachtbaren biologischen Merkmalen und sind oft unabhängig von der Wahrnehmung oder dem sozialen Einfluss des Probanden messbar und überprüfbar. Im Gegensatz dazu werden digitale Phänotypen aus Daten konstruiert, die in hohem Maße von Kontext, Benutzerinteraktion und technologischer Vermittlung abhängen. Die für die digitale Phänotypisierung verwendeten Daten sind anfällig für Variationen in der Art und Weise, wie Individuen die Technologie nutzen, was ihren physiologischen oder psychologischen Zustand möglicherweise nicht genau oder inkonsistent widerspiegelt.

Darüber hinaus birgt die Reduzierung einer Person auf beobachtbare Merkmale die Gefahr eines Essenzialismus, d.h. dass die beobachteten Merkmale als notwendige Eigenschaften einer Person fehlinterpretiert werden können. In den Sozialwissenschaften beschreibt Essenzialismus allgemein die Tendenz, Individuen oder Gruppen auf der Grundlage oberflächlicher oder allzu vereinfachter Merkmale feste Wesenszüge zuzuschreiben. Im Kontext der digitalen Phänotypisierung ist dies relevant und kritisch und birgt die Gefahr, die komplexe, mitunter fluide Natur der menschlichen Identität und gelebten Erfahrung auf eine begrenzte Anzahl von beobachtbaren digitalen Daten zu reduzieren. Dieser Reduktionismus kann problematisch sein, insbesondere dann, wenn digitale Phänotypen verwendet werden, um wichtige Entscheidungen über Behandlungen oder Interventionen im Bereich der psychischen Gesundheit zu treffen. Es besteht die Gefahr eines »Datenessenzialismus«, der Personen aufgrund ihres digitalen Verhaltens kategorisiert, was zu Stigmatisierung, Diskriminierung oder Fehldiagnosen führen kann.

Wenn zum Beispiel ein digitaler Phänotyp eine Neigung zu depressivem Verhalten allein aufgrund einer verminderten Smartphonenutzung oder einer verringerten Aktivität in den sozialen Medien nahelegt, könnte er die differenzierten Lebensumstände des Einzelnen übersehen, die seine digitalen Aktivitäten beeinflussen. Dies könnte zu unangemessenen oder unwirksamen Behandlungsempfehlungen führen, die nicht auf die zugrunde liegenden Ursachen der beobachteten Verhaltensweisen eingehen.

Die Bedeutung der Phänotypisierung bei der Erstellung digitaler Zwillinge erfordert daher eine kritische Prüfung. Diese Kritik geht über die Genauigkeit der digitalen Darstellungen hinaus und umfasst auch die umfassenderen Auswirkungen auf die personale Identität und Autonomie.

Konzeptuelle Aspekte der Autonomie im Hinblick auf Datennutzung

Das Prinzip der Autonomie, hier verstanden als die Fähigkeit einer Person zur Selbstbestimmung und das davon abgeleitete moralische Recht, eigenständige Entscheidungen zu treffen, , ist eine wichtige Voraussetzung für einen selbstbestimmten Umgang mit Daten, die zur (digitalen) Phänotypisierung genutzt werden können und somit für die Erstellung und Verwendung von digitalen Zwillingen.

Während in der Bioethik in vielen Traditionen Autonomie vorwiegend im Hinblick auf einzelne Personen betrachtet wird, eröffnet das Konzept der Relationalität eine neue Dimension in der Analyse. Diese Perspektive einer relationalen Autonomie, die beispielsweise von *Sara Goering* vertreten wird,[14] geht davon aus, dass Autonomie und Handlungsfähigkeit nicht nur Attribute isolierter Individuen sind, sondern in hohem Maße von Beziehungen und sozialen Kontexten geprägt werden. Die relationale Autonomie unterstreicht, dass die Fähigkeit des Einzelnen, autonome Entscheidungen zu treffen, von seinen Beziehungen zu anderen, einschließlich der Familie, der Gemeinschaft und gesellschaftlicher Strukturen, geprägt und beeinflusst wird. In ähnlicher Weise bezieht sich der Begriff der relationalen Handlungsfähigkeit (*relational agency*) auf die Fähigkeit des Einzelnen, innerhalb des Netzes dieser Beziehungen autonom zu handeln.

Zur Autonomie im Kontext digitaler Zwillinge gehört beispielsweise die, in Abschnitt II.2 untersuchte, Frage, inwieweit Patient:innen die Kontrolle über die Verwendung ihrer Daten haben und umfassend darüber informiert werden sollten. Aus einer relationalen Perspektive würde man ergänzen, dass hierfür eben auch die Angehörigen, Partner:innen und andere nahe Bezugspersonen eine wichtige Rolle spielen können.

14 Borrmann u.a. 2024; Goering u.a. 2017.

Gerechtigkeit und Fairness im Kontext digitaler Gesundheitstechnologien

Die Begriffe Gerechtigkeit und Fairness sind in ethischen Diskussionen von grundlegender Bedeutung, insbesondere bei der Bewertung der Verteilung von und Fragen des Zugriffs auf Gesundheitstechnologien wie digitalen Zwillingen. Diese Konzepte dienen als moralische Begriffe, die dabei helfen zu bestimmen, wie Nutzen und Lasten auf Individuen, aber auch verschiedene Gruppen innerhalb der Gesellschaft verteilt werden sollten.

Ein Aspekt, der insbesondere für den Zugang und die Verteilung von Gesundheitsgütern relevant ist in der ethischen Diskussion, ist die Dimension der strukturellen Ungerechtigkeit. Insbesondere die Arbeiten von *Iris Marion Young* haben einen wesentlichen Beitrag geleistet für das Verständnis, wie systemische Strukturen Ungleichheiten schaffen und aufrechterhalten können.[15] Youngs Fokus auf die sozialen Strukturen, die materielle und immaterielle Güter und Lasten ungleich über die Bevölkerung verteilen, unterstreicht die Bedeutung struktureller Faktoren, wie Armut oder Arbeitslosigkeit, hinsichtlich des Zugangs zu und Nutzung von Gesundheitstechnologien.[16]

Ein weiteres wichtiges Konzept, das in der Diskussion um Gerechtigkeit in digitalen Räumen und bei Systemen der Künstlichen Intelligenz (KI) eine zunehmend wichtige Rolle spielt, ist *epistemische Gerechtigkeit*. Epistemische Gerechtigkeit bezieht sich auf das Recht des Einzelnen, an wissensproduzierenden Aktivitäten teilzunehmen und als glaubwürdige:r Wissende:r (im Sinne eines epistemischen Subjekts) anerkannt zu werden. Der Begriff wurde von *Miranda Fricker* geprägt,[17] die zwei Hauptformen von epistemischer Ungerechtigkeit identifizierte: testimoniale und hermeneutische Ungerechtigkeit. Testimoniale Ungerechtigkeit liegt vor, wenn Sprecher:innen, beispielsweise aufgrund von Vorurteilen oder offener Diskriminierung, nicht die gebührende Glaubwürdigkeit zuerkannt wird. Dies wirkt sich auf die Fähigkeit aus, zu kommunizieren und gleichberechtigt an Diskussionen teilzunehmen. Hermeneutische Ungerechtigkeit liegt hingegen vor, wenn ein wichtiger Bereich der eigenen sozialen Erfahrung aufgrund struktureller Lücken in den kollektiven Interpretationsressourcen dem kollektiven Verständnis entzogen wird. So ist beispielsweise die Erhebung von Perspektiven, Einstellungen und Wertorientierungen von Betroffe-

15 Young 2013.
16 Herzog/Kellmeyer/Wild 2022.
17 Fricker 2007.

nen, wie Menschen mit (chronischen) Erkrankungen, kein nennenswerter Bestandteil der empirischen Forschung zu digitalen Zwillingen.[18]

In Abschnitt II.2 führen wir aus, dass eine Analyse der komplexen Aspekte von Gerechtigkeit und Fairness bei digitalen Zwillingen, wie bei Gesundheitstechnologien insgesamt, einen mehrdimensionalen Ansatz erfordert, der sich sowohl auf deontologische Ansätze als auch auf Theorien der strukturellen Ungerechtigkeit und epistemischen Gerechtigkeit stützt.

Vulnerabilität im Kontext digitaler Technologien in der Medizin

In unserer Analyse berücksichtigen wir zudem Vulnerabilität als grundlegende philosophisch-anthropologische Dimension als eine weitere konzeptionelle Erweiterung unseres Ansatzes. Theorien der Vulnerabilität betonen, dass verschiedene Faktoren wie Krankheit, sozioökonomischer Status und systemische Ungleichheiten die Fähigkeit des Einzelnen beeinträchtigen können, seine Interessen zu schützen oder seine Autonomie auszuüben. In erster Näherung kann Vulnerabilität zunächst konzeptionell als jedem Menschen innewohnende Möglichkeit der Verletzlichkeit, sowohl biologisch, psychologisch, aber auch sozial und ökonomisch, verstanden werden. Es ist daher ein multidimensionales Konzept und kann auf unterschiedlichen Ebenen (individuell, Gruppen, Gesellschaften) relevant werden.[19]

Vulnerabilität wird auch von verschiedenen internationalen Organisationen, darunter die Weltgesundheitsorganisation (WHO) und die Vereinten Nationen (UN), breit diskutiert, wobei sie je nach Schwerpunkt und Zielsetzung unterschiedliche Aspekte betonen.[20]

Aus dieser Perspektive wird Vulnerabilität als eine Kombination von Faktoren verstanden, die die Fähigkeit der Menschen einschränken, sich auf verschiedene Belastungen und Schocks, einschließlich wirtschaftlicher, sozialer und ökologischer Veränderungen, vorzubereiten, sie zu bewältigen und

18 Bezeichnenderweise finden sich in der aktuellen Literatur eher Erhebungen mit Expert:innen zu Digital Twins (De Maeyer/Markopoulos 2021) oder gar Interviews mit Ärztinnen und Ärzten zur Verwendung eines digitalen Zwillings ihrer selbst (*digital twin doctor*), vgl. Zalake 2023, statt systematischer qualitativer Forschung zu Einstellungen von Patient:innen.

19 Brown/Ecclestone/Emmel 2017; Ganguli-Mitra/Biller-Andorno 2011.

20 Die Weltgesundheitsorganisation (WHO) als Teil der Vereinten Nationen (UN) definiert Vulnerabilität als: »The conditions determined by physical, social, economic, and environmental factors or processes which increase the susceptibility of an individual, a community, assets, or systems to the impacts of hazards.« WHO 2024; vgl. UN 2024.

sich davon zu erholen. Diese Definition umfasst die Anfälligkeit für Schäden, die mangelnde Fähigkeit, die Auswirkungen zu antizipieren und zu bewältigen, sowie die Unfähigkeit, sich von den Schäden oder Veränderungen wirksam zu erholen.

Catriona MacKenzie, aus der Perspektive der feministischen Philosophie, vereint diese externen und internen Aspekte von Vulnerabilität als einen Zustand, der sowohl dem Menschen inhärent ist als auch durch soziale, politische und wirtschaftliche Faktoren kontextuell hergestellt oder verschärft wird. Dies ermöglicht ein differenziertes Verständnis der Erfahrungen von Patient:innen im Gesundheitssystem und unterstreicht die Notwendigkeit, dass Gesundheitstechnologien wie digitale Zwillinge mit einem ausgeprägten Bewusstsein für die Vulnerabilitäten entwickelt und implementiert werden, die sie aufdecken oder verschärfen können.

Dieses Verständnis von Vulnerabilität als eine grundlegende anthropologische Dimension ermöglicht uns, über abstrakte ethische Prinzipien hinauszugehen und die gelebten Erfahrungen der Menschen zu berücksichtigen, die mit digitalen Zwillingstechnologien interagieren. Es zwingt uns zu fragen: Wer ist am meisten gefährdet, durch diese Technologien in welcher Weise geschädigt zu werden? Wie können digitale Zwillinge so gestaltet werden, dass sie die am meisten gefährdeten Personen schützen und stärken? Indem wir die Vulnerabilität in unsere ethische Analyse einbeziehen, vertiefen wir unser Verständnis für das komplexe Zusammenspiel von Technologie, Gesundheit und Umwelt.

Zusammenfassend lässt sich zu diesen konzeptionellen Überlegungen sagen, dass der ethische Rahmen für die folgenden Überlegungen aus dem oben ausgeführten Verständnis von struktureller Ungerechtigkeit und einem ethisch-anthropologischen Verständnis von Vulnerabilität besteht.

2. Spezifische ethische Herausforderungen Digitaler Zwillinge

In diesem Abschnitt werden einige, in bisherigen Beiträgen in der ethischen Debatte bislang eher unterbeleuchtete, Überlegungen vorgestellt, die für eine verantwortungsvolle Entwicklung und Umsetzung von digitalen Zwillingstechnologien im Gesundheitswesen unerlässlich sind. Der Schwerpunkt der Analyse liegt dabei auf den Themen digitale Phänotypisierung und den Risiken eines Datenessenzialismus, den ethischen Aspekten

digitaler Vulnerabilität und den Herausforderungen durch strukturelle Ungerechtigkeit.

Ethische Risiken von digitaler Phänotypisierung und Datenessenzialismus

Im Mittelpunkt der digitalen Zwillinge steht der komplexe Prozess der, von Gesundheitsanthropologen treffend bezeichneten, »Datafizierung« (*datafication*),[21] bei dem die physischen Eigenschaften und die Gesundheitsdynamik von Menschen in digitale Datenpunkte umgewandelt werden. Die Reduzierung der menschlichen Komplexität auf quantifizierbare Daten, bezeichnen wir im Folgenden als *Datenessenzialismus*. Ein ethisches Kernproblem besteht darin, dass die menschliche Gesundheit und Identität möglicherweise zu stark vereinfacht wird und die Gefahr besteht, dass die Komplexität des Individuums, welches teils schwer zu quantifizierende Dimensionen menschlicher Erfahrung in sich vereint, jenseits der Daten aus den Augen verloren wird.

Die reduktionistische Perspektive, dass der Gesundheitszustand, das Verhalten und die Identität einer Person vollständig durch digitale Datenmodelle erfasst und verstanden werden könnte, übersieht die Komplexität und Fluidität der menschlichen Identität, die mit quantifizierbaren Daten nicht vollständig erfasst werden kann. Bei einer zu starken Fokussierung auf digitale Phänotypisierung besteht daher die Gefahr, dass der Gesundheitszustand und die Identität des Einzelnen zu stark vereinfacht und falsch dargestellt werden, was zu einem Gesundheitsparadigma führen könnte, das datengesteuerten Modellen Vorrang vor einem differenzierten Verständnis von Patient:innen als komplexe und mehrdimensionale Individuen einräumt.

Darüber hinaus wirft die Konstruktion digitaler Identitäten durch Phänotypisierung ethische Fragen nach der Authentizität und dem Eigentum an diesen Identitäten auf. Da digitale Zwillinge immer ausgefeilter werden, könnte die Unterscheidung zwischen dem digitalen und dem physischen Selbst verschwimmen. Dies könnte mit der Zeit unsere tradierten Vorstellungen von personaler Identität und Handlungsfähigkeit (*personal agency*) – welche wiederum eng verknüpft mit unserem Verständnis von Autonomie sind – im digitalen Zeitalter in Frage stellen.

21 Ruckenstein/Schüll 2018.

Abgesehen von den ethischen Risiken im Zusammenhang mit Identität und Personalisierung birgt die digitale Phänotypisierung auch konkrete Risiken im Zusammenhang mit dem Missbrauch digital konstruierter Identitäten für moralisch problematische oder illegale Zwecke. Die detaillierten Gesundheitsprofile, die durch die digitale Phänotypisierung erstellt werden, könnten beispielsweise zur Zielscheibe für Angriffe auf die Privatsphäre werden, wobei der unbefugte Zugriff auf sensible Gesundheitsdaten zu Identitätsdiebstahl, Diskriminierung oder sogar Erpressung führen könnte.[22] Die Granularität der Daten, die bei der digitalen Phänotypisierung verwendet werden, verstärkt die potenziellen Auswirkungen solcher Verstöße und stellt ein erhebliches Risiko für die Privatsphäre und die Sicherheit des Einzelnen dar.

Darüber hinaus erstreckt sich der Missbrauch der digitalen Phänotypisierung auch auf unheilvollere Szenarien, wie Cyberangriffe auf Krankenhäuser, Gesundheitssysteme oder Bioterrorismus.[23] Durch die Ausnutzung der Schwachstellen digitaler Gesundheitsdaten und der Systeme, die sie verwalten, könnten böswillige Akteure Angriffe inszenieren, die die Privatsphäre des Einzelnen gefährden und die öffentliche Gesundheit bedrohen. Die Manipulation digitaler Zwillingsdaten könnte beispielsweise zu falschen Diagnosen, unangemessenen Behandlungen oder der vorsätzlichen Einführung von Ineffizienzen im Gesundheitswesen führen. Solche Szenarien unterstreichen den dringenden Bedarf an robusten Datenschutzmaßnahmen und ethischen Richtlinien für die digitale Phänotypisierung und digitale Zwillinge im Gesundheitswesen.

Autonomie im Kontext digitaler Zwillinge

Digitale Zwillinge versprechen, den Patient:innen durch personalisierte Modellierung ihres Gesundheitszustands und durch maßgeschneiderte Interventionen mehr Entscheidungskompetenz zu verleihen, beispielsweise in der Auswahl von Therapieverfahren nach Beratung durch ihre Behandler:in. Diese Befähigung steht im Einklang mit den oben skizzierten Ansätzen einer relationalen Autonomie und Agency, da sie potenziell die Fähigkeit der Patient:innen verbessert, in Zusammenarbeit mit den Gesundheitsdienstleistern und Anderen (beispielsweise Angehörigen) fun-

22 Luh/Yen 2020.

23 Jørgensen/Shukla/Katt 2024; Al-Dalati 2023.

dierte Entscheidungen über ihre Gesundheitsversorgung zu treffen. Diese Befähigung ist jedoch nicht ohne Risiken. Die umfangreiche Datenerfassung, die für digitale Zwillinge erforderlich ist, wirft wie oben ausgeführt Bedenken hinsichtlich des Schutzes der Privatsphäre, der Datensicherheit und des potenziellen Missbrauchs von persönlichen Gesundheitsinformationen auf. Es besteht somit die Gefahr, dass gerade die Technologie, die den Patient:innen mehr Handlungs- und Entscheidungsspielraum geben soll, ihre Autonomie untergräbt, indem sie ihre tatsächliche Kontrolle über ihre Gesundheitsdaten vermindert oder zumindest erschwert. Das Gleichgewicht zwischen der Nutzung der Vorteile digitaler Zwillinge für die Stärkung der Patient:innen und dem Schutz der Patientenautonomie und des Datenschutzes stellt daher ein kritisches ethisches Dilemma dar.

So erfordern die meisten Datenzwillinge eine kontinuierliche, umfassende Datenerhebung und -verarbeitung zur Erstellung und Aktualisierung. Eine wichtige Frage ist dabei, inwieweit bestehende Standards und Verfahren der informierten Einwilligung (*informed consent*), angesichts der Komplexität, die mit dem Verständnis und der Zustimmung zur Verwendung persönlicher Gesundheitsdaten für Datenzwillinge verbunden ist, ein hinreichendes Instrument zur Wahrung der Autonomie sein können. Ein Faktor ist dabei die Fähigkeit des Einzelnen, bestimmte Datennutzungsmodelle auf der Grundlage klarer, umfassender Informationen zu verstehen, zu bewerten und ihnen freiwillig zuzustimmen. Die dynamische und sich fortlaufend weiterentwickelnde Natur digitaler Zwillinge in Verbindung mit den komplizierten Algorithmen, die ihrer Funktionalität zugrunde liegen, verkompliziert die Anforderung an eine informierte Einwilligung und kann dazu führen, dass die Patient:innen nicht mehr verstehen, wie ihre Daten verwendet werden und für welche Zwecke.

Einerseits ist die informierte Einwilligung nach wie vor *das* zentrale Instrument zur Wahrung der individuellen Autonomie und erfüllt neben dieser moralischen auch eine entscheidende Funktion im Rechtsverhältnis zwischen Patient:innen und Behandler:innen.

In der aktuellen bioethischen Forschung wird die normative Qualität der Verfahren im Gesundheitswesen, mit denen Behandler:innen eine informierte Einwilligung einholen, jedoch zunehmend kritisiert. Die Debatte um die Frage, ob im Zeitalter steigender Komplexität medizinischer Verfahren etablierte Informed-Consent-Modelle noch zeitgemäß sind und die Inter-

essen von Patient:innen ausreichend schützen ist nicht neu,[24] wird aber durch die rasante Innovationsdynamik der KI und Datenmedizin weiter verschärft. Ein zentraler Kritikpunkt ist dabei die Frage, ob traditionelle Consent-Modelle in der Lage sind, Patient:innen angemessen über die möglichen (auch unintendierten) Folgen der Erhebung, Verarbeitung und Speicherung digitaler Daten aufzuklären und angemessenen Datenschutz bieten und gleichzeitig mit der technologischen Entwicklung Schritt halten.[25] Die EU Datenschutz-Grundverordnung (DS-GVO), beispielsweise, stellt hohe Anforderungen an die Transparenz und die Kontrolle der Nutzer:innen über ihre Daten. Sie fordert, dass die Zustimmung spezifisch, informiert und eindeutig sein muss.[26] Dies kann bei komplexen digitalen Gesundheitstechnologien, wie digitalen Zwillingen, zu einer Herausforderung werden, da oft nicht vollständig nachvollziehbar ist, welche Daten gesammelt werden, wie sie analysiert und verwendet werden und welche langfristigen Auswirkungen dies haben könnte.[27]

Darüber hinaus wird kritisiert, dass die dynamische Natur digitaler Technologien und die fortlaufende Datenanalyse eine einmalige Einwilligung obsolet machen, da sich die Verwendungsweisen der Daten im Laufe der Zeit erheblich ändern können. In diesem Zusammenhang wird, beispielsweise auch im Rahmen der Medizininformatik-Initiative, zuletzt das Thema breite Einwilligung (*broad consent*) wieder stärker in den Fokus der, durchaus kontrovers geführten, Diskussion gerückt.[28] Die Diskrepanz zwischen der statischen Natur traditioneller Consent-Verfahren und der dynamischen Verwendung von Gesundheitsdaten führt jedoch auch in *broad consent* Modellen mitunter zu einer Lücke in der Schutzwirkung für die Betroffenen. Forscher:innen und Ethiker:innen fordern daher eine Überarbeitung, so dass die Verfahren künftig eine fortlaufende und dynamische Zustimmung ermöglichen, welche die Patientenautonomie stärkt und eine kontinuierliche Auseinandersetzung und Anpassung an neue Informationslagen und technologische Entwicklungen ermöglicht.[29]

---

24 Bester/Cole/Kodish 2016; O'Neill 2009.

25 Wiertz/Boldt 2022; Donnelly/McDonagh 2019.

26 DS-GVO Artikel 4 Nr. 11 (Definition der Einwilligung): Hier wird die Einwilligung definiert als »jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung«. Artikel 7 gibt Bedingungen für die Einwilligung an.

27 Vanberg 2021.

28 Zenker u.a. 2024; Hofmann 2022; Fröhlich/Spiecker 2022; Hallinan 2020.

29 Budin-Ljøsne u.a. 2017; Mascalzoni u.a. 2022.

Nachteile solcher sehr granulären und iterativen Formen der Zustimmung – beispielsweise elektronisch mittels einer Plattform und/oder App – sind, dass die vorgeschlagenen Modelle oft eine hohe Verfügbarkeit, digitale Kompetenz und grundlegendes Verständnis für komplexe Forschungsszenarien seitens der Betroffenen voraussetzen. Diese Herausforderungen könnten sich als relevante Barrieren für die Akzeptanz, tatsächliche Nutzung (*uptake*) und Effektivität dynamischer Consentverfahren erweisen.

Ethische Rahmenbedingungen und Zustimmungsprozesse müssen daher weiterentwickelt werden, insbesondere auch um die relationalen Dimensionen der Autonomie und Agency im Bezug auf Datennutzung widerzuspiegeln und den Einfluss sozialer Kontexte und Beziehungen auf die Fähigkeit des Einzelnen, Autonomie auszuüben, zu berücksichtigen. Dies bedeutet, dass die Transparenz in Bezug auf die Datennutzung erhöht werden muss indem technische Verfahren – wie beispielsweise *differential privacy*[30] oder *federated learning*[31] – genutzt werden, um die Zustimmungsprozesse und -verfahren adaptiv und iterativ zu gestalten. Darüber hinaus kann die Einbeziehung von Patient:innen, Familien, Communities und Gesundheitsdienstleistern in einen kontinuierlichen Dialog über die ethischen Auswirkungen digitaler Zwillinge dazu beitragen, das Spannungsfeld zwischen Befähigung und Risiko im Hinblick auf die Autonomie zu bewältigen und Digitale Zwillinge als vielversprechende Innovation zu fördern.

Vulnerabilität im Kontext digitaler Zwillinge

Die Verbindung des Datenessenzialismus mit der ethischen Linse der Vulnerabilität, insbesondere dem Konzept der »digitalen Vulnerabilität«[32], bereichert die ethische Analyse in vielerlei Hinsicht. Der Begriff »Digitale Vulnerabilität« erkennt an, dass die Digitalisierung von persönlichen Gesundheitsinformationen und Identitäten diese nicht lediglich in neutrale Datenpunkte verwandelt. Vielmehr setzt sie die betroffenen Individuen neuen Formen von Risiken, Zwängen und potenzieller Ausbeutung aus. Dieses Konzept verdeutlicht, wie die reduktionistischen Tendenzen des Datenessenzialismus die Vulnerabilität im Sinne einer Gefährdung des Einzelnen für konkrete Schäden potenziell verschärfen können. Dies ge-

30 Hassan/Rehmani/Chen 2020.
31 Nagaraj u.a. 2023; Yazijy/Schölly/Kellmeyer 2022.
32 Kellmeyer 2020.

schieht nicht nur durch mögliche Beeinträchtigungen der Privatsphäre und individuellen Autonomie. Ebenso wird die Berücksichtigung und Modellierung der vielschichtigen sozialen und umweltbedingten Determinanten von Gesundheit[33] vernachlässigt, die sich nicht ohne Weiteres quantifizieren oder in Datenmodelle übersetzen lassen.

Diese Perspektive zwingt uns, kritisch zu reflektieren, inwiefern aktuelle Visionen digitaler Zwillingstechnologien die komplexen gelebten Erfahrungen und soziokulturellen Einbettungen von Individuen, insbesondere aus marginalisierten oder besonders verletzlichen Gemeinschaften, ausreichend berücksichtigen.

Die anthropologische Konzeptualisierung von Vulnerabilität durch *Catriona MacKenzie*, wie oben ausgeführt, verbindet die internen, dem Menschen inhärenten Aspekte von Vulnerabilität mit externen, durch soziale, politische und wirtschaftliche Faktoren bedingten oder verschärften Dimensionen. Dieses ganzheitliche Verständnis erlaubt es, die vielschichtigen Erfahrungen von Patienten im Gesundheitssystem differenziert zu erfassen. Es unterstreicht die Notwendigkeit, dass Gesundheitstechnologien wie digitale Zwillinge von Beginn an mit einem ausgeprägten Bewusstsein für jene Vulnerabilitäten entwickelt und implementiert werden müssen, die sie möglicherweise aufdecken oder sogar exazerbieren könnten. Der Vulnerabilitätsansatz zwingt uns, stets die kritischen Fragen zu stellen: Wer ist am meisten gefährdet, durch diese Technologien in welcher Weise geschädigt zu werden? Wie können digitale Zwillinge gestaltet werden, dass sie die verletzlichsten Personen aktiv schützen und stärken?

Wenngleich die personalisierte Präzisionsmedizin durch digitale Zwillingstechnologien zweifelsohne bedeutende Fortschritte in der Gesundheitsversorgung verspricht, müssen bestehende oder dadurch möglicherweise exazerbierte bzw. neu entstehende Vulnerabilitäten daher äußerst sorgfältig und systematisch untersucht werden. Dies erfordert allerdings eine substanzielle Förderung methodisch komplexer sozialwissenschaftlicher Begleitforschung, um diese vielschichtigen Wechselwirkungen zwischen Technologie, Gesundheit, sozialen Strukturen und individuellen Lebenswelten wissenschaftlich plausibel und tiefgehend analysieren zu können.

Indem wir die inhärenten Grenzen eines rein datengesteuerten Ansatzes anerkennen und uns das Konzept der digitalen Vulnerabilität als integralen Bestandteil ethischer Analysen zu eigen machen, können wir gezielt Kon-

33 Marmot/Wilkinson 2005.

zepte entwickeln, die das Potenzial digitaler Zwillingstechnologien in der Medizin ausschöpfen, ohne bestehende Vulnerabilitäten zu verschlimmern, oder im besten Fall sogar zu reduzieren.

Ethische Implikationen Digitaler Zwillinge im Hinblick auf Gerechtigkeit

Wie oben beschrieben, bezieht sich Gerechtigkeit im bioethischen Diskurs meist auf die moralische Verpflichtung, auf der Grundlage einer fairen Abwägung zwischen konkurrierenden Ansprüchen zu handeln. Im Hinblick auf digitale Zwillinge im Gesundheitswesen ist es daher entscheidend zu prüfen, wie diese Technologie für verschiedene soziale Gruppen zugänglich und nutzbringend gemacht werden kann, um strukturelle Ungerechtigkeiten und Ungleichheiten in der Gesundheitsversorgung anzugehen.

Die Verheißung digitaler Zwillinge im Gesundheitswesen ist verlockend und bietet eine Zukunft, in der die Gesundheitsversorgung jedes Einzelnen auf seine einzigartige Konstitution zugeschnitten werden kann. Dieses Versprechen wird jedoch durch die potenzielle Aufrechterhaltung und Verschlimmerung bestehender struktureller Ungerechtigkeiten innerhalb des Gesundheitssystems überschattet. Die Zugänglichkeit digitaler Zwillingstechnologien, die in erster Linie von sozioökonomischen, geografischen und kulturellen Faktoren abhängt, birgt ein erhebliches Risiko, die Kluft zwischen denjenigen, die über reichlich Ressourcen verfügen, und denjenigen, die keine haben, zu vergrößern.

Durch die Anwendung des Ansatzes von *Iris Marion Young*[34] können wir erkennen, wie digitale Zwillinge unbeabsichtigt bestehende Ungleichheiten verstärken können, ohne dass ein absichtliches Eingreifen erforderlich ist.

Die hohen Kosten für die Entwicklung und den Einsatz digitaler Zwillinge könnten beispielsweise dazu führen, dass sie sich auf wohlhabendere Gesundheitssysteme konzentrieren und selbst innerhalb dieser Länder, wirtschaftlich benachteiligte Bevölkerungsgruppen an den Rand drängen. Dies veranschaulicht Youngs Begriff der Marginalisierung, bei dem den Schwächsten der Zugang zu wichtigen Diensten und Technologien verwehrt wird, was die gesundheitlichen Ungleichheiten weiter verschärft.

Darüber hinaus kann der Rückgriff auf umfangreiche und vielfältige Datensätze zur Erstellung genauer und effektiver digitaler Zwillinge, die aus nicht-repräsentativen (aus globaler Perspektive) Daten aus Ländern mit ho-

34 Young 2009.

hem Einkommen stammen, inhärente Verzerrungen (im Sinne von Biases) verstärken. Wenn die Daten in erster Linie die Gesundheitsprofile bestimmter Gruppen widerspiegeln, besteht die Gefahr, dass die besonderen gesundheitlichen Bedürfnisse und Bedingungen von Minderheitenbevölkerungen, deren Daten möglicherweise unterrepräsentiert oder falsch dargestellt werden, an den Rand gedrängt werden. Dies untergräbt die Wirksamkeit digitaler Zwillinge für diese Gruppen und verstärkt ein Narrativ, in dem ihre gesundheitlichen Erfahrungen und Ergebnisse als weniger bedeutsam angesehen werden.

Im Zusammenhang mit digitalen Zwillingstechnologien bedeutet dies eine konzertierte, international koordinierte Anstrengung, um sicherzustellen, dass Datenerhebungs- und Algorithmenentwicklungsprozesse inklusiv und repräsentativ für das gesamte Spektrum der menschlichen Vielfalt sind. Auf diese Weise können die Risiken von Ausbeutung und Machtlosigkeit gemindert und sichergestellt werden, dass digitale Zwillinge als Werkzeuge zur Ermächtigung bislang unterrepräsentierter und marginalisierter Gruppen und nicht zur Unterdrückung dienen. Das Gebot, dafür zu sorgen, dass die Vorteile des technologischen Fortschritts gerecht verteilt werden, steht im Einklang mit Youngs Forderung nach sozialer Gerechtigkeit. Dies erfordert Strategien und Praktiken, die speziell auf die Beseitigung von Zugangsbarrieren, einschließlich wirtschaftlicher, geografischer und kultureller Hindernisse, abzielen.

Die Anwendung des theoretischen Rahmens von Iris Marion Young auf die Analyse digitaler Zwillingstechnologien im Gesundheitswesen zeigt, dass die Erzielung gerechter Ergebnisse mehr als nur technologische Innovationen erfordert. Es erfordert eine Neugestaltung der Gesundheitspraktiken und -politiken, um Gerechtigkeit, Inklusivität und den aktiven Abbau systemischer Vorurteile in den Vordergrund zu stellen. Auf diese Weise können wir das transformative Potenzial digitaler Zwillinge nutzen, um eine fortschrittliche, gerechte und solidarische Zukunft der Gesundheitsversorgung für alle zu schaffen.

Im Zusammenhang mit digitalen Gesundheitstechnologien wie digitalen Zwillingen ist zudem die epistemische Gerechtigkeit von entscheidender Bedeutung, um sicherzustellen, dass das Wissen und die Erfahrungen aller potenziellen Nutzergruppen bei der Entwicklung, Einführung und Regulierung dieser Technologien berücksichtigt werden. Dazu gehört, dass unterschiedliche Patientenerfahrungen anerkannt werden und sichergestellt wird, dass diese Technologien bestehende gesundheitliche Ungleichheiten

oder strukturelle Ungerechtigkeiten nicht verstärken. Die Algorithmen der digitalen Zwillinge sollten so konzipiert sein, dass sie die unterschiedlichen medizinischen Reaktionen verschiedener Rassen, Geschlechter und sozioökonomischer Gruppen berücksichtigen. Auch dies erfordert naturgemäß ein hohes Maß and internationaler Kooperation und den entsprechenden politischen Willen. Eine wichtige Rolle kann dabei die Einbeziehung von Betroffenen durch hohe Grade von Partizipation sein.

IV. Partizipation und Good Governance in der Entwicklung und Implementierung Digitaler Zwillinge.

1. Das Potenzial partizipativer Forschung und Entwicklung digitaler Zwillinge

Modelle partizipativer Forschung und Entwicklung und ihr ethischer Mehrwert

Ausgehend von den an anderer Stelle entwickelten Überlegungen,[35] befasst sich dieser Abschnitt mit der Integration partizipativer Modelle in die Forschung und Technologieentwicklung, insbesondere im Zusammenhang mit digitalen Zwillingen im Gesundheitswesen. Die ethische Entwicklung und der Einsatz digitaler Zwillinge im Gesundheitswesen können nicht im Alleingang erfolgen. Eine wesentliche Rolle, sowohl für die ethische Legitimation als auch für die Akzeptanz, spielen partizipative Formen der Forschung und Entwicklung.

Partizipative Forschung und Entwicklung beinhaltet oft *mixed-methods* Ansätze mit Fokusgruppen, Interviews, Methoden aus der Designforschung und psychologischer Forschung zu Mensch-Technik-Interaktion.[36] Diese Ansätze können produktiv auf die Entwicklung digitaler Gesundheitstechnologien übertragen werden, um sicherzustellen, dass die Perspektiven und Bedürfnisse der Nutzer in den Entwicklungsprozess einfließen.

Eine partizipative Forschung, die von Communities geleitet wird, bietet einen Paradigmenwechsel in der Entwicklung medizinischer KI-Systeme. Diese Ansätze betonen die aktive Einbindung von Communities in alle Phasen des Forschungs- und Entwicklungsprozesses, von der Definition der

35 Kellmeyer 2024.

36 Chevalier/Buckles 2019; Schneider 2010; Björling/Rose 2019.

Forschungsfrage bis zur Interpretation der Ergebnisse. Durch die aktive Beteiligung der Communities können die einzigartigen Einsichten, gelebten Erfahrungen und Bedürfnisse der Betroffenen direkt in die Entwicklung der Technologien einfließen. Dies fördert die ethische Integrität der Technologien und stellt sicher, dass sie sowohl technisch solide als auch sozial verantwortungsvoll eingebettet sind.

Partizipative Forschung und Entwicklung bietet somit einen vielversprechenden Weg, um sicherzustellen, dass digitale Zwillinge und andere medizinische KI-Systeme den Bedürfnissen und Werten betroffener Communities entsprechen, denen sie dienen sollen. Durch die Einbeziehung der Betroffenen in den Entwicklungsprozess können diese Technologien nicht nur technisch innovativ, sondern auch sozial und ethisch gerecht gestaltet werden. Dies fördert nicht nur die Akzeptanz und Wirksamkeit der Technologien, sondern trägt auch zu einer gerechteren und inklusiveren Gesundheitsversorgung bei.

Partizipation kann somit ein entscheidendes Instrument zur Förderung gesellschaftlicher Teilhabe sein, indem sie das immense Potenzial der Einbeziehung verschiedener Interessengruppen und Betroffenen in die Gestaltung und Steuerung von Gesundheitstechnologien ausschöpft. Solche partizipatorischen Modelle sind unerlässlich, um sicherzustellen, dass digitale Zwillinge in einer Weise entwickelt werden, die den Bedürfnissen, Werten und Bestrebungen der Gemeinschaften, denen sie dienen sollen, gerecht wird.

Fallstudien und theoretische Modelle

Wenn man über minimale Formen der Beteiligung und Teilhabe hinausgeht, wird deutlich, wie partizipative Forschungsmethoden aus den Sozialwissenschaften und dem Design Thinking auf die Entwicklung medizinischer KI angewendet werden können. Hierfür kommen viele unterschiedliche Formen der Beteiligung in Frage, darunter Cooperative Inquiry, Action Research, Co-Creation und andere.

Mit diesem Paradigma von *beyond participation* wird deutlich, dass von Communities geleitete partizipative Ansätze vielversprechend sind, um die ethischen Herausforderungen bei der Entwicklung digitaler Zwillinge anzugehen und abzumildern. Diese Verlagerung hin zu einem integrativeren und gemeinschaftsorientierten Ansatz erhöht die Relevanz und Wirksamkeit digitaler Gesundheitstechnologien und stellt sicher, dass sie einen positiven

Beitrag zur Gleichheit und Zugänglichkeit der Gesundheitsversorgung leisten.

Aufbauend auf diesen theoretischen Erkenntnissen wollen wir zwei konkrete Beispiele dafür untersuchen, wie die partizipative, gemeinschaftsgeleitete Entwicklung der digitalen Zwillingsforschung spezifische ethische Risiken wie die Verletzung der Privatsphäre und strukturelle Ungerechtigkeit wirksam entschärfen könnte:

Beispiel 1: Vermeidung der Verletzung der Privatsphäre durch community-basierte Gestaltung bei der Überwachung der psychischen Gesundheit:
Der Kontext: Digitale Zwillinge bei der Überwachung der psychischen Gesundheit sammeln sensible Daten über den psychischen Zustand, die Aktivitäten und die Interaktionen von Personen. Verletzungen der Privatsphäre sind ein großes Problem, da ein unbefugter Zugriff oder Missbrauch dieser Daten verheerende Auswirkungen auf die Privatsphäre und das allgemeine Wohlbefinden des Einzelnen haben könnte.

Community-basierter Ansatz: Ein partizipatorischer, community-basierter Ansatz bezieht Patient:innen mit psychischen Erkrankungen, Therapeuten und Datenschutzbeauftragte in den Entwurfs- und Entwicklungsprozess der digitalen Zwillinge ein. Durch diese Zusammenarbeit wird sichergestellt, dass Bedarfe zum Schutz der Privatsphäre mit robusten technischen Möglichkeiten des Datenschutzes (*privacy engineering*) verbunden werden können, die auf die spezifischen Bedürfnisse und Anliegen von Patient:innen mit psychischen Erkrankungen zugeschnitten sind.

Konkrete Schritte und Ergebnisse:
1. Planung-Workshops: Durchführung von Workshops mit allen Beteiligten, um Datenschutzbedenken und Präferenzen in Bezug auf die Datenerfassung, -verarbeitung und -weitergabe zu ermitteln.
2. Durchdachter Datenschutz: Integration dieser Grundsätze in die Technologie des digitalen Zwillings von Anfang an, um Datenminimierung, Verschlüsselung und nutzergesteuerte Einstellungen für die gemeinsame Nutzung von Daten zu gewährleisten.
3. Iterative Überprüfung und Feedback-Schleifen: Einrichtung eines kontinuierlichen Feedback-Mechanismus, bei dem die Nutzer:innen Bedenken bezüglich des Datenschutzes melden und Verbesserungen vorschla-

gen können, was zu iterativen Aktualisierungen führt, die den Schutz der Privatsphäre verbessern.

Dieser Ansatz bringt nicht nur die Technologie mit den spezifischen Erwartungen der Nutzer:innen in Bezug auf den Schutz der Privatsphäre in Einklang, sondern fördert auch das Vertrauen in das digitale Zwillingssystem und gewährleistet seine ethische und sozial verantwortliche Nutzung in der psychiatrischen Versorgung.

Beispiel 2: Beseitigung struktureller Ungerechtigkeiten beim Zugang zu Hilfsmitteln für das Diabetesmanagement
Der Kontext: Digitale Zwillinge, die für das Diabetesmanagement entwickelt wurden, versprechen personalisierte Versorgungspläne, die das Diabetesmanagement erheblich verbessern könnten. Es besteht jedoch das Risiko, strukturelle Ungerechtigkeiten zu verschärfen, da marginalisierte Individuen oder Communities möglicherweise nur begrenzten Zugang zu solchen fortschrittlichen Technologien haben.

Community-basierter Ansatz: Einbindung verschiedener Betroffenen-Communities, einschließlich derjenigen mit niedrigem sozioökonomischem Hintergrund, aus ländlichen Gebieten und unterrepräsentierten ethnischen Gruppen, in den Entwicklungsprozess digitaler Zwillinge für das Diabetesmanagement.

Konkrete Schritte und Ergebnisse:
1. Bedarfsanalyse: Gemeinsame Ermittlung von Zugangshindernissen wie Kosten, digitale Konnektivität und kulturelle Relevanz, die diese Gemeinschaften daran hindern könnten, von digitalen Zwillingstechnologien zu profitieren.
2. Lösungen für integratives Design: Entwicklung skalierbarer und kosteneffizienter digitaler Zwillinge, möglicherweise über mobile Plattformen, die für verschiedene Communities zugänglich sind, und Gewährleistung der Anpassungsfähigkeit des Systems an unterschiedliche Gesundheitsinfrastrukturen.
3. Gemeinde-nahes Engagement von Gesundheitshelfer:innen: Schulung von *community health workers* (CHWs), um bei der Umsetzung und laufenden Unterstützung des digitalen Zwillings zu helfen und sicher-

zustellen, dass es effektiv in die bestehenden Gesundheitspraktiken vor Ort integriert wird.

Durch die Einbeziehung dieser Communities in den Design- und Entwicklungsprozess kann das Projekt strukturelle Ungerechtigkeiten adressieren und im besten Fall abmildern und so die gerechte Verteilung der Vorteile der Technologie sicherstellen. Dieser partizipatorische Ansatz verbessert nicht nur die Zugänglichkeit und Relevanz digitaler Zwillingstechnologien für das Diabetesmanagement, sondern trägt auch dazu bei, die gesundheitlichen Ungleichheiten zu verringern in dem auch Gruppen und Individuen in Entwicklungsprozesse einbezogen werden können, die bislang, beispielsweise aufgrund strukturell mitbedingter Faktoren (beispielsweise da sie von Armut betroffen sind und/oder mangelnde Bildung aufweisen), marginalisiert sind.

Diese Beispiele verdeutlichen das große Potenzial partizipativer, community-basierter Ansätze, um ethische Risiken im Zusammenhang mit digitalen Zwillingstechnologien zu mindern und sicherzustellen, dass sie in einer Weise entwickelt und eingesetzt werden, die ethisch vertretbar und gerecht ist und den vielfältigen Bedürfnissen der Communities von Betroffenen entspricht.

2. Auf dem Weg zu einer ethischen und rechtlichen eingebetteten Good Governance

Der rasche Fortschritt und die Integration der digitalen Zwillingstechnologie in der Biomedizin und im Gesundheitswesen machen deutlich, wie wichtig eine umfassende ethische und rechtliche Einbettung und letztlich Kontrolle ist. Diese Governance muss die Patient:innenrechte, die Privatsphäre und den gleichberechtigten Zugang schützen. Daher besteht ein ausgeprägter Bedarf an Rechts- und Regulierungsrahmen, die in der Lage sind, die vielfältigen Herausforderungen zu bewältigen, die durch digitale Zwillinge entstehen. Diese Rahmenbedingungen sollten an die sich entwickelnde Landschaft der digitalen Gesundheitstechnologien anpassbar sein und gleichzeitig die Grundprinzipien der Ethik und Rechtmäßigkeit aufrechterhalten. Da an anderer Stelle im Band (insbesondere im Beitrag von *Gruber* und *Zihlmann*) diese Aspekte aus rechtlicher Perspektive vertieft behandelt

werden, sollen an dieser Stelle nur einige allgemeinere Überlegungen vorgestellt werden.

Rechtliche und regulatorische Rahmenbedingungen auf mehreren Ebenen

Die Entwicklung und Umsetzung digitaler Zwillinge im Gesundheitswesen erfordert rechtliche und regulatorische Rahmenbedingungen, die auf verschiedenen Ebenen – lokal, national und international – greifen. Diese Rahmenbedingungen sollten sich ausdrücklich mit den Patient:innenrechten befassen und sicherstellen, dass die Privatsphäre der Patient:innen geschützt wird und der Zugang zu diesen Technologien gerecht und nichtdiskriminierend ist. Dies erfordert einen dynamischen Regulierungsansatz, der auf den technologischen Fortschritt reagiert, in der Lage ist, Risiken abzumildern und die Interessen aller Beteiligten proaktiv zu wahren.[37]

Die Europäische Union (EU) ist ein Beispiel für proaktive Governance im digitalen Bereich. Sie hat mehrere Verordnungen umgesetzt, die als solide Rechtsgrundlage für die Governance von digitalen Zwillingen im Gesundheitswesen dienen könnten. Die europäische Datenschutz-Grundverordnung (DS-GVO) setzt einen globalen Maßstab für Datenschutz und Privatsphäre und bietet klare Richtlinien für die Erhebung, Verarbeitung und Speicherung personenbezogener Daten.[38] In ähnlicher Weise zielen die Verordnung über digitale Dienstleistungen (Digital Services Act)[39] und die bevorstehende EU KI-Verordnung (EU AI Act)[40] darauf ab, digitale Dienstleistungen bzw. Anwendungen der künstlichen Intelligenz zu regulieren. Diese Verordnungen bieten eine normativ gewichtige und substanzielle rechtliche Grundlage für den ethischen Einsatz und die Steuerung digitaler Zwillingstechnologien, wobei der Schwerpunkt auf Transparenz, Verantwortlichkeit und Verbraucherschutz liegt.

Die globale Landschaft der Governance digitaler Gesundheitstechnologien ist jedoch durch erhebliche rechtliche Diskontinuitäten gekennzeichnet, insbesondere zwischen Rechtsordnungen wie der EU und den Vereinigten Staaten. Die DS-GVO und der Health Insurance Portability and Accountability Act (HIPAA) in den USA sind ein Beispiel für solche Diskrepanzen,

37 Hovenga und Grain 2013; Ienca u.a. 2022; Floridi 2018.
38 Phillips 2018.
39 Söderlund u.a. 2024.
40 Fraser u.a. 2023; Duffourc and Gerke 2023.

insbesondere in Bezug auf Datenschutzstandards und Datenschutzbestimmungen.[41] Diese Unterschiede stellen Akteure im Bereich medizinischer KI vor Herausforderungen bei der Einhaltung von Rechtsvorschriften und behindern die grenzüberschreitende Interoperabilität von Lösungen für das digitale Gesundheitswesen. Die Lösung dieser Probleme ist daher von entscheidender Bedeutung, um die internationale Entwicklung und den Einsatz von digitalen Zwillingen im Gesundheitswesen zu ermöglichen.

V. Zusammenfassung und Empfehlungen

Das Versprechen von Datenzwillingen für eine noch stärker personalisierte Medizin muss mit einem kritischen Bewusstsein für bestehende Ungleichheiten in der Gesundheitsversorgung und das Risiko, dass diese Technologien diese Ungleichheiten verschärfen könnten, ins Verhältnis gesetzt werden. Eine zentrale ethische Herausforderung ist das Konzept des Datenessenzialismus. Im Mittelpunkt steht dabei die Frage, ob die digitalen Darstellungen von Individuen, die aus Datenpunkten von genetischen Informationen bis hin zu Lebensgewohnheiten konstruiert werden, wirklich das facettenreiche Wesen des Menschen erfassen können. Indem Daten als essenzielle und akkurate Repräsentation der menschlichen Gesundheit und Identität in den Vordergrund gestellt werden, besteht die Gefahr, dass die Komplexität individueller Erfahrungen, Bedingungen und sozialer Kontexte zu stark vereinfacht wird. Eine solche Vereinfachung kann zu Gesundheitslösungen führen, die zwar technisch ausgereift sind, aber nicht auf die differenzierten Bedürfnisse des Einzelnen eingehen, was zu Fehldiagnosen, unangemessenen Behandlungen und allgemeinen Missverständnissen zwischen Leistungserbringer:innen und Patient:innen führen kann.

Die Auswirkungen eines solchen Datenessenzialismus gehen über den Bereich der Patientenversorgung hinaus und betreffen auch den Schutz der Privatsphäre und die Auswirkungen auf die Gesellschaft im Allgemeinen. Da digitale Modelle zunehmend Individuen abbilden, verschwimmen die Grenzen zwischen persönlicher Identität und Datendarstellung, was Fragen zu Eigentum, Kontrolle und Zustimmung in Bezug auf persönliche Daten aufwirft. Die Möglichkeit des Missbrauchs oder des unbefugten Zugriffs auf

41 Mulder/Tudorica 2019.

diese Daten verkompliziert die ethische Landschaft weiter und führt zu Risiken, die das Vertrauen in Gesundheitssysteme und -technologien untergraben könnten.

In dieser Hinsicht sind die Autonomie der Patient:innen und die Komplexität der informierten Zustimmung ein weiterer kritischer Bereich für die ethische Analyse. Digitale Zwillinge stellen besondere Herausforderungen für die Autonomie von Patient:innen dar, insbesondere im Hinblick auf die Verwendung persönlicher Gesundheitsdaten. Die Sicherstellung einer echten informierten Zustimmung, die die Patienten über die Nutzung und potenziellen Risiken ihrer Daten vollständig aufklärt, ist essenziell, um ihre Autonomie zu wahren und Vertrauen aufzubauen.

Vulnerabilität ist ein weiteres wichtiges Thema im Kontext digitaler Zwillinge. Besonders gefährdete Gruppen könnten durch den Einsatz dieser Technologien weiter marginalisiert werden, wenn ihre spezifischen Bedürfnisse und Risiken nicht angemessen berücksichtigt werden. Die Berücksichtigung von Vulnerabilität erfordert eine gezielte Anstrengung, um sicherzustellen, dass digitale Zwillinge inklusiv gestaltet werden und den besonderen Anforderungen und Schutzbedürfnissen dieser Gruppen gerecht werden.

Gerechtigkeit im Gesundheitswesen bedeutet, dass der Zugang zu digitalen Zwillingstechnologien fair und gleichberechtigt gestaltet sein muss. Die Beseitigung systemischer Diskriminierung und die Gewährleistung eines gleichberechtigten Zugangs zu digitalen Zwillingen ist unerlässlich, um ihr volles Potenzial auszuschöpfen, ohne benachteiligte Individuen und Bevölkerungsgruppen weiter zu marginalisieren. Dies erfordert eine gründliche ethische Analyse und eine bewusste Verpflichtung zu sozialer Gerechtigkeit und Fairness.

Die Rolle partizipativer Forschung und Entwicklung ist entscheidend, um sicherzustellen, dass digitale Zwillinge in einer Weise entwickelt werden, die den Bedürfnissen, Werten und Bestrebungen der Gemeinschaften, denen sie dienen sollen, gerecht wird. Partizipative Modelle, die die Einbeziehung verschiedener Interessengruppen und Betroffenen fördern, tragen zur ethischen Integrität und Akzeptanz der Technologien bei.

Darüber hinaus sind Modelle einer Good Governance notwendig, um sicherzustellen, dass die Entwicklung und Nutzung digitaler Zwillinge transparent, inklusiv und gerecht erfolgt. Dies beinhaltet die Etablierung von Richtlinien und Rahmenwerken, die den fairen Zugang, den Schutz der Privatsphäre und die Wahrung der Autonomie gewährleisten. Basierend auf

den zusammengefassten Erkenntnissen aus dem vorliegenden Text werden hier vier Schlüsselempfehlungen für den effektiven Umgang mit diesen Herausforderungen gegeben:

1. *Förderung der ethischen und rechtlichen Kompetenzen*

Die Verbesserung der ethischen und rechtlichen Kenntnisse aller an digitalen Zwillingstechnologien beteiligten Akteure ist von entscheidender Bedeutung, um die Komplexität der Mehrebenen-Governance zu bewältigen. Es sollten Bildungsinitiativen und -ressourcen entwickelt werden, um das Verständnis für die ethischen Grundsätze und rechtlichen Bestimmungen für digitale Gesundheitstechnologien zu verbessern. Dazu gehört auch die Sensibilisierung für den möglichen Missbrauch der digitalen Phänotypisierung und die Bedeutung des Datenschutzes und der Privatsphäre. Indem sichergestellt wird, dass Entwickler:innen, Gesundheitsdienstleister und Patient:innen gut über die ethischen und rechtlichen Überlegungen zu digitalen Zwillingen informiert sind, kann die Gesellschaft zu einer ethischeren und gesetzeskonformeren Landschaft der Gesundheitstechnologie beitragen.

2. *Integration partizipativer Modelle in die Technologieentwicklung und -verwaltung*

Um sicherzustellen, dass die Technologien des digitalen Zwillings auf ethisch vertretbare und sozial verantwortliche Weise entwickelt und implementiert werden, sind partizipative Modelle, die ein breites Spektrum von Interessengruppen einbeziehen – darunter Patient:innen, Gesundheitsdienstleister, Techniker:innen und politische Entscheidungsträger:innen – von wesentlicher Bedeutung. Dieser community-basierte Ansatz für Forschung und Entwicklung kann dazu beitragen, spezifische ethische Risiken wie die Verletzung der Privatsphäre und strukturelle Ungerechtigkeit zu mindern, indem verschiedene Perspektiven und Bedürfnisse von Anfang an berücksichtigt werden. Darüber hinaus können partizipative Governance-Modelle die Relevanz, Inklusivität und Effektivität rechtlicher und regulatorischer Rahmenbedingungen verbessern, indem sie sicherstellen,

dass die gelebten Erfahrungen und das Fachwissen aller Beteiligten in diese einfließen.

3. *Entwicklung eines mehrstufigen Regulierungs- und Governanceansatzes mit Schwerpunkt auf der internationalen Zusammenarbeit*

Angesichts des länderübergreifenden Charakters digitaler Gesundheitstechnologien besteht ein dringender Bedarf an mehrstufigen Regulierungsrahmen, die nationale Erwägungen berücksichtigen und die internationale Zusammenarbeit und Standardisierung erleichtern. Die proaktive Haltung der Europäischen Union mit der DS-GVO, dem Digital Services Act und der kommenden KI-Verordnung bietet eine solide Grundlage für eine solche Governance. Diese Rahmenwerke sollten als Modelle für die Schaffung harmonisierter Standards dienen, die Patientenrechte, Datenschutz und gerechten Zugang gewährleisten und gleichzeitig ein innovatives Umfeld fördern. Die internationale Zusammenarbeit, etwa durch die Einrichtung eines globalen Regulierungsgremiums für digitale Gesundheitstechnologien oder eines Abkommens, könnte die Angleichung unterschiedlicher Rechtssysteme wie der DS-GVO in der EU und des HIPAA in den USA erleichtern und so die Interoperabilität und die Einhaltung von Vorschriften in verschiedenen Ländern gewährleisten.

4. *Dynamische und anpassungsfähige Regulierung und Governance*

Der rasche technologische Fortschritt im Bereich der digitalen Gesundheit erfordert dynamische und anpassungsfähige Regulierungsmechanismen, die auf neue ethische Herausforderungen und Innovationen reagieren können. Die Einrichtung spezieller Aufsichtsgremien oder die Implementierung regulatorischer Testumgebungen (*regulatory sandboxes*) könnte die Erprobung und Verfeinerung von Governance-Ansätzen in realen Umgebungen ermöglichen. Diese Mechanismen sollten flexibel sein und eine rasche Aktualisierung der Vorschriften als Reaktion auf neue Entwicklungen ermöglichen, ohne dabei den Schutz der Patient:innenrechte und der Privatsphäre zu vernachlässigen.

Diese Empfehlungen bieten einen strategischen Fahrplan für die Bewältigung der ethischen und rechtlichen Komplexität, die mit digitalen Zwillingstechnologien im Gesundheitswesen verbunden ist. Durch die Förderung der internationalen Zusammenarbeit, die Integration partizipativer Modelle, die Priorisierung adaptiver Governance und die Verbesserung der Kompetenz können die Beteiligten zusammenarbeiten, um sicherzustellen, dass diese innovativen Technologien einen positiven Beitrag zur Zukunft der Medizin leisten und dabei die Autonomie, die Vulnerabilität und die Gerechtigkeit der Patient:innen berücksichtigen.

Literatur

Albashiti, Fady/ Thasler, Reinhard/Wendt, Thomas/Bathelt, Franziska/Reinecke, Ines/ Schreiweis, Björn (2024): Die Datenintegrationszentren – Von der Konzeption in der Medizininformatik-Initiative zur lokalen Umsetzung in einem Netzwerk Universitätsmedizin, in: *Bundesgesundheitsblatt – Gesundheitsforschung – Gesundheitsschutz*, 25.4.2024.

Al-Dalati, Issam (2023): Chapter 10 – Digital Twins and Cybersecurity in Healthcare Systems, in: El Saddik, Abdulmotaleb (Hg.): *Digital Twin for Healthcare*, Cambridge, S. 195–221.

Barricelli, Barbara R./Fogli, Daniela (2024): Digital Twins in Human-Computer Interaction: A Systematic Review, in: *International Journal of Human–Computer Interaction* 40, Heft 2, S. 79–97.

Beauchamp, Tom L./Childress, James F. (2001): *Principles of Biomedical Ethics*, Oxford.

Bester, Johan/Cole, Cristie M./Kodish, Eric (2016): The Limits of Informed Consent for an Overwhelmed Patient: Clinicians' Role in Protecting Patients and Preventing Overwhelm, in: *AMA Journal of Ethics* 18, Heft 9, S. 869–886.

Birk, Rasmus H./Samuel, Gabrielle (2022): Digital Phenotyping for Mental Health: Reviewing the Challenges of Using Data to Monitor and Predict Mental Health Problems, in: *Current Psychiatry Reports* 24, Heft 10, S. 523–528.

Björling, Elin A./Rose, Emma (2019): Participatory Research Principles in Human-Centered Design: Engaging Teens in the Co-Design of a Social Robot, in: *Multimodal Technologies and Interaction* 3, Heft 1, S. 8.

Borrmann, Vera/Versalovic, Erika/Brown, Timothy/Scholl, Helena/Klein, Eran/Goering, Sara/Müller, Oliver/Kellmeyer, Philipp (2024): Situated and Ethically Sensitive Interviewing: Critical Phenomenology in the Context of Neurotechnology, in: Heinrichs, Jan-Hendrik/ Beck, Birgit/ Friedrich, Orsolya (Hg.) *Neuro-ProsthEthics: Ethical Implications of Applied Situated Cognition*, Berlin/Heidelberg, S. 167–93.

Brown, Kate/Ecclestone, Kathryn/Emmel, Nick (2017): The Many Faces of Vulnerability, in: *Social Policy and Society* 16, Heft 3, S. 497–510.

Budin-Ljøsne, Isabelle/Teare, Harriet J. A./Kaye, Jane/Beck, Stephan/ Bentzen, Heidi B./ Caenazzo, Luciana/Collett, Clive u.a. (2017): Dynamic Consent: A Potential Solution to Some of the Challenges of Modern Biomedical Research, in: *BMC Medical Ethics* 18, Heft 1, S. 4.

Chevalier, Jacques M./ Buckles, Daniel J. (2019): *Participatory Action Research: Theory and Methods for Engaged Inquiry*, London.

Coorey, Genevieve/Figtree, Gemma A./Fletcher, David F./Snelson, Victoria J./Vernon,Stephen Thomas/Winlaw, David/Grieve,Stuart M. u.a. (2022): The Health Digital Twin to Tackle Cardiovascular Disease—a Review of an Emerging Interdisciplinary Field, in: *Npj Digital Medicine* 5, Heft 1, S. 1–12.

De Maeyer, Christel/Markopoulos, Panos (2021): Experts' View on the Future Outlook on the Materialization, Expectations and Implementation of Digital Twins in Healthcare, in: *Interacting with Computers* 33, Heft 4, S. 380–394.

Dlima, Schenelle Dayna/Shevade, Santosh/ Menezes, Sonia Rebecca/Ganju, Aakash (2022): Digital Phenotyping in Health Using Machine Learning Approaches: Scoping Review, in: *JMIR Bioinformatics and Biotechnology* 3, Heft 1, e39618.

Donnelly, Mary/McDonagh, Maeve (2019): Health Research, Consent and the GDPR Exemption, in: *European Journal of Health Law* 26, Heft 2, S. 97–119.

DS-GVO [= Europäische Kommission] (2016): *Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)*, Amtsblatt L 119/1, https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679 [21.5.2024].

Duffourc, Mindy Nunez/Gerke, Sara (2023): The Proposed EU Directives for AI Liability Leave Worrying Gaps Likely to Impact Medical AI, in: *Npj Digital Medicine* 6, Heft 1, S. 1–6.

Fagherazzi, Guy (2020): Deep Digital Phenotyping and Digital Twins for Precision Health: Time to Dig Deeper, in: *Journal of Medical Internet Research* 22, Heft 3, e16770.

Floridi, Luciano (2018): Soft Ethics and the Governance of the Digital, in: *Philosophy & Technology* 31, Heft 1, S. 1–8.

Fraser, Alan G./Biasin, Elisabetta/Bijnens, Bart/Bruining, Nico/Caiani, Enrico G./Cobbaert, Koen/Davies, Rhodri H. u.a. (2023): Artificial Intelligence in Medical Device Software and High-Risk Medical Devices – a Review of Definitions, Expert Recommendations and Regulatory Initiatives, in: *Expert Review of Medical Devices* 20, Heft 6, S. 467–491.

Fricker, Miranda (2007): *Epistemic Injustice: Power and the Ethics of Knowing*, Oxford.

Fröhlich, Wiebke/ Spiecker, Indra (2022): Die breite Einwilligung (Broad Consent) in die Datenverarbeitung zu medizinischen Forschungszwecken – der aktuelle Irrweg der MII, in: *GesundheitsRecht* 21, Heft 6, S. 346–353.

Ganguli-Mitra, Agomoni/Biller-Andorno, Nikola (2011): Vulnerability in Healthcare and Research Ethics, in: *The SAGE Handbook of Health Care Ethics*, erste Auflage, Los Angeles/London, S. 239–250.

Goering, Sara/Klein, Eran/Dougherty, Darin D./Widge, Alik S. (2017): Staying in the Loop: Relational Agency and Identity in Next-Generation DBS for Psychiatry, in: *AJOB Neuroscience* 8, Heft 2, S. 59–70.

Hallinan, Dara (2020): Broad Consent under the GDPR: An Optimistic Perspective on a Bright Future, in: *Life Sciences, Society and Policy* 16, Heft 1, S. 1.

Hassan, Muneeb Ul/Rehmani, Mubashir Husain/Chen, Jinjun (2020): Differential Privacy Techniques for Cyber Physical Systems: A Survey, in: *IEEE Communications Surveys Tutorials* 22, Heft 1, S. 746–789.

Hernandez-Boussard, Tina/Macklin, Paul/Greenspan, Emily J./Gryshuk, Amy L./Stahlberg, Eric/Syeda-Mahmood, Tanveer/Shmulevich, Ilya (2021): Digital Twins for Predictive Oncology Will Be a Paradigm Shift for Precision Cancer Care, in: *Nature Medicine* 27, Heft 12, S. 2065–2066.

Herzog, Lisa/Kellmeyer, Philipp/Wild, Verina (2022): Digital Behavioral Technology, Vulnerability and Justice: Towards an Integrated Approach, in: *Review of Social Economy* 80, Heft 1, S. 7–28.

Hofmann, Sebastian (2022): Forschungsklausel statt Broad Consent: Sekundärnutzung von Patientendaten ohne Einwilligung, dafür mit Opt-out, in: *Datenschutz und Datensicherheit – DuD* 46, Heft 12, S. 756–61.

Hovenga, Evelyn J. S./Grain, H. (2013): *Health Information Governance in a Digital Environment*, Amsterdam.

Ienca, Marcello/Fins, Joseph J./Jox, Ralf J./Jotterand, Fabrice/Voeneky, Silja/Andorno, Roberto/ Ball, Tonio u.a. (2022): Towards a Governance Framework for Brain Data, in: *Neuroethics* 15, Heft 2, S. 20.

Insel, Thomas R. (2017): Digital Phenotyping: Technology for a New Science of Behavior, in: *JAMA* 318, Heft 13, S. 1215–1216.

Jørgensen, Cecilie Solberg/Shukla, Ankur/Katt, Basel (2024): Digital Twins in Healthcare: Security, Privacy, Trust and Safety Challenges, in: Katsikas,Sokratis/Abie, Habtamu/Ranise, Silvio/Verderame, Luca/ Cambiaso, Enrico/Ugarelli, Rita/Praça, Isabel u.a. (Hg.): *Computer Security. ESORICS 2023 International Workshops*, Basel, S. 140–53.

Kellmeyer, Philipp (2024): Beyond Participation: Towards a Community-Led Approach to Value Alignment of AI in Medicine, in: *Developments in Neuroethics and Bioethics* 7, S. 249–269.

Kellmeyer, Philipp (2020): Digital Vulnerability: A New Challenge in the Age of Super-Convergent Technologies, in: *Bioethica Forum* 12, Heft ½, S. 60–62.

Lucas, Jaisalmer de Frutos/Haugo, Hans Torvald (2024): Moving Forward with the European Health Data Space: The Need to Restore Trust in European Health Systems, in: *The Lancet Regional Health – Europe* 40, 100906.

Luh, Frank/Yen, Yun (2020): Cybersecurity in Science and Medicine: Threats and Challenges, in: *Trends in Biotechnology* 38, Heft 8, S. 825–28.

Mackenzie, Catriona/Rogers, Wendy/Dodds, Susan (2013): *Vulnerability: New Essays in Ethics and Feminist Philosophy*, Oxford.

Marmot, Michael/Wilkinson, Richard (2005): *Social Determinants of Health*, Oxford.

Mascalzoni, Deborah/Melotti, Roberto/Pattaro, Cristian/Pramstaller, Peter P./Gögele, Martin/De Grandi, Alessandro/Biasiotto, Roberta (2022): Ten Years of Dynamic Consent in the CHRIS Study: Informed Consent as a Dynamic Process. *European Journal of Human Genetics* 30, Heft 12, S. 1391–97.

Milne-Ives, Madison/Fraser, Lorna K./Khan, Asiya/Walker, David/van Velthoven, Michelle H./May, Jon/Wolfe, Ingrid/Harding, Tracey/Meinert, Edward (2022): Life Course Digital Twins–Intelligent Monitoring for Early and Continuous Intervention and Prevention (LifeTIME): Proposal for a Retrospective Cohort Study, in: *JMIR Research Protocols* 11, Heft 5, e35738.

Molnár-Gábor, Fruzsina/Beauvais, Michael J. S./Bernier, Alexander/Jimenez, Maria P. N./Recuero, Mikel/Knoppers, Bartha M. (2022): Bridging the European Data Sharing Divide in Genomic Science, in: *Journal of Medical Internet Research* 24, Heft 10, e37236.

Mulder, T./Tudorica, M. (2019): Privacy Policies, Cross-Border Health Data and the GDPR, in: *Information & Communications Technology Law* 28, Heft 3, S. 261–74.

Nagaraj, Divya/Khandelwal, Priya/Steyaert, Sandra/ Gevaert, Olivier (2023): Augmenting Digital Twins with Federated Learning in Medicine, in: *The Lancet Digital Health* 5, Heft 5, S. e251–e253.

O'Neill, Onora (2009): Some Limits of Informed Consent, in: Levine, Martin L. (Hg.): *The Elderly*, New York, S. 103–106.

Phillips, Mark (2018): International Data-Sharing Norms: From the OECD to the General Data Protection Regulation (GDPR), in: *Human Genetics* 137, Heft 8, S. 575–582.

Ruckenstein, Minna/Schüll, Natasha D. (2018): The Datafication of Health, in: *Annual Review of Anthropology* 46, S. 261–78.

Sager, Sebastian (2023): Digital Twins in Oncology, in: *Journal of Cancer Research and Clinical Oncology* 149, Heft 9, S. 5475–77.

Schepers, Josef/Fleck, Julia/Schaaf, Jannik (2022): Die Medizininformatik-Initiative und Seltene Erkrankungen: Routinedaten der nächsten Generation für Diagnose, Therapiewahl und Forschung, in: *Bundesgesundheitsblatt – Gesundheitsforschung – Gesundheitsschutz* 65, Heft 11, S. 1151–58.

Schneider, Barbara (2010): *Hearing (Our) Voices: Participatory Research in Mental Health*, Toronto.

Shamanna, Paramesh/Dharmalingam, Mala/Sahay, Rakesh/Mohammed, Jahangir/Mohamed, Maluk/Poon, Terrence/Kleinman, Nathan/Thajudeen, Mohamed (2021): Retrospective Study of Glycemic Variability, BMI, and Blood Pressure in Diabetes Patients in the Digital Twin Precision Treatment Program, in: *Scientific Reports* 11, Heft 1, 14892.

Shamanna, Paramesh/ Saboo, Banshi/Damodharan, Suresh/ Mohammed, Jahangir/Mohamed, Maluk/Poon, Terrence/Kleinman, Nathan/Thajudeen, Mohamed (2020): Reducing HbA1c in Type 2 Diabetes Using Digital Twin Technology-Enabled Precision Nutrition: A Retrospective Analysis, in: *Diabetes Therapy* 11, Heft 11, S. 2703–2714.

Söderlund, Kasia/Engström, Emma/Haresamudram, Kashyap/Larsson, Stefan/Strimling, Pontus (2024): Regulating High-Reach AI: On Transparency Directions in the Digital Services Act, in: *Internet Policy Review* 13, Heft 1.

Vanberg, Aysem D. (2021): Informational Privacy Post GDPR – End of the Road or the Start of a Long Journey?, in: *The International Journal of Human Rights* 25, Heft 1, S. 52–78.

Venkatesh, Kaushik P./Brito, Gabriel/Boulos, Maged N. K. (2024): Health Digital Twins in Life Science and Health Care Innovation, in: *Annual Review of Pharmacology and Toxicology* 64, Heft 1, S. 159–170.

Viola, Francesco/Del Corso, Giulio/De Paulis, Ruggero/Verzicco, Roberto (2023): GPU Accelerated Digital Twins of the Human Heart Open New Routes for Cardiovascular Research, in: *Scientific Reports* 13, Heft 1, 8230.

WHO [= Weltgesundheitsorganisation] (2024): *Vulnerability and Vulnerable Populations*, https://wkc.who.int/our-work/health-emergencies/knowledge-hub/community-disaster-risk-management/vulnerability-and-vulnerable-populations [30.5.24].

Wiertz, Svenja/Boldt, Joachim (2022): Evaluating Models of Consent in Changing Health Research Environments, in: *Medicine, Health Care and Philosophy* 25, Heft 2, S. 269–280.

UN [=Vereinte Nationen] (2024): *Vulnerability*, https://www.undrr.org/terminology/vulnerability [30.5.24].

Yazijy, Suhail/Schölly, Reto/Kellmeyer, Philipp (2022): Towards a Toolbox for Privacy-Preserving Computation on Health Data, in: *Studies in Health Technology and Informatics* 290, S. 234–237.

Young, Iris Marion (2013): *Responsibility for Justice*, Oxford/New York.

Zalake, Mohan (2023): Doctors' Perceptions of Using Their Digital Twins in Patient Care, in: *Scientific Reports* 13, Heft 1, 21693.

Zenker, Sven/Strech, Daniel/Jahns, Roland/Müller, Gabriele/Prasser, Fabian/Schickhardt, Christoph/Schmidt, Georg/Semler, Sebastian C./Winkler, Eva/ Drepper, Johannes (2024): National standardisierter Broad Consent in der Praxis: erste Erfahrungen, aktuelle Entwicklungen und kritische Betrachtungen, in: *Bundesgesundheitsblatt – Gesundheitsforschung – Gesundheitsschutz*, 19.4.2024.

Zugangsverantwortung: Die Zukunft und Notwendigkeit von informationeller Selbstbestimmung

Selbst- und Fremdbestimmung im Datendickicht

Benjamin Müller

I. Ausgangssituation

Wenn heute von Daten gesprochen wird, sind in der Regel digitale Daten gemeint. Sie fallen aufgrund der Protokollierung automatisch bei jedem Betrieb von computerbasierten Systemen an. Insofern produziert heute nahezu jedes technische Gerät während der Nutzung permanent Daten. Sobald es mit anderen Netzwerken oder dem Internet verbunden wird, entstehen wiederum Protokolldaten über diese Verbindung und eventuelle Transaktionsdaten. Handelt es sich um Geräte des persönlichen Gebrauchs wie Tablets oder Smartphones erhalten die Daten schließlich einen Personenbezug. Die »smarten« Geräte des Alltags sammeln permanent Daten ihrer eigenen Nutzung und Vernetzung, die wiederum von den Herstellern und Anbietern gesammelt werden, denn solche auf den ersten Blick unscheinbaren Daten bilden inzwischen eines der Kerngeschäfte der globalen Wirtschaft. Die Art und auch Qualität von Daten kann dabei sehr unterschiedlich ausfallen. Teils bedarf es erst einer aufwendigen Aufbereitung, um sie für weitere Zwecke nutzen zu können. Das einzelne Datum ist tendenziell wertlos, erst aus einer gewissen Menge lassen sich verwertbare Informationen gewinnen. Da sie verlustfrei kopiert werden können, ist ein Zugang meist ausreichend zur Datenteilung. Wer alles wann und wie mit mir über meine Geräte Daten produziert, wer sie wo speichert, kopiert und verwaltet, entzieht sich häufig meiner Kontrolle und meinem Wissen. Ich kann all die Datenspuren, die ich hinterlasse, weder vollständig überprüfen, noch bekomme ich in den meisten Fällen überhaupt etwas von ihnen mit. Sogar die eindeutige Zuschreibung, wem die Daten gehören, also das Sprachspiel des Eigentums, ist wegen ihrer komplexen Entstehungsgeschichte schon problematisch geworden

und es darum auch meistens schwierig, noch von »meinen« Daten zu sprechen.

Zumeist suchen wir selbst den Zugang zu Unternehmen und Plattformen, weil diese uns vielversprechende Dienste und Angebote bereitstellen, die aus dem alltäglichen Leben kaum noch wegzudenken sind. Im Gegenzug erheben sie während unserer Nutzung umfangreiche Daten über dieselbe. Es wird zum Beispiel festgehalten, wie lange wir einkaufen, bei welchen Produkten wir am meisten Zeit verbracht haben und vieles mehr. Durch die Analyse dieser Daten lässt sich entweder direkt gezielte Werbung zuschalten oder die Ergebnisse der Datenanalyse an dritte verkaufen. Diese Taktik ist zunächst keine explizite Neuheit des Digitalen, sondern wurde auch schon zuvor in physischen Kaufläden umgesetzt. Von dem generellen Marktaufbau, über die Platzierung von den teuren Produkten in bequemer Sicht- und Greifhöhe bis zu der sogenannten Quengelzone vor der Kasse beruht alles ebenfalls auf vorangegangen Konsumstudien. Neu scheint hier zunächst nur der Umfang zu sein, in dem nun digitale Daten gesammelt und analysiert werden. Man könnte daher meinen, es läge in der Verantwortung der Kunden, ihren Besuch zu regeln und sich nicht zu sehr kontrollieren zu lassen. Sie bestimmen durch ihren Besuch über den Datenzugang der Unternehmen, das heißt ihre Nutzung der Angebote, vom Kaufladen über die Suchmaschine bis zu sozialen Medien. Das ist zwar nicht vollkommen falsch, wird aber den heutigen Gegebenheiten längst nicht mehr gerecht. Denn durch die ungeheure Masse an Daten wurde auch eine neue Qualität der Auswertung erreicht. Wer noch immer meint, man könne mit ein paar scheinbar zusammenhanglosen Daten nicht viel anfangen, unterschätzt maßlos die heutigen Verarbeitungsmöglichkeiten. Führt man gesammelte Daten zur maschinellen Auswertung in Einzel- oder auch Gruppenprofile zusammen, lassen sich daraus Vorlieben, Neigungen, Leidenschaften, Interessen, Freunde, Bekanntenkreise, sogar Konfessionen, Gesundheitszustände und andere sensible Informationen ableiten. Dabei gilt: Je mehr Daten, desto bessere, das heißt wahrscheinlichere Ergebnisse. Die gigantische Datenmasse führt mittlerweile zu erschreckend guten Statistiken über den aktuellen Status und sogar Voraussagen über künftiges Verhalten. Ganze Lebensabschnitte ließen sich rekonstruieren anhand von Daten über Standorte, Käufe, Bezahlvorgänge, Suchanfragen, Webseitenbesuche, genutzte Anwendungen und vielem mehr. Die Nutzung von Onlineangeboten macht inzwischen einen beträchtlichen Teil des alltäglichen Lebens aus und

dabei fallen fast überall Daten an, die mittlerweile eifrig gesammelt und gehandelt werden.

Wie steht es um die Freiheit unter diesen Bedingungen global vernetzter Technologien? Die persönliche Freiheit wird heute meist als Selbstbestimmung adressiert, die jedoch auch gesellschaftliche Effekte aufweist. Ist diese Selbstbestimmung nun gefährdet? Immerhin sind versuchte Manipulationen im Digitalen längst nicht mehr so offensichtlich durchschaubar, wie es vielleicht noch im Supermarkt der Fall ist, weswegen es auch immer schwieriger wird, die Verantwortung konkret einzelnen Akteuren zuzuschreiben. Die schiere Menge und Komplexität der verschiedenen Daten und ihrer Erhebung und damit potentiellen Risiken überfordern und es scheint unmöglich, die Lage noch vollständig überblicken zu wollen. Bräuchte man aber überhaupt so einen Überblick? Muss man über alle technischen Details aufgeklärt sein, um sich in der heutigen Welt noch selbstbestimmt zu behaupten?

Zu diesen akuten Problemen gesellen sich darüber hinaus noch grundlegende Schwierigkeiten bei Freiheitsfragen, die sich als Dialektik bezeichnen lassen. Diese wiederholen sich im digitalen Bereich und können an Datenzugängen veranschaulicht werden.

Zunächst skizziere ich allgemein die komplexe Problemlage der Selbstbestimmung im demokratischen Kontext, um sie anschließend in Hinblick auf ihre Dialektik weiter zuzuspitzen und schließlich zwei der üblichen Lösungsansätze gegen Manipulation in den Blick zu nehmen. Datenschutz und Aufklärung erweisen sich selbst als problematisch, weil sie derselben dialektischen Spannung ausgesetzt sind und die Gefahr bergen, vom Hilfreichen ins Schädliche umzuschlagen. Wie üblich sieht sich die Freiheit sowohl mit zeitlich aktuellen als auch systematischen Herausforderungen konfrontiert, die sich im Datendickicht miteinander verflechten.

II. Selbstbestimmung in der Demokratie und im Digitalen

Anfang der 80er Jahre führte eine geplante Volkszählung in Deutschland zu einer generellen Datenschutzdiskussion und gipfelte in einem Urteil des Bundesverfassungsgerichts, das ein Grundrecht auf »informationelle Selbstbestimmung« etablierte und deren unabdingbare Bedeutung für die Demokratie betonte.

»Individuelle Selbstbestimmung setzt aber – auch unter den Bedingungen moderner Informationsverarbeitungstechnologien – voraus, daß dem Einzelnen Entscheidungsfreiheit über vorzunehmende oder zu unterlassende Handlungen einschließlich der Möglichkeit gegeben ist, sich auch entsprechend dieser Entscheidung tatsächlich zu verhalten. Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß.«[1]

Inzwischen ist es tatsächlich so, dass »Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß.« Heute ist es allerdings weniger der Staat, als vielmehr große Unternehmen und vermittelt über deren Plattformen sogar die Öffentlichkeit, welche diese Risiken für Einzelpersonen darstellen. Ist deren Freiheit dadurch wirklich »wesentlich gehemmt«, wie befürchtet? Sofern informationelle Selbstbestimmung als Grundrecht gilt, steht die Politik auch in der Pflicht, dieses Grundrecht zu verteidigen. Eine Aufgabe, der sie aktuell aber in dem hier geforderten Umfang kaum noch gerecht werden könnte. Dass wir uns ständig an der Welt abarbeiten müssen, Bedingungen ertragen, Widerständen und Gefahren begegnen ist zunächst nichts Neues. Allerdings sehen wir uns in einer umfassend digitalisierten Welt mit einer neuen Qualität von Risiken konfrontiert: unbemerkte, kontaktlose, weil digitale Überwachung sowie Manipulationsmöglichkeiten subtilster Art, die auf gesammelten Daten beruhen. Wenn hierdurch die persönliche Freiheit eingeschränkt würde, hätte das auch unmittelbare Auswirkungen auf die Demokratie. Der Begriff *Demokratie* ist gebildet aus den altgriechischen Wörtern *demos* (Volk) und *kratein* (herrschen), also das Volk herrscht. Eine Demokratie beruht demnach vom Prinzip her auf einer freien Bürgerschaft, die grundsätzlich in der Lage ist, selbst über ihre Belange zu bestimmen. Freie Selbstbestimmung ist demnach eine demokratische Voraussetzung.[2] Im Volkszählungsurteil heißt es hierzu, dass »Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten

1 BVerfG, 15. Dezember 1983 (»Volkszählungsurteil«), 146, S. 33.
2 Ausführlich hierzu Winter 2017.

freiheitlichen demokratischen Gemeinwesens«[3] darstellt. In dem Fall stünde vor dem Hintergrund der umfassenden Digitalisierung nicht nur die Selbstbestimmung auf dem Prüfstand, sondern auch dieses Ideal einer Demokratie, woran sich inzwischen das ganze europäische Selbstverständnis orientiert. Demokratie steht heute in Europa im Allgemeinen als Chiffre für die Losungen der Französischen Revolution: Freiheit, Gleichheit und Solidarität. Dazu treten die Würde des Menschen und die Menschenrechte. All diese Ideen bilden in ihrem Zusammenspiel den modernen demokratischen Horizont. Demokratie meint insofern nicht mehr bloß eine Regierungs-, sondern gleich eine ganze Lebensform. In einem demokratischen Land zu leben heißt für uns heute, dass diese Ideen hier als Leitbilder fungieren, Geltung beanspruchen können sowie die Überzeugung, dass sie ausnahmslos allen Menschen zustehen und diese sogar ein Recht darauf haben. Dieses Recht ist in der Charta der Grundrechte der Europäischen Union und im deutschen Grundgesetz fest verankert.

Das erwähnte Grundrecht auf informationelle Selbstbestimmung ist dem Ansinnen nach eine Ausbuchstabierung, die den digitalen Entwicklungen Rechnung tragen soll. »Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.«[4] Zur Zeit seiner Etablierung ging es dabei vorrangig um konkrete Personendaten wie Name, Adresse, Staatsangehörigkeit und dergleichen. Heute spricht man an Stelle von »persönlichen« Daten weitläufiger von »personenbezogenen« Daten. Dabei ist jedoch keineswegs klar, wie weitläufig dieser Bezug zu verstehen ist und damit ebenso wenig, welche Informationen darunter fallen und dieser informationellen Selbstbestimmung unterliegen sollen oder überhaupt noch können. Denn selbst wenn bestimmte Informationen nicht eigens gesammelt werden, lassen sie sich womöglich über gesammelte Daten erschließen. Man müsste also tendenziell nicht nur informationell, sondern auch datafiziell selbstbestimmt sein. Das führte zu der Debatte über *Datensouveränität*.[5] In beiden Fällen bleibt jedoch gleichermaßen unklar, wie ich überhaupt über mich betreffende Informationen und Daten konkret bestimmen können oder souverän sein soll? Zumal wenn ich in den meisten Fällen erst gar nichts von deren Erhebung und Sammlung mitbekomme.

3 BVerfG, 15. Dezember 1983, 146, S. 33.
4 Ebd., 147, S. 33 f.
5 Vgl. Augsberg/Gehring 2022.

Die im Fokus stehenden Kernbegriffe Souveränität und Selbstbestimmung bleiben erstaunlich vage und deutungsoffen. In der Alltagsrede, die sich gerne auch in Politik und Recht verirrt, vermischen sich vor allem die vielfältigen Bedeutungen von »Bestimmen«,[6] sodass letztlich unklar bleibt, was genau mit »Selbstbestimmung« angesprochen sein soll und welche Möglichkeiten sie konkret bietet. Um die Souveränität ist es kaum besser bestellt. Nicht umsonst streitet die Philosophie seit Jahrhunderten um ein adäquates Verständnis dieser Leitideen. Mögliche Deutungen reichen vom bloßen Beeinflussen über das Entscheiden bis hin zum Beherrschen. Dabei ist nicht nur die Frage, wie weitreichend Selbstbestimmung sein *kann*, sondern anschließend auch, wie weitreichend sie sein *sollte*.

Ob Selbstbestimmung oder Souveränität, beide Varianten suggerieren gerne eine Kontrolle über Daten und Informationen, die in den wenigsten Fällen vorhanden ist. Und diese Kontrollvorstellung bürdet wiederum den Einzelnen eine Verantwortung auf, die unter den vorherrschenden Bedingungen kaum noch angemessen zu vertreten ist. Vollständig souverän und selbstbestimmt wäre ich allenfalls noch durch die völlige Abschaltung meiner technischen Geräte. Immerhin gibt es vom generellen Nutzungsverhalten bis zu spezifischen Einstellungsmöglichkeiten noch weitere Spielräume. Weder bin ich vollständig selbst bestimmt, noch unterliege ich durchgängig einer äußeren Fremdbestimmung. Im gegenwärtigen Datendickicht befinden wir uns wohl stets in der Schwebe.

Die für die Demokratie so bedeutungsvolle Selbstbestimmung ist also in zweierlei Hinsicht prekär: einerseits wird sie durch neueste Manipulationsmöglichkeiten gefährdet, andererseits scheint sie selbst unverstanden und noch nicht begriffen.

Vielfältigkeit und Uneinigkeit beruhen hierbei jedoch nicht nur auf mangelnden Klärungsversuchen, sondern liegen wenigstens zum Teil bereits in der Sache selbst: der Freiheit. Souveränität und Selbstbestimmung sind Formen der Freiheit und diese wiederum weist eine eigene Dialektik auf. Freiheit bewegt sich stets zwischen Unbestimmtheit und Bestimmtheit, ist immer zugleich Freiheit und Notwendigkeit. Beide Momente gehören wesentlich zur Natur der Sache dazu, können aber je nach Kontext unterschiedlich stark gewichtet sein und darüber hinaus binnen kürzester Zeit in ihr Gegenteil umschlagen. Historisch prägnant zeigte sich dies etwa, als die Französische Revolution unmittelbar in die Schreckensherrschaft

6 Vgl. hierzu Gamm 2011.

von Robespierre mündete, die jener sogar noch als Ausdruck von Tugend und Gerechtigkeit verteidigte. Hegel argumentiert, dass beides, also sowohl Revolution als auch Terror, bereits systematisch in der Aufklärung angelegt sind und sogar notwendige Entwicklungsstufen des Geistes darstellen.[7] Diese insbesondere von Adorno und Horkheimer weiter untersuchte »Dialektik der Aufklärung«[8] lässt sich nun auch an der Digitalisierung beobachten. Im Folgenden versuche ich, diese inhärente Ambivalenz speziell an Datenzugängen aufzuzeigen und ihrer Problematik bei Datenschutz und Aufklärung über technische Zusammenhänge nachzuspüren.

III. Die Dialektik der Daten und ihrer Zugänge

Der anfängliche Enthusiasmus über die neuen Vernetzungstechnologien als freimachender Erfindung ist mittlerweile abgeflacht und vielmehr erkannt worden, dass dieselbe neben Möglichkeiten des freien Austausches zugleich effektivste Maßnahmen der Überwachung und Manipulation bietet. Digitalisierung und Datafizierung können die demokratischen Ideen gleichermaßen fördern und herausfordern. Daten spielen dabei eine herausragende und zwiespältige Rolle, da sie beides sowie die zugrundeliegenden Technologien überhaupt erst ermöglichen. Unternehmen gewähren Zugang zu ihren Angeboten über eine bestimmte Schnittstelle, die sie wiederum mit den Daten der Nutzenden versorgt und große Datensammlungen ermöglicht. Prinzipiell kann man sich zwar für oder gegen die Nutzung unter solchen Bedingungen entscheiden, einige Unternehmen haben inzwischen aber derartige Monopolstellungen aufgebaut, dass ihre Nutzung nicht immer freiwillig geschieht. Gewisse Berufssparten müssen bestimmte Plattformen nutzen, sofern sie nicht in der Lage sind einen immensen Wettbewerbsnachteil in Kauf zu nehmen. Im sozialen Bereich führt der sogenannte »Gruppenzwang« zur quasi verpflichtenden Nutzung, ohne die wichtige Ereignisse verpasst werden und soziale Isolierung die Folge sein könnte. Hinzu tritt die generelle Lebenssituation: manche sind auf die Verwendung kostenloser Varianten an-

7 Vgl. Hegel 1970 [1806/07], S. 398–441.

8 Vgl. deren gleichnamiges Buch. Vor dem Hintergrund des Nationalsozialismus und Zweiten Weltkriegs verfolgen sie die Frage, »warum die Menschheit, anstatt in einen wahrhaft menschlichen Zustand einzutreten, in eine neue Art von Barbarei versinkt.« Adorno/Horkheimer 1969, S. 1

gewiesen, müssen sich bestimmten Unternehmen ausliefern, weil sie keine Zeit und Geld haben, um sich etwas anderes zu leisten, oder mit Technik unerfahrene Menschen, die schlicht aus Unkenntnis die erstbesten Angebote nutzen, etwa vorinstallierte Programme, die sich diesen ausgewählten Platz in der Regel teuer erkauft haben. Unter solchen Bedingungen endet denn auch die Freiwilligkeit der mit der Nutzung fast immer einhergehenden Datengabe. Die einzelnen stehen einer Übermacht gegenüber, gegen die sie allein nicht ankommen. Jorinde Schulz spricht in ihrer Untersuchung von Onlineplattformen sogar von *Hörigkeit*, *Verfügbarmachung*, *Sanktionsregime* und *Plattformpaternalismus*.[9]

Monopole untergraben die Wahlfreiheit und widersprechen dadurch sowohl dem Ideal der freien Marktwirtschaft als auch der freien Selbstbestimmung. Insofern liegt es nicht nur im Interesse des Marktes, sondern auch der Demokratie, dass stets Alternativen angeboten werden und nicht wenige Konzerne allein solche Monopolstellungen einnehmen, wie es aktuell der Fall ist. Nicht selten handelt es sich bei diesen Marktstellungen allerdings auch um eine Frage des Trends und lässt sich daher von beiden Seiten nur schwer kontrollieren. Im Zeitraum der letzten zwanzig Jahre lassen sich zahlreiche Auf- und Niedergänge großer Dienste oder Plattformen im Internet leicht beobachten. Sie sind nicht immer so unantastbar wie es kurzzeitig scheinen könnte. Ehemals vermeintlich unverzichtbare Angebote sind mitunter schon wenige Jahre später vollkommen vergessen.[10]

Aus dieser Sicht ist die beständige Überwachung und Anpassung des eigenen Netzwerkes für die Anbietenden sogar überlebensnotwendig geworden, um den jeweiligen Anforderungen der Kundschaft gerecht zu werden. Beide Parteien sind voneinander abhängig, keine hat absolute Narrenfreiheit. Und der Anspruch der Kundschaft wächst ständig. Da sie zugleich der alles ermöglichende Datenlieferant ist, darf sie aber keinesfalls vergrault werden. Kundenunfreundliche Dienste haben im Digitalen heutzutage eher geringe Halbwertszeiten. Gerade kleinere Unternehmen können Negativbewertungen im Internet schnell in unangenehme Situationen bringen. Nur wenige Nischen und Markenprodukte mögen hier vielleicht die Ausnahme sein.

Diesem impliziten Kampf um den besten Service verdanken wir wiederum dessen beharrliche Weiterentwicklung. Digitale Dienste bieten dadurch

9 Vgl. Schulz 2019.

10 Zum Beispiel Myspace, ICQ, MSN, Vine, Skype und viele andere.

zuvor ungeahnte Möglichkeiten, sodass sich der Freiheitsspielraum in gewissen Bereichen effektiv vergrößert hat. Es gibt zum Beispiel vielfältige Optionen, um sich sofort mit Menschen auf der ganzen Erde auszutauschen, sei es durch Nachrichten, Telefonate oder direkte Videoübertragungen. Dadurch werden sogar neue Formen von Kritik, Revolte und Widerstand möglich, man denke etwa an den Arabischen Frühling, sowie die Chance, global Solidarität zu bekennen, wie etwa nach Terroranschlägen oder kriegerischen Auseinandersetzungen.

All diese Leistungen haben gleichwohl ihren Preis. Sie erfordern Zugang zu den entsprechenden Nutzungsdaten. Und große Datensammlungen erlauben Rückschlüsse auf Gewohnheiten und Bedürfnisse, die uns häufig selbst gar nicht bewusst sind. In der digitalen Welt wissen Anbieter daher nicht selten besser über unsere Bedürfnisse Bescheid als wir selbst, weil sie nicht danach fragen, was wir von uns selbst denken und uns einreden, sondern weil sie vermittelt über Daten beobachten, was wir tatsächlich tun. Indirekt ist der gläserne Mensch bereits vielfach gelebte Realität. Interessanterweise wird dieser Umstand kaum noch als störend empfunden, vielmehr hat man sich wohl daran gewöhnt und damit abgefunden. Der Handel, Daten gegen Leistung einzutauschen, scheint den meisten offenbar ein gutes Geschäft zu sein. In kritischer Hinsicht ließe sich sogar von »einem kollektiven Verdrängungs- und Herunterspielungseffekt in Bezug auf die persönlichen, sozialen und gesellschaftlichen Folgen der Nutzung durch die dabei anfallenden Massendaten« sprechen.[11] Dem entgegen ist allerdings auch nicht von der Hand zu weisen, wie unheimlich bequem und alltagserleichternd es ist, sich den großen Unternehmen und Plattformen auszuliefern. Ihr Service ist in der Regel tatsächlich vorzüglich, eben um den kaum spürbaren Preis der Daten, über den sie sich finanzieren. Sie wissen in der Regel schon mehr über uns als wir selbst und sie wissen, wann wir was gerne hätten, denn genau mit diesem Wissen verdienen sie ihr Geld. Sie sind eine Art digitaler Butler, der einem jeden Wunsch von den Augen abliest und immer weiter in die dekadente Verschwendung treibt. Dank Hegel und Nietzsche wissen wir, wie diese Situation auf lange Sicht meistens ausgeht: der Herr ruht sich aus, wird fauler und dümmer, während der Knecht arbeitet und sich bildet, dadurch immer klüger wird und

11 Mühlhoff 2019, S. 83.

zusehends die Kontrolle übernimmt.[12] Das Verhältnis wird sich also mit der Zeit voraussichtlich umkehren und ist nicht davor gefeit, dies immer wieder zu tun. Heute übernehmen wir meist selbst die Rolle des Herren, der sich alles abnehmen lässt und darum stetig mehr verdummt, unmündiger und unselbstständiger wird, weil er schließlich manche Aufgaben gar nicht mehr allein ausführen könnte. Wir geraten in eine Abhängigkeit von dem Knecht. Am bezeichnendsten steht hierfür das permanent bei sich getragene Smartphone.

Es ließe sich an dieser Stelle aber auch ketzerisch fragen, was daran eigentlich so schlimm sei? Ist ein dekadentes, umsorgtes Leben nicht seit Menschengedenken ein erträumtes Ideal? Dass diese Sichtweise sich zunehmender Beliebtheit erfreut, lässt sich problemlos am gegenwärtigen Inhalt sozialer Medien ablesen. Die Nutzung umsorgender Dienste ist umso verlockender, weil zahllose digitale Angebote vermeintlich kostenlos zur Verfügung gestellt werden, weil man scheinbar nichts bezahlen muss, man gibt, ohne einen direkten Verlust zu bemerken. Nur zu gern schieben wir also das »verdrießliche Geschäft« (Kant[13]) des eigenen Denkens und Handelns auf die angebotene Technik. Damit füttern und fördern wir zugleich unsere virtuellen Diener, zunächst tatsächlich zu unserem eigenen Vorteil. Denn je geschickter und besser diese Diener, die technischen Dienste sind, umso besser ist auch ihr Service für uns, umso bequemer wird unser Leben. So lautet ihr Versprechen und verführendes Angebot. Schlimmstenfalls verlernen wir dabei zusehends unseren Verstand und erst recht unsere Vernunft zu gebrauchen. Denn je mehr man sich an diese angenehmen Bequemlichkeiten gewöhnt, umso weniger möchte man auf sie verzichten. Und je mehr man sich abnehmen lässt, umso mehr verlernt man womöglich, Dinge selbst zu erledigen.

Das Ziel aller Anbieter ist die langfristige Bindung an ihre Plattform und deren Dienste, um ebenso langfristig die daraus resultierende Datengewinnung sowie Werbeeinnahmen sicher zu stellen. Medienbibliotheken und Softwareanwendungen werden beispielsweise nicht mehr gekauft, sondern abonniert, also für eine bestimmte Zeit ein Zugangsrecht erworben. Einmal

12 Siehe Hegel 1970 [1806/07], insbesondere der gleichnamige Abschnitt über »Herrschaft und Knechtschaft« und Nietzsche 1988 [1887]. Allerdings ist bei beiden Autoren die Thematik für das ganze Werk bedeutsam und taucht immer wieder an verschiedenen Stellen auf. Literarisch humoristische Darstellungen des dummen Herrn und klugen Knechts finden sich unter anderem bei Cervantes und Diderot.

13 Kant 2011 [1784], S. 53.

diesen Zugang erlangt, kann es äußerst schwerfallen, sich wieder davon zu lösen. Aus den vielen schmackhaften Angeboten entstehen wiederum allzu leicht subtile Forderungen. All die zugänglichen Medien wollen schließlich auch konsumiert werden. Neben dem generellen Zeitverlust besteht hier ein hohes Suchtrisiko. Wir mögen durch Technik bisweilen Zeit gewinnen, verplempern diese aber gleich wieder durch deren nahezu permanente Nutzung. Und wir werden dadurch nicht nur an sie gewöhnt, sondern auch durch sie geprägt. Denn die permanente Datensammlung erzeugt auch neue Möglichkeiten der Beeinflussung. Je mehr Daten jemand über mein Verhalten hat, desto mehr Informationen kann er daraus ableiten und je mehr Informationen jemand über mich hat, desto leichter kann er mich manipulieren. Diese Manipulation ist real und wird bereits alltäglich angewandt. Die Wirtschaft beobachtet über Daten ihre potentielle und aktive Kundschaft und bemüht sich gezielt um deren Kaufkraft oder Nutzung. Sie sucht und erkennt Schwächen, um etwas zu verkaufen. Wer beispielsweise ein großer Liebhaber von Filmen ist, kann leichter dazu angeregt werden wieder ins Kino zu gehen. Wer sich für Mode interessiert und bereits viel Geld für Kleidung ausgegeben hat, wird voraussichtlich auch zukünftig zu solchen Ausgaben bereit sein. Bei solcher Manipulation geht es weniger um Bedürfnisbefriedigung als vielmehr um deren bewusste Erzeugung. Werbung schafft Bedürfnisse. Wer nichts von all den neuen Medien, Gütern und Geräten, Anwendungen und vielem anderen weiß, könnte sie gar nicht erst begehren. Mitunter sind deshalb Werbung und Profilerstellung so ein riesiges Geschäft. Wir meinen, selbst darüber zu bestimmen, was wir alles konsumieren, meist sind wir dabei aber schon längst die Opfer subtiler Manipulation geworden. Allerdings nehmen wir diese Gefahr buchstäblich in Kauf für all die Annehmlichkeiten, die uns die digitalen Nutzungsangebote bieten.

Um solcher Manipulation doch noch entgegenzuwirken haben sich unter anderem zwei Strategien etabliert, Datenschutz und Aufklärung, die jedoch dieselbe Dialektik aufweisen und dadurch mitunter selbst zum Problem werden können.

Datenschutz

Obwohl mittlerweile potentiell jedes mit Technik in Verbindung stehendes Verhalten über digitale Daten nachverfolgt werden kann, beschränkt sich die

Furcht davor meist nur auf spezifische Bereiche. Die Bonität wird beispielsweise eher geheim gehalten als der Standort, manche Konsumgüter werden begeistert präsentiert, andere beschämt verheimlicht. Entsprechend ergeben sich differenzierte Anforderungen an den Datenschutz. Dieser soll mich der Idee nach vor äußeren Einflüssen bewahren, damit ich frei bin, mich selbst zu bestimmen. Ohne die gewünschte Freiheit der Selbstbestimmung gäbe es erst gar keinen Anlass für Datenschutz.[14] Fraglich ist jedoch, wie weitreichend dieser Schutz sein kann und muss, um die Selbstbestimmung zu wahren und abermals, was diese dann konkret ausmacht und umfasst.

In der Europäischen Union sind personenbezogene Daten rechtlich geschützt und jede Person hat ein gesetzliches Auskunftsrecht darüber, welche sie betreffenden erhobenen Daten vorliegen.[15] Solche Auskünfte können Laien aber in der Regel gar keine hilfreichen Informationen vermitteln, denn den gesammelten Daten sieht man nicht an, welche Aussagekraft ihnen innewohnt, einzig die schiere Masse könnte beeindrucken oder erschrecken. Hinzu kommt, dass Unternehmen nicht nur Daten mit Bezug auf meine Person vorliegen, sondern über mich und meine Preisgabe meist auch direkt oder indirekt Informationen über andere Personen mitgeliefert werden. Zum Beispiel sind die werkseitig installierten Adressbücher, Telefon- und Kontaktdienste der meisten Smartphones heutzutage mit dem Internet verbunden und teilen ihre erfassten Daten mit den Anbietern. Sobald ich einen neuen Kontakt in ein solches Adressbuch aufnehme, werden diese Kontaktdaten weitergeleitet. Selbst wenn ich mich sogar gänzlich vom Internet abkapseln würde, hätte ich also keine Garantie, dass nicht andere Menschen Daten und Informationen über mich hochladen, sei es nun bewusst oder unabsichtlich. Ebenso wenig lässt sich das als Privatperson überprüfen. Informationelle Selbstbestimmung, wie sie noch im Volkszählungsurteil beschrieben wurde, ist in vollem Umfang nicht mehr möglich, falls sie es denn jemals war.

Müssten die Datenschutzvorgaben also strenger gefasst werden? Hier ist Vorsicht geboten. Überzogener Datenschutz kann durchaus auch selbst ein Hindernis für die Selbstbestimmung darstellen, denn manche Dienste funktionieren eben nur mit entsprechenden Daten. Der Datenschutz muss aufpassen, dass er nicht selbst die Freiheit zu sehr einschränkt, die er doch

14 Interessanterweise taucht der Ausdruck »Selbstbestimmung« in der europäischen Datenschutzgrundverordnung nicht auf.

15 EU Grundrechte Charta II, 8 sowie ergänzend DSGVO, Art. 15 Abs. 1.

eigentlich bewahren will. Die angeleitete Eigenüberwachung mittels Daten und Diensten etwa kann paradoxerweise auch frei machen oder eröffnet zumindest eine Vielzahl neuer Möglichkeiten, beispielsweise eine eigene Leistungsanalyse beim Sport, Hilfestellung bei Diäten oder Unterstützung bei der Suchtbekämpfung. Nicht selten liegt es deshalb im Interesse der Nutzenden, Daten zu teilen und Zugang zu gewähren, um für sie zugeschnittene Leistungen oder sogar Vorteile zu erhalten, etwa günstigere Beiträge bei Versicherungen. Bislang funktioniert dies nur in dieser Richtung. Es wäre aber ebenfalls denkbar und technisch problemlos umsetzbar, das Verhältnis umzukehren, sodass Versicherungen beispielsweise bei riskantem Fahrverhalten und ungesundem Lebensstil höhere Beiträge verlangen. Man könnte sogar dafür argumentieren, dass es sich hier um berechtigte Kalkulationen handelt, die vielleicht nötig sind, um den Versicherungsschutz zu gewährleisten. Die Datengabe könnte im Extremfall zur grundsätzlich verpflichtenden Bedingung eines Vertragsabschlusses gemacht werden. Hiergegen legt der Datenschutz aber bislang sein berechtigtes Veto ein: Die Datengabe muss freiwillig bleiben und darf keine unerwünschten Nachteile mit sich bringen, andernfalls wäre die Fremdbestimmung zu groß.

Da der Personenbezug in vielen Fällen gar nicht relevant ist, liegt die mittlerweile gängige Kompromisslösung in der Anonymisierung oder Pseudonymisierung der Daten. Ob dadurch immer ein ausreichender Schutz gewährleistet werden kann, ist umstritten.

Aufklärung

Eine generell beliebte Strategie gegen allerlei Übel ist die Aufklärung über dieselben. Man könnte meinen, die fruchtbarste Abhilfe gegen Manipulationen wäre eine umfassende Aufklärung darüber, welche Daten bei der alltäglichen Techniknutzung anfallen, wer wie darauf Zugriff hat, welche Informationen daraus zu gewinnen sind und welche Folgen es haben kann, wenn Unternehmen bestimmte Daten von mir und meinem Umfeld zur Verfügung stehen. Informationell selbstbestimmt könnte ich vielleicht nur sein, wenn ich über all diese Möglichkeiten und Risiken der Informationsgewinnung anderer über mich aufgeklärt bin. Dann könnte ich in vielen Fällen zumindest potentiell entscheiden, welche Anbieter ich nutzen möchte und welche Daten, Risiken und Vereinbarungen dabei anfallen, abgesehen von meinen bewusst und gezielt geteilten Informationen (Nachrichten, Bilder, Kom-

mentare und vieles andere). Es zeigt sich hier aber ein prinzipielles Problem der komplexen Zeit: einerseits sollen die Menschen sich selbst bestimmen können, andererseits können sie dabei den vielfältigen Anforderungen gar nicht mehr gerecht werden. Die Lage ist inzwischen selbst bei Alltagshandlungen so komplex, dass sich fragen lässt, ob ich als einzelner, selbst wenn ich mich ausführlich informieren und recherchieren würde, überhaupt noch in der Lage wäre mich in gewissen Situationen selbstbestimmt zu entscheiden, weil ich die Lage mit ihren unzähligen Verflechtungen erst gar nicht vollständig überblicken und letzten Endes auch nicht adäquat beurteilen kann. Ganz abgesehen von den technischen Wissensanforderungen, wann Daten anfallen, wie überhaupt die Datenteilung geschieht, welche Prozesse ständig im Hintergrund laufen, wie diese miteinander verzahnt sind und vielem mehr.

Die Komplexität ist ein ernstzunehmendes Problem für sich, es lässt sich jedoch noch früher ansetzen: Muss ich denn überhaupt vollständig aufgeklärt und informiert sein, um mich zu entscheiden und selbst zu bestimmen? Ganz abgesehen davon, ob eine so umfangreiche Aufklärung für einzelne überhaupt zu leisten wäre, zumal als Nebenbeschäftigung, hat dieser Ansatz seine eigenen Schwächen. Denn Aufklärung führt nicht immer direkt zu mehr Selbstbestimmtheit, bisweilen bewirkt sie sogar genau das Gegenteil. Silja Samerski hat dieses Paradox am Beispiel der genetischen Aufklärung vorgeführt: die Beratung führt notwendig in die Zwangslage, sich entscheiden zu müssen (in diesem Fall für oder gegen einen Gentest), um sodann für diese Entscheidung und ihre Folgen auch noch die Verantwortung übernehmen zu müssen. »Ich möchte die Annahme infrage stellen, dass genetische Aufklärung zu einem eigenen, unabhängigen Urteil befähigen kann. Mir scheint vielmehr, dass genetische Aufklärung eine Freiheit verkehrt: die Freiheit, ohne Bevormundung selbst wissen und entscheiden zu können.«[16] Beharrt man auf einer zuvor nötigen Aufklärung untergräbt man gerade die prominent von Kant formulierte Mündigkeit, sich seines Verstandes ohne Leitung eines anderen zu bedienen.[17] Das Beispiel der genetischen Aufklärung ist eine solche fremde Anleitung von außen. Zumal hier sogar die Entscheidung selbst aufgedrängt wird. Samerski resümiert: »Eine selbstbestimmte Entscheidung zu treffen, ist heute kein Freiheitsrecht, sondern eine neue Pflicht.«[18] Sofern Selbstbestimmung wie hier auf

16 Samerski 2010, S. 11

17 Vgl. Kant 2011 [1784], S. 53.

18 Samerski 2010, S. 92; vgl. Žižek 2020, S. 46 f.

bloße Zustimmung oder Ablehnung reduziert, also vor eine absolute Wahl gestellt wird, kann sie kaum noch als frei betrachtet werden. Zudem fordert der von allen Seiten kommende Druck die Zustimmung bereits vor der Entscheidung.

Gleiches gilt im Übrigen auch für die sogenannte »Informierte Einwilligung« im medizinischen Kontext oder bei alltäglicher Internetnutzung, wenn Webseiten und Plattformen mir zuvor eine solche Einwilligung zur Datenverarbeitung abnötigen. Ob all diese erteilten Einwilligungen wirklich so freiwillig und informiert erfolgen wie es von der Datenschutzgrundverordnung eigentlich vorgesehen ist,[19] darf bezweifelt werden. In der Regel werden sie lediglich erteilt, um Zugang zu erhalten zu Behandlungen, Diensten, Webseiten oder Plattformen und insofern bloß als das geringere Übel akzeptiert.

Aufklärung ist also ein zwiespältiges Unternehmen. Gänzlich auf sie verzichten lässt sich aber auch nicht. Völlige Unwissenheit würde die Manipulationsgefahr deutlich erhöhen.

»Wir hegen keinen Zweifel – und darin liegt unsere petitio principii –, daß die Freiheit in der Gesellschaft vom aufklärenden Denken unabtrennbar ist. Jedoch glauben wir, genauso deutlich erkannt zu haben, daß der Begriff eben dieses Denkens, nicht weniger als die konkreten historischen Formen, die Institutionen der Gesellschaft, in die es verflochten ist, schon den Keim zu jenem Rückschritt enthalten, der heute [1944] überall sich ereignet. Nimmt Aufklärung die Reflexion auf dieses rückläufige Moment nicht in sich auf, so besiegelt sie ihr eigenes Schicksal.«[20]

Trotz allem stellen Aufklärung und Informierte Einwilligung, ebenso wie der Datenschutz, nach wie vor große Errungenschaften dar, die wir nicht verlieren wollen, weil sie zumindest eine Handlungsmöglichkeit bieten. Ich *könnte* nun immerhin Nein sagen und mich widersetzen. Selbst wenn ich das praktisch niemals tue, ist dieser Freiheitsgewinn weiterhin in allen drei Fällen zu verteidigen, eingedenk ihrer potentiellen Risiken.

Es ließen sich noch deutlich mehr Konstellationen schildern, die die Ambivalenz von Datenzugängen veranschaulichen. Smart Cities, Sozial-

19 Vgl. DSGVO, Art. 4 Nr. 11: »›Einwilligung‹ der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist«.

20 Adorno/Horkheimer 1969, S. 3.

kredit-Systeme, digitale Informationsquellen, Künstliche Intelligenz und vieles mehr bergen ebenfalls die geschilderte Dialektik. Paradoxerweise erhöhen sich in diesen Systemen Abhängigkeit und Freiheit häufig parallel. Jedes Zugeständnis auf der einen Seite birgt potentielle Probleme auf der gegenüberliegenden. Man kann diese Dialektik aber auch nicht umgehen, sondern muss sie als prinzipiellen Konfliktfall anerkennen und lernen, mit ihr umzugehen. Sie kann nicht aufgelöst, sondern muss ausgehalten werden. Vorschnelle Verbote oder Zugeständnisse können das Umschlagen beschleunigen und so allzu leicht unerwünschte Folgen mit sich führen. Im Politischen wie im Privaten bedarf es daher einer stetigen Abwägung zwischen Nutzen und Abhängigkeit, Freiheitsgewinn und -verlust. Die Frage nach der Zugangsverantwortung stellt sich auf beiden Seiten.

IV. Aussichten

Datenzugänge sind ein gesamtgesellschaftliches Thema. Das digitale Datendickicht überwuchert immer mehr Bereiche des Lebens, ist mit allem verflochten und wir müssen uns darin behaupten. Die Verflechtungen reichen von basalsten Alltagsfragen bis hin zu den Idealen unserer Kultur. Es geht also nicht nur um Fragen des Datenschutzes oder Abwägungen von Zugangsöffnung oder -schließung, sondern darüber hinaus um das generelle Selbstverständnis, mit dem solche Fragen angegangen werden. Für eine demokratische Lebensform ist die Digitalisierung insofern nicht nur eine Herausforderung, sondern gleichfalls eine wiederholte Aufforderung, sich mit dem eigenen Horizont auseinanderzusetzen. Globale Vernetzung, unvorstellbare Datenmengen und deren Auswertung bieten noch lange nicht ausgeschöpfte Möglichkeiten, sowohl Chancen als auch Risiken für das demokratische Projekt. Die Regelung von Datenzugängen steht dementsprechend vor der Schwierigkeit, einerseits gewünschte Zugänge zu ermöglichen, etwa für die Politik und bestimmte Forschungsvorhaben, und andererseits vor unerwünschten Zugriffen zu schützen, nämlich solchen, die das Recht des Einzelnen und die Demokratie herausfordern. Ins Extrem getrieben wären beide Varianten fatal und sind zu vermeiden, sowohl die grenzenlose Öffnung, *open access* von allem für alle, als auch die rigorose Verschließung aller Daten. Im ersten Fall könnten mühsam errungene Erkenntnisse gleichermaßen Opfern und Unterdrückern zufließen, also Machtasymmetrien eher verfestigen als aufbrechen, im zweiten Fall würde

niemand von dem Potential der Datenmassen profitieren können, die für viele Bereiche mittlerweile die Arbeitsgrundlage darstellen. Dass sich dabei gewisse Schwierigkeiten nicht ausschließen lassen, sondern vielen Ansätzen von vornherein inhärent sind, wurde versucht zu zeigen.

Verantwortung ist in diesem Komplex nicht leicht zu verorten. Der traditionell subjektbezogene Begriff gerät hier bisweilen an seine Grenzen. Womöglich bräuchte es sogar ein neues, eher kollektives Verständnis von Verantwortung. Einerseits trägt zwar jeder Mensch die Verantwortung für sich selbst und das eigene Handeln, andererseits gibt es heute unzählige unklare Bedingungen, die potentiell überfordern und Verantwortungszuschreibungen erschweren. Ich kann zum Beispiel über die durch mein Verhalten generierten Daten oft nicht bestimmen, weil ich erst gar nichts von ihnen mitbekomme. Andererseits muss ich aber auch nicht immer über sämtliche Details aufgeklärt sein, um mich generell gegen eine Datensammlung und -verarbeitung zu entscheiden. Und sofern ich mich für sogenannte Datenspenden entscheide, tue ich das wiederum auf eigene Verantwortung und es bleibt mir daher selbst überlassen, ob ich mich zuvor darüber ausführlich informiere oder eben nicht.

Der demokratische Staat indes muss die Möglichkeit der Selbstbestimmung nicht nur aus reiner Nächstenliebe garantieren, sondern schlichtweg um sein eigenes Bestehen zu erhalten. Wenn die Grundrechte nicht mehr gewährleistet wären, gäbe es auch keine freie Bevölkerung mehr, die den Staat legitimiert. Wahlen würden zu einer bloßen Farce degradiert, wie man es leider in manchen Ländern schon beobachten konnte. Der Schein der Demokratie soll gewahrt bleiben, doch ihr Herz hat aufgehört zu schlagen. Demokratien sterben heute weniger durch direkte Machtergreifung und Putsch, als durch schleichende Prozesse über Gesetze, Verordnungen oder die Aufhebung dergleichen, auch Zensur oder eine extrem polarisierte Bevölkerung, die den demokratischen Diskurs beeinträchtigen und schließlich aufheben würde.[21]

Möchte man an den demokratischen Ideen festhalten, ist zu überlegen, wie sie mit den aktuellen Gegebenheiten und Möglichkeiten zu vereinbaren sind. Welche Wege müssen eingeschlagen werden, um ihre Verwirklichung weiter zu ermöglichen und zu befördern? Welche Hindernisse stehen diesem Projekt im Weg? Ein markantes Problem besteht darin, dass der öffentliche Raum des Internets aktuell zu einem Großteil von wenigen großen Tech-

21 Vgl. Levitsky/Ziblatt 2018.

nikkonzernen dominiert wird. Sie haben dadurch einen immensen, nicht zu unterschätzenden Einfluss auf Medien, Konsum, Wahlen, Politik, kurzum auf unsere gesamte Lebenswelt. Je mehr ihre Macht steigt, umso kleiner wird unsere Freiheit. Wer die Technik kontrolliert, kontrolliert inzwischen die Welt. »Alles wird heute von digitalen Netzwerken gesteuert, vom Transport bis zur Gesundheit, von der Elektrizität bis zum Wasser. Aus diesem Grund ist das Netz heute unser wichtigstes Gemeingut und der Kampf darum, wer es kontrolliert, ist *der* entscheidende Kampf.«[22] Zwar müssen sich auch Unternehmen und Konzerne gewissen Regelungen, Gesetzen und Forderungen beugen, dennoch sind sie prinzipiell allein für das Regelwerk ihrer Plattformen und Dienste verantwortlich. In der digitalen Welt sind wir insofern oftmals fremdbestimmt, da wir uns entweder diesen vorherrschenden Regeln fügen müssen oder unsere Nutzung einstellen. Der Ausschluss von den größten Plattformen und Diensten käme heute aber beinahe schon einer Verbannung ins Exil gleich. Eine solche Abhängigkeit ist aus demokratischer Sicht eigentlich nicht hinnehmbar, es bedarf einer Rückeroberung dieses öffentlichen Raumes. Aber wie könnte eine Revolution im Digitalen aussehen? Wie ließe sich das Internet demokratisch gestalten? Bräuchte es vielleicht mehr staatliche Plattformen oder mehr Auflagen für bestehende Angebote? Mit diesen und ähnlichen Fragen wird man sich zukünftig weiter zu beschäftigen haben.

Allzu leicht wird heute allerdings die Verantwortung allein den Unternehmen oder der Politik zugeschrieben. Ohne die Millionen von täglichen Nutzenden und der wählenden Bevölkerung wären aber beide hilflos. Wir alle tragen gleichermaßen Verantwortung für die Entwicklung, weil wir meist zu bequem sind, um uns politisch zu engagieren, zu bequem, um uns um unseren Datenschutz zu kümmern, zu bequem, um uns zu bilden und aufzuklären und zu bequem, um die Manipulationen, denen wir täglich ausgesetzt sind, überhaupt zu bemerken und zu hinterfragen. Wir selbst sind ebenfalls und ganz maßgeblich für den Erhalt der Demokratie und ihrer Ideen verantwortlich, denn diese sind nur wirklich, wenn sie im Handeln der Menschen ihren lebendigen Ausdruck finden.

22 Žižek 2020.

Literatur

Adorno, Theodor/Horkheimer, Max (1969): *Dialektik der Aufklärung. Philosophische Fragmente*, Frankfurt am Main.

Augsberg, Steffen/Gehring, Petra (2022): *Datensouveränität. Positionen zur Debatte*, Frankfurt am Main.

DSGVO [= Europäische Kommission] (2016): *Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)*, Amtsblatt L 119/1, https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679 [21.5.2024].

Europäische Kommission (2012): *Charta der Grundrechte der Europäischen Union*, Amtsblatt C 326/391, https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:12012P/TXT [21.5.2024].

Gamm, Gerhard (2011): *Bestimmung, in:* Kolmer, Petra/ Wildfeuer, Armin G. (Hg.): *Neues Handbuch philosophischer Grundbegriffe*, Freiburg, S. 361–386.

Hegel, Georg Wilhelm Friedrich (1970 [1830]): Enzyklopädie der philosophischen Wissenschaften III, in; ders.: *Werke*, Band 10, Frankfurt am Main.

Hegel, Georg Wilhelm Friedrich (1970 [1806/07]): Phänomenologie des Geistes, in; ders.: *Werke*, Band 3, Frankfurt am Main.

Schulz, Jorinde (2019): Klicklust und Verfügbarkeitszwang, in: Mühlhoff, R.; Breljak, A.; Slaby, J. (Hg.): *Affekt Macht Netz. Auf dem Weg zu einer Sozialtheorie der Digitalen Gesellschaft*, Bielefeld, S. 131–153.

Kant, Immanuel (2011 [1784]): Beantwortung der Frage: Was ist Aufklärung?, in: ders.: *Werke*, Band VI, Darmstadt, S. 51–61.

Levitsky, Steven/Ziblatt, Daniel (2018): *Wie Demokratien sterben*, München.

Mühlhoff, Rainer (2019): Big data is watching you. Digitale Entmündigung am Beispiel von Facebook und Google, in: Mühlhoff, R./ Breljak, A./ Slaby, J. (Hg.): *Affekt Macht Netz. Auf dem Weg zu einer Sozialtheorie der Digitalen Gesellschaft*, Bielefeld, S. 81–107.

Nietzsche, Friedrich (1988 [1887]): Zur Genealogie der Moral, in: *Kritische Studienausgabe (=KSA)*, Band 5, München, S. 245–412.

Samerski, Silja (2010): *Die Entscheidungsfalle*, Darmstadt.

Winter, Max (2017): Demokratietheoretische Implikationen des Rechts auf informationelle Selbstbestimmung, in: Friedewald, Michael/Lamla, Jörn/Roßnagel, Alexander (Hg.): *Informationelle Selbstbestimmung im digitalen Wandel*, Wiesbaden.

Žižek, Slavoj (2020): *Hegel im verdrahteten Gehirn*, Frankfurt am Main.

Regulatorische Verantwortung für den Datenzugang: Entwicklungslinien und Gestaltungsoptionen

Steffen Augsberg

I. Problemaufriss: Datenzugang als Verantwortungsproblem

Im traditionellen Verständnis der sogenannten informationellen Selbstbestimmung[1] steht das Individuum im Fokus, dem die betroffenen Daten zugeordnet sind. Das Bundesverfassungsgericht spricht entsprechend in seinem Volkszählungsurteil ganz ausdrücklich von der »Befugnis *des Einzelnen*, grundsätzlich selbst über die Preisgabe und Verwendung *seiner* persönlichen Daten zu bestimmen.«[2] Damit weist diese grundrechtliche Fundierung des Datenschutzgedankens von Anfang an eine inhärente Spannung auf: Sie ist einerseits – wie das Datenschutzrecht insgesamt – Ausdruck eines durchaus erstaunlichen gesetzgeberischen und gerichtlichen Weitblicks; die rechtlichen Regelungen nahmen frühzeitig Gefährdungen in den Blick, die angesichts des damaligen Stands der Technik bestenfalls zu erahnen waren.[3] Exemplarisch hierfür ist die hellsichtige Aussage des Bundesverfassungsgerichts, es werde künftig keine belanglosen Daten mehr geben.[4] Diese zunächst gewagte Prognose hat sich im Zuge der Digitalisierung und der damit verbundenen kontinuierlichen De- und Rekontextualisierung von Daten[5] klar als zutreffend herausgestellt und ist heute wichtiger denn je. Andererseits knüpft die damals neue grundrechtliche Garantie – wie später auch das sogenannte Computergrundrecht (»Grundrecht auf Ver-

1 Grundlegend BVerfGE 65, 1 ff.

2 BVerfGE 65, 1 (Hervorhebung hinzugefügt).

3 Siehe hierzu auch Buchheim/S. Augsberg 2024; zur Entwicklungsgeschichte ferner knapp Hornung/Spiecker gen. Döhmann 2019, Rn. 5 ff.; ausführlich Schöndorf-Haubold 2020; Bull 2011, S. 22 ff.

4 Vgl. BVerfGE 65, 1 (43, 45). Dazu näher etwa Hornung/Spiecker gen. Döhmann 2019, Rn. 28 ff. m.w.N.

5 Vgl. dazu etwa Deutscher Ethikrat 2017, S. 86 ff.

traulichkeit und Integrität informationstechnischer Systeme«[6]) strukturell an bekannte Mechanismen der Grund- als Freiheits- bzw. Abwehrrechte an.[7] Der hiermit typischerweise verbundene Bezug auf den freiheitsgefährdenden Staat wird zwar frühzeitig ergänzt durch eine nähere Ausgestaltung, die (auf einfachgesetzlicher Basis) auch die datenschutzrechtlichen Pflichten anderer Privatrechtssubjekte miteinbezieht. Dennoch bleibt auch für die informationelle Selbstbestimmung das klassische subjektiv-rechtliche (Grund-)Rechtsmodell zentral,[8] das wiederum historisch starke Verbindungen zu einem an den Staat adressierten Eigentumsschutz aufweist.[9] Daten erscheinen damit ebenfalls als etwas, das dem Einzelnen »gehört« und das er gegen Andere, insbesondere den Staat, verteidigen kann bzw. muss.

Diese eigentumsanaloge Grundausrichtung ist in der Folge immer wieder thematisiert und teilweise kritisiert worden.[10] Sie wirkt sich auch auf die Problematik der Zugangsgewähr aus, denn letztere wird auch infolge dieser basalen Strukturentscheidung herkömmlich als primär individuell wahrzunehmende Aufgabe verstanden. Wer für wen welche Daten öffnet, ist damit eine Frage, die jedenfalls prioritär durch einzelne Personen zu beantworten ist. Folgerichtig bildet die informierte, auf einen konkreten Verwendungszweck bezogene Einwilligung dieser »Berechtigten« nach wie vor die datenschutzrechtliche Standardlegitimation.[11] Alternativlos ist eine solche Behandlung des Datenzugangsproblems indes nicht. Vielmehr ist – um eine klare Gegenposition zu markieren – auch eine stärker kollektivistische Perspektive vorstellbar, die Daten weitestgehend aus dem Bezug zur Einzelperson löst und sie statt dessen der Allgemeinheit zuordnet.[12] Wo nämlich Daten in dieser Weise zum Allgemeingut bestimmt werden, sind Zugangsregeln entweder obsolet oder jedenfalls nicht länger einzelnen Individuen überantwortet. Mit der Verantwortung verschiebt sich gegebenenfalls auch die grundlegende Beweislast: wenn im individualorientierten Modell die Freiheit über die »eigenen« Daten als vorgegebene Ordnung erscheint,

6 BVerfGE 120, 274 (302 ff.), vgl. dazu statt vieler etwa Herrmann 2010; Bull 2011, S. 34 f., 56 f.

7 Dazu nur I. Augsberg 2021, S. 23 ff.

8 Dazu näher Düwell in diesem Band.

9 Vgl. zum Hintergrund einer entsprechenden Kritik I. Augsberg 2021, S. 73 ff.; zu Entwicklung und Voraussetzungen von Subjektvorstellungen siehe näher Vesting 2021.

10 Vgl. grundlegend und m.w.N. jüngst Behrendt 2023; siehe auch Ladeur 2009.

11 Vgl. etwa Ulbricht/Weber 2017. Dass datenschutzrechtlich neben der Einwilligung auch andere Erlaubnistatbestände existieren, steht dem nicht entgegen, siehe näher noch unten.

12 Vgl. allgemein auch die Beiträge in: Fischer-Lescano/Franzki/Horst 2018.

deren Beeinträchtigung *a priori* verboten, mindestens aber gesondert zu begründen und rechtfertigen ist, ist in der Allgemeingutvariante umgekehrt die Abschottung legitimationsbedürftig. Das erklärt, warum dies eine insbesondere im Kontext der Wissenschaft populäre Position ist, soweit »Open Science« als (idealisiertes) Gegenmodell zum zugangsbegrenzenden Datenschutz präsentiert wird.[13]

Beide Konzepte sind ersichtlich schon in ihrer jeweiligen, mehr oder weniger kontingenten Konstruktion angreifbar; vor allem aber sind sie funktional problematisch, soweit mindestens zweifelhaft ist, ob sie den Herausforderungen der Gegenwart (noch) entsprechen: wo die kollektivistische Zuordnung nicht nur die »Tragik der Allmende«[14] berücksichtigen muss, sondern zumal die individuelle Schutzbedürftigkeit ignoriert, stellt der Fokus auf das Individuum eine allenfalls als Ideal hilfreiche, *in praxi* aber regelhaft weniger privilegierende denn belastende Inbezugnahme der Datengeber dar. Denn das auf den ersten Blick den Interessen des Einzelnen dienende Modell erweist sich bei genauerer Betrachtung als zumindest partiell dysfunktional: es droht die Betroffenen zu überfordern, mit der Folge, dass entweder eine den realen Gefahren entsprechende Kontrolle nicht mehr gelingt oder aber in überschießender Tendenz die Kontrolle so extensiv ausgedehnt wird, dass auch gesellschaftlich wünschenswerte, individuellen Interessen nicht zuwiderlaufende Datennutzungen ausgeschlossen werden.[15]

Vor diesem Hintergrund ist in Ergänzung der analytischen Überlegungen zu den Normstrukturen und Subjektstatus[16] danach zu fragen, welche regulatorisch-gestalterische Antwort die hier zunächst nur angedeuteten Probleme vermeidet oder zumindest verringert. Das schreibt in gewissem Sinne ältere Untersuchungen zu alternativen Regelungsstrategien fort,[17] setzt aber grundlegender an. Konkret ist zu problematisieren, ob eine angemessene Reaktion nicht darin bestehen könnte/sollte, den Daten selbst größere Aufmerksamkeit zu schenken, also Schutz- und Zugangsansprüche an ihnen und den mit ihnen verbundenen möglichen Konsequenzen auszurichten. Zu diesem Zweck ist zunächst noch einmal knapp die historische Entwicklung des aktuellen Datenschutzmodells zu rekapitulieren (dazu II.).

13 Kritisch dazu Gehring in diesem Band.

14 Dazu klassisch Hardin 1968.

15 Für eine stärkere Berücksichtigung der »impersonalen Dimension der Rechtssubjektivität« auch schon Vesting 2021, S. 229 f.

16 Siehe Düwell in diesem Band.

17 Vgl. S. Augsberg 2022.

In einem nächsten Schritt sind Perspektiven zu Verantwortungsaspekten zu eröffnen (dazu III.), an die sich Ausführungen zu stärker vom Individuum gelösten – aber dieses nicht ignorierenden – Regulierungs- und Gestaltungsoptionen anschließen (dazu IV.). In diesem Rahmen können Anleihen in mindestens vierfacher Hinsicht genommen werden: (1) mit Blick auf die allgemeine kollektive Dimension der Grundrechte (überindividuell, aber nicht postindividuell), (2) beim Modell der »informationellen Freiheitsgestaltung«, (3) bei den sogenannten inpersonalen Grundrechten sowie (4) bei konkreten, datenschutzinternen und technologieinduzierten Weiterentwicklungen. Ein knapper Ausblick verweist auf die Möglichkeit und gegebenenfalls auch Erforderlichkeit, Verantwortung auch für die Gestaltung von Verantwortlichkeit(en) zuzuweisen (dazu V.).

II. Rückblick: Grundlagen und Entwicklungsschritte

Das Datenschutzrecht ist eine vergleichsweise junge Materie, deren Ursprünge in wissenschaftlichen Überlegungen und richterrechtlichen Festlegungen liegen.[18] Das, was heute mit einiger Sicherheit als »informationelle Selbstbestimmung« bezeichnet wird, sucht man deshalb im Grundgesetz vergeblich. Darüber hinaus enthält der Verfassungstext auch keine sonstigen expliziten Regelungen zum »Datenschutz«. Dennoch werden die entsprechenden rechtlichen Vorgaben zutreffend als verfassungsbasiert eingeordnet.[19] Die einschlägigen, durch kreative Verfassungsinterpretation gewonnenen[20] Vorgaben liefern indes keine präzise Detailsteuerung, sondern konstituieren »lediglich einen Ordnungsrahmen, dessen nähere Ausgestaltung dem Gesetzgeber zugewiesen ist.«[21] Diesen Spielraum, aber auch die dahinterstehenden verfassungsnormativen Grundannahmen gilt es, näher zu untersuchen. Weil es sich um ein zwar relativ junges, aber doch vergleichsweise komplexes und ausdifferenziertes Rechtsgebiet handelt, ist hierfür ein kurzer Blick auf die Entstehungsgeschichte des Datenschutzrechts hilfreich.[22] Während sich vereinzelte individualbezogene

18 Vgl. zum Folgenden auch Barczak 2023, Rn. 90 ff. m.w.N.
19 Dazu statt vieler Schöndorf-Haubold 2020, S. 35 ff.
20 Vgl. dazu allgemein Reimer 2020, S. 125 ff.; siehe auch Bryde 2016.
21 Deutscher Ethikrat 2017, S. 126.
22 Vgl. näher Schöndorf-Haubold 2020, S. 69 ff. m.w.N.; Timmermann 2019.

Geheimnisschutzregelungen schon relativ früh nachweisen lassen,[23] wurde ein weiterreichender allgemeiner Schutz der Privatsphäre erst Ende des 19. Jahrhunderts prominent als Gebot des US-amerikanischen Verfassungsrechts postuliert.[24] Das hier entwickelte Konzept von *privacy* im Sinnes eines *right to be left alone* wurde später – schon unter dem Eindruck modernerer Datenverarbeitung, aber selbstredend noch himmelweit entfernt von deren heutiger Ausprägung – dahingehend weiterentwickelt, dass ein (Grund-)Rechtsschutz dafür besteht, selbst zu bestimmen, ob und welche persönlichen Daten weitergegeben, gespeichert und verarbeitet werden dürfen.[25] Diese Grundidee einer umfassenden individuellen Kontrolle und Verfügungsgewalt nimmt erkennbar Anleihen am Schutz des Eigentums. Ungeachtet der später näher zu betrachtenden Frage, inwieweit dies den Eigenarten einer (digitalen) Datensphäre[26] gerecht wird, schließt sie damit zunächst an ein politisch wie rechtlich weithin konsentiertes, unser Wirtschafts- wie Rechtssystem prägendes Modell an.

Wohl auch deshalb erwies sich die Idee rasch als politisch außerordentlich erfolgreich; sie wurde in zahlreichen Gesetzgebungsakten umgesetzt. Nationaler wie internationaler Vorreiter war dabei das Land Hessen, das in Reaktion auf zunehmend automatisierte Datenverarbeitung 1970 das erste Datenschutzgesetz überhaupt erließ und zugleich den Posten des Datenschutzbeauftragten schuf. 1974 trat in Schweden das erste nationale Datenschutzgesetz in Kraft; 1976 wurde durch den Bundesgesetzgeber das Bundesdatenschutzgesetz vorgelegt, das dem persönlichkeitsrelevanten Missbrauch von Daten im öffentlichen wie im privaten Bereich entgegenwirken sollte. Auf europäischer Ebene[27] wurde 1995 unter kompetentieller Berufung auf die Binnenmarktklausel des Art. 114 AEUV die Europäische Datenschutzrichtlinie erlassen. Seit 2018 gilt die Datenschutz-Grundverordnung (DSGVO), die den Schutz personenbezogener Daten und den freien Datenverkehr innerhalb der Union gewährleisten soll. Mit dieser unmittelbar geltenden, also im Unterschied zur Richtlinie keiner Umsetzung durch die nationalen Gesetzgeber bedürftigen Verordnung sollte zum einen eine weitergehende Harmonisierung der Datenschutzregelungen erreicht werden. Zum anderen sollten bewährte datenschutzrechtliche Grundsätze

23 Vgl. dazu Austermühle 2002.
24 Warren/Brandeis 1890.
25 Siehe Westin 1967; vgl. auch Neuroth 2023.
26 Dazu näher Lambach in diesem Band.
27 Vgl. nur Di Martino 2005.

mit moderneren Regelungstechniken verbunden werden – etwa, indem das Prinzip der Datensparsamkeit als (auch) technische Aufgabe eingeordnet wurde, das sogenannte *privacy by design*.[28]

Für die verfassungsnormative Verankerung entscheidend ist nach wie vor das eingangs bereits erwähnte sogenannte Volkszählungsurteil des Bundesverfassungsgerichts aus dem Jahre 1983.[29] Das Gericht konnte dabei auf die zunächst von den Zivilgerichten entwickelte und von ihm selbst aufgenommene Rechtsprechung zum allgemeinen Persönlichkeitsrecht aufbauen. Dieses in Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG verortete Grundrecht wird in dieser Entscheidung in Richtung eines »Datenschutzgrundrechts« weiterentwickelt. Das Urteil enthält die angesichts der seinerzeitigen technischen Möglichkeiten extrem hell- und weitsichtige Aussage, unter den Bedingungen der automatisierten Datenverarbeitung gebe es kein belangloses Datum mehr. Das erweitert den Anwendungsbereich des Datenschutzrechts potentiell enorm. Aufbauend auf eine bereits 1971 in einem Gutachten entwickelte Figur[30] wird das »Recht auf informationelle Selbstbestimmung« als Sonderfall des Persönlichkeitsschutzes bestimmt. Dabei wird der Schutz normativ denkbar hoch aufgehängt: Das Gericht hält ein staatliches Vorgehen, das den Menschen in seiner ganzen Persönlichkeit, und sei es anonym im Rahmen einer statistischen Erhebung, zwangsweise registrierte und katalogisierte, für menschenwürdeverletzend. Denn dies bedeutete, Menschen wie Sachen zu behandeln, die in jeder Hinsicht einer Bestandsaufnahme zugänglich sind.[31] Diesseits dieser Extremkonstellation sind indes Rechtfertigungen von Eingriffen denkbar, insbesondere auf Basis einer informierten Einwilligung der Betroffenen. Damit erhält die Befugnis des Einzelnen, über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen, eine grundrechtliche Basis – zugleich wird eine bestimmte verfassungsrechtsfundierte Konstruktion geschaffen, die Individuen sowohl berechtigt wie fordert. Für die Ebene der Europäischen Union existiert insoweit sogar eine ausdrückliche Bestimmung: Artikel 8 der Charta der Grundrechte der Europäischen Union garantiert

28 Vgl. Art. 25 DS-GVO; siehe näher etwa Klingbeil/Kohm 2021 m.w.N.; Cavoukian 2011; van Rest u.a. 2014; Waldman 2020; vgl. dazu auch Bull 2015, S 86 ff.; Hansen 2019, Rn. 5 ff. m.w.N.

29 BVerfGE 150, 1 ff.; siehe dazu und zu nachfolgenden Entscheidungen ausführlich Schöndorf-Haubold (2020), S. 75 ff.

30 Steinmüller 1971; vgl. umfassend Albers 2005.

31 Ein aktuelles Buch fasst diesen (gerade nicht mehr nur oder vorrangig den Staat betreffenden) Zustand sehr drastisch mit dem Begriff der »Datensklaven« zusammen, siehe Caspar 2023.

ausdrücklich den Schutz personenbezogener Daten als ein im europäischen Recht verankertes Grundrecht.[32] Demgegenüber erfasst die Europäische Menschenrechtskonvention den Datenschutz nur über die entsprechende Auslegung des Art. 8 (Achtung des Privat- und Familienlebens, der Wohnung und der Korrespondenz); völkerrechtlich relevant ist ferner das 1981 vom Europarat, der völkerrechtlichen Organisation der europäischen Staaten, verabschiedete, 1985 in Kraft getretene und 2018 um ein Protokoll ergänzte Europäische Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten.

III. Verantwortung als Schlüsselbegriff moderner Regulierungsregime

Als »folgenbasiertes Legitimationskonzept« beschreibt Verantwortung eine prinzipiell hochabstrakte, unterschiedlich auszubuchstabierende normative Zurechnungsstrategie. Im Kontext des Datenschutzes erfolgt insoweit derzeit eine spezifische Komplexitätsreduktion, die klare Vorteile bietet, aber auch Fragen aufwirft. Denn mehr oder weniger klar ausgesprochen liegt den benannten Regelungsbemühungen ein eher schlichtes Modell zugrunde, demzufolge für das Datenschutzrecht primär die sogenannten personenbezogenen Daten relevant sind, für die infolge der konkreten Zuordnung zu einer Person dann eine einseitige Verantwortungszuweisung vorgenommen werden kann: »Meine Daten gehören mir!« bedeutet dann eben auch, dass nur bzw. jedenfalls in allererster Linie ich die Verantwortung für diese Daten trage. Diese personale Einseitigkeit verleiht den entsprechenden Verantwortungszuweisungen eine vergleichsweise große Klarheit und Dauer. Das erinnert an die alte, dem Grimm'schen Wörterbuch zu entnehmende Beschreibung von Verantwortung als »Zustand der Verantwortlichkeit«; denn dieses Begriffsverständnis deutet auf eine für charakteristisch erachtete Stabilität dieser Zuschreibung. Indes wird ein solches Verständnis unter den Bedingungen moderner, vielfältig vernetzter Gesellschaften[33] herausgefordert, weil der Vorstellung eindeutig feststehender Verantwortung zunehmend das Bewusstsein für

32 Siehe dazu etwa I. Augsberg 2015, Rn. 1 ff. m.w.N.

33 Dazu im vorliegenden Zusammenhang statt vieler Ladeur 2015.

unvermeidbare Interaktionen, Interdependenzen und hieraus resultierende Verantwortungsverflechtungen entgegenzuhalten ist. Dies gilt zumal unter den Bedingungen der Digitalisierung, denn dieser – notorisch unscharf bestimmte – Kontext bedingt neue Unklarheiten hinsichtlich konkreter Handlungsbeiträge und Ursachenzusammenhänge. Damit werden die, in unübersichtlichen modernen Gesellschaftsverhältnissen ohnehin zunehmend unwahrscheinlichen, eindeutigen Zuweisungen zusätzlich erschwert bis verunmöglicht. Erhellend wirkt in diesem Zusammenhang zunächst ein doppelter Seitenblick auf verwaltungsrechtswissenschaftliche und ethische Debatten, bevor ein Argument für ein dynamisiertes und komplexeres, Verantwortung aus klassischen Subjektmodellen lösendes Konzept entwickelt werden kann.

1. Verantwortungsverständnisse und -ebenen im Verwaltungsrecht

Der Begriff der Verantwortung ist aus den aktuellen Regulierungsdebatten nicht wegzudenken und prägt zumal das Verwaltungsrecht.[34] Zugleich handelt es sich um einen Schlüssel- und Brückenbegriff, der in spezifischer Weise in seiner rechtlichen Relevanz betrachtet und von parallelen, etwa philosophischen,[35] Begriffsverständnissen abgegrenzt werden sollte. Neben unterschiedlichen Verantwortungsbegriffen und -modellen sind indes auch unterschiedliche Verantwortungsebenen in den Blick zu nehmen: namentlich ist eine individuelle von einer kollektiven und eine einzelfallbezogene von einer systemischen Verantwortung zu unterscheiden. Für das Recht und die Rechtswissenschaft ist ferner die Erkenntnis entscheidend, dass in Mehrebenensystemen – etwa Bundesstaaten oder der Europäischen Union – nahezu zwangsläufig eine größere Vielzahl (potentiell) Verantwortlicher zu berücksichtigen sind. Um Verantwortungsdiffusion und einen möglichen Zustand der pluralen Nichtverantwortlichkeit zu vermeiden, bedarf es deshalb abgrenzender Regularien, die allerdings die Dynamik der entsprechenden Systeme mitberücksichtigen müssen.

34 Vgl. nur Klement 2006, passim; Ladeur 2016b, S. 35 ff.
35 Vgl. bspw. Heidbrink 2003.

2. Multiakteursverantwortung

In einem durchaus vergleichbaren Sinn wird das Verantwortungsproblem auch in ethischen Debatten behandelt. Demnach lässt sich der Verantwortungsdiskurs praxis- und regulierungsorientiert knapp dahingehend zusammenfassen, dass Verantwortung nicht naturwüchsig besteht, sondern normativ zugewiesen wird und genau deshalb typischerweise nicht einzelnen Akteuren zugeordnet werden kann. Stattdessen gilt es, die unterschiedlichen Verantwortlichkeiten multipler Akteure herauszuarbeiten und auf dieser Basis eine Multiakteursverantwortung zu begründen. Eine einseitige Verantwortungszuweisung ist demnach zwar nicht pauschal ausgeschlossen, verfehlt aber die komplexen Zusammenhänge der Lebenswelt und ist damit auch weniger geeignet, die erforderliche Praxiseignung, Relevanz und Akzeptanz zu garantieren. Demgegenüber bleibt das Konzept der Multiakteursverantwortung zwar vordergründig zunächst etwas unterbestimmt. Es kann aber gerade aufgrund dieser Vagheit mit Blick auf konkrete Anwendungsszenarien – etwa den Umgang mit Big Data im Gesundheitswesen oder mit klimaschutzbezogenen Maßnahmen[36] – näher bestimmt und entfaltet werden.

3. Verantwortung als transsubjektives, fluides Konstrukt

Die damit angedeuteten Erkenntnisse hinsichtlich der Pluralität, Ausdifferenziertheit und Entwicklungsoffenheit von Verantwortung können mit Blick auf den Datenschutz bereichsbezogen ergänzt und weiterentwickelt werden. Verantwortung setzt herkömmlich am Subjektstatus an. Genau dieser erfährt aber in digitalen Szenarien eine neue, durchaus widersprüchliche Weiterentwicklung: Der Möglichkeit massiv konkretisierender Zuspitzung korrespondiert eine *cog in the machine*-Logik, die den Einzelnen weniger als Person denn als Akkumulation von Daten erfasst, die ihrerseits nur in größeren Zusammenhängen interessante Einsichten ermöglichen. Hinzu treten KI-induzierte Infragestellungen klassischer Personalitäts- und Subjektverständnisse. Besonders anschaulich wird dies am Beispiel der sog. digitalen Zwillinge, die sich durch die Gleichzeitigkeit von Übereinstimmung und Differenz gegenüber der zugrunde liegenden realen Person

36 Vgl. einerseits Deutscher Ethikrat 2017 und andererseits Deutscher Ethikrat 2024.

auszeichnen.[37] Problemabspannend wirken könnte mit Blick auf die damit nur angedeuteten neuen Herausforderungen nicht so sehr ein pauschaler Abschied vom Verantwortungsbegriff als vielmehr dessen kontinuierliche Weiterentwicklung. Dabei ist namentlich der Vielfalt potentiell Beteiligter Rechnung zu tragen und Subjektivität kontextbezogen und responsiv zu konstruieren. Dass der Verantwortung, so verstanden, »immer ein Unmaß und eine Unabsehbarkeit eingeschrieben bleibt«[38], ist dann Stärke, nicht Schwäche des Konzepts.

IV. Subjektivierung der Daten und/oder Entsubjektivierung des Datenschutzrechts?

Die visionäre Innovationskraft, die mit dem Volkszählungsurteil verbunden ist, hat dafür gesorgt, dass die in ihm niedergelegten normativen Grundannahmen vergleichsweise gut »gealtert« sind. Das ist in einem Regelungsbereich, der durch eine erhebliche technologische Entwicklungsgeschwindigkeit gekennzeichnet ist, alles andere als selbstverständlich. Allgemein gilt, dass die frühen gerichtlichen wie gesetzgeberischen Vorgaben zum Datenschutz angesichts kaum präzise prognostizierbarer neuer Risiken zwar erstaunlich zukunftsgerichtet, entwicklungsoffen und gelungen erscheinen. Dennoch kommt man heute nicht umhin, in vielen auch aktuellen Regelungen – etwa der DSGVO – einen (weiterhin) der Entstehungszeit des Datenschutzrechts verhafteten Regelungsansatz zu identifizieren. Gerade der an sich gut nachvollziehbare Versuch, technologieneutrale und damit adaptive Vorschriften zu formulieren, führt dazu, dass die zunehmende Komplexität der modernen Datenverarbeitung rechtliche Neubewertungen erforderlich macht – das betrifft selbst früher kaum problematisierte Rechtsbegriffe wie den »Personenbezug«.[39] Noch weitergehend kann grundlegend gefragt werden, wie gut das herkömmliche Datenschutzrecht auf die Herausforderungen durch die Digitalisierung und die eng mit ihr verbundenen Entwicklungen im Bereich von »Big Data« und Künstlicher Intelligenz vorbereitet ist.[40] Insbesondere die beiden letztge-

37 Siehe Gruber/Zihlmann in diesem Band.
38 So in anderem Kontext treffend Flatscher 2016, S. 160.
39 Vgl. dazu Buchheim/Augsberg 2024.
40 Vgl. zum folgenden schon Deutscher Ethikrat 2017, S. 128 ff. m.w.N.

nannten, in sich selbstredend hochkomplexen, Aspekte sind ersichtlich mit einem erheblichen Konfliktpotential verbunden. Denn sie stehen stellvertretend für einen »Datenhunger« der modernen Gesellschaft, der einerseits kritisch zu hinterfragen, andererseits aber nicht wegzudenkende Funktionsbedingung zahlreicher moderner Errungenschaften und zukünftiger Optionen ist.[41] Wer beispielsweise das erkenntnistheoretische Potential von Big Data effektiv nutzen will, kann nicht länger vorbehaltlos auf einem klar vorherbestimmten Verwendungszweck bestehen oder eine rigide Befolgung des Prinzips der Datensparsamkeit bzw. Datenminimierung verlangen.[42]

Gleichzeitig ist nicht von der Hand zu weisen, dass sich datenschutzbezogene Empfindlichkeiten ändern können: Für eine Generation, die mit oft freizügiger Selbstpräsentation in sozialen Netzwerken aufgewachsen ist und für die das »Bezahlen« mit eigenen Daten einen selbstverständlichen Bestandteil der Netzökonomie bildet, sind die traditionell starken Bedenken ersichtlich nicht immer nachvollziehbar oder überzeugend. Allerdings wäre es ein fataler Irrtum, anzunehmen, dass die Gefahren geringer geworden wären – eher ist das Gegenteil der Fall. Angesichts massiver Machtasymmetrien im Verhältnis insbesondere zwischen einzelnen Individuen und großen (Internet-)Konzernen sowie der zunehmenden Möglichkeiten, selbst intimste Aspekte aus Datenspuren herauszulesen, sind persönlichkeits- wie freiheitsrelevante Beeinträchtigungen sogar wahrscheinlicher denn je. Gerade mit Blick auf die Relevanz sozialer Medien und die damit verbundenen Manipulationsmöglichkeiten wächst zudem das Bewusstsein dafür, dass der Datenschutz auch dazu dient, ein adäquates Funktionieren der demokratischen Meinungsbildungs- und Entscheidungsprozesse abzusichern.[43]

Angesichts dieser hier nur angedeuteten Prozesse der technischen wie sozialen Evolution und Disruption ist offenkundig, dass eine Weiterentwicklung des datenschutzrechtlichen Kontroll- und Schutzkonzepts nicht nur eine Möglichkeit, sondern eine Notwendigkeit ist. Das verweist zunächst auf die zuständigen demokratischen Instanzen, also die nationalen wie supranationalen Gesetzgebungsorgane. Den möglichen gesetzlichen Festlegungen wird dabei durch das Verfassungsrecht kein allzu enger Rahmen vorgegeben: Das insoweit grundlegende Recht auf informationelle Selbstbestimmung zählt nicht zu den klassischen Grundrechten. Es ist vielmehr,

41 Siehe Pfeiffer in diesem Band.

42 Siehe dazu schon Ladeur 2016a.

43 Vgl. dazu etwa Zimmermann 2021; Pieper 2019; siehe auch Deutscher Ethikrat 2023, S. 252 ff.

wie gezeigt, als kreative interpretative Weiterentwicklung des Persönlichkeitsrechts durch das Bundesverfassungsgericht »erfunden« worden. Das kann konstruktiv aus rechtstheoretischer Perspektive kritisiert werden.[44] Es verdeutlicht aber in jedem Fall, dass Grundrechte »in die Zeit hinein« zu verstehen sind, keine unumstößlichen und unveränderlichen Weisheiten abbilden, sondern ihrerseits den gesellschaftlichen Anforderungen angepasst werden können und sollen. Die »normative Kraft der Verfassung«[45] erweist sich so gerade in ihrer Fähigkeit, auf lebensweltliche Veränderungen und daraus resultierende neuartige Herausforderungen und Gefährdungen zu reagieren.[46] Prägnante Beispiele liefert insbesondere die Rechtsprechung des Bundesverfassungsgerichts. Indes handelt es sich hierbei nicht um ein exklusiv dem Verfassungsgericht vorbehaltenes Privileg. Vielmehr ist auch der Gesetzgeber als »Erstinterpret« der Grundrechte[47] und in der »offenen Gesellschaft der Verfassungsinterpreten«[48] letztlich jeder einzelne Bürger zu entsprechenden Auslegungsvorschlägen berechtigt.

1. Wen (oder was) schützt das Datenschutzrecht?

Schon mit Blick auf das Verantwortungskonzept kann, wie gezeigt, eine gewisse Lösung vom Subjekt empfohlen werden. Diese Überlegung ist für den konkreten Anwendungsbereich des Datenschutzes bzw. des Zugangs zu Daten und den hierfür erforderlichen Regeln näher zu entfalten. Dabei ist selbstredend zuzugestehen, dass es das vorhandene Datenschutzrecht in seiner Komplexität verkannte, wenn man es pauschal nur auf die radikalen Alternativen individualbezogen/kollektivistisch herunterbräche. Stattdessen enthält schon das geltende Recht eine Reihe kompromisshafter Bestimmungen und Erlaubnistatbestände, die dem übergreifenden Interesse an Datennutzung Rechnung tragen, etwa mit Blick auf die privilegierte Sekundär- und Tertiärnutzung von Daten. Dennoch bleibt die individuelle Einwilligung konzeptionell wie rechtspraktisch der wichtigste Rechtfertigungsgrund. Gleichzeitig erscheint der Datenzugang als Zielsetzung einer

44 Vgl. jüngst Behrendt 2023.
45 Hesse 1959.
46 Vgl. allgemein zum Konzept des learning law Luhmann 1983, S. 208 ff.; Ladeur 1995, S. 103 ff.; Calliess 1999, S. 121 f.
47 Dazu umfassend Jestaedt 1999.
48 Grundlegend Häberle 1975; siehe auch Höfling 1987.

Reihe neuerer Gesetzgebungsvorhaben. Das verweist jedenfalls rechtspolitisch auf ein als unzureichend erachtetes kurrentes Datennutzungsregime und kann damit im vorliegenden Sinne auf einen tieferliegenden Konstruktionsfehler des Rechts des Datenschutzes/Datenzugangs verstanden werden.

Herkömmlichem Verständnis entsprechend ist der Begriff »Datenschutz« im Prinzip ein *misnomer*, weil Schutzsubjekt gerade nicht die – in diesem Sinne gar nicht subjektfähigen – Daten, sondern die mit ihnen in Verbindung gesetzten Datengeber sind. Statt von einem »Schutz personenbezogener Daten« wäre deshalb präziser von einem »Schutz datenrelevanter Personen« zu sprechen. Denn die zumindest leicht »schiefe« Bezugnahme auf die Daten kreiert eine Reihe von Problemen, weil deren genaue Zuordnung der Daten schon im Regelfall keineswegs einfach ist. Erst recht gilt dies für die zahlreichen, fast zwangsläufig Zugehörigkeiten verschleiernden Verfahren der Verbreitung, Nutzung und Weiterverarbeitung von Daten. Instruktiv wirken können insoweit die Erkenntnisse aus der Diskussion über ein »Dateneigentum«.[49] Gerade dass diese zwischenzeitlich relativ intensiv geführte Debatte im Ergebnis weitgehend fruchtlos geblieben ist, verdeutlicht, wie schwierig eine entsprechend eindeutige und dauerhafte Zuordnung ist. Dies ließe sich weiterentwickeln zu der Fragestellung, ob dem »Datenschutz« nicht eine eigene Logik zugrunde liegt, weil es eben tatsächlich die Daten selbst sind, die schutzbedürftig sind (oder auch nicht).

2. Lehren aus der objektiven und der kollektiven Dimension der Grundrechte

Grundrechte werden traditionell vor allem als Freiheits- oder Abwehrrechte des Einzelnen gegen den Staat verstanden. Obwohl schon früh die »Gemeinschaftsbezogenheit und Gemeinschaftsgebundenheit der Person«[50] (an)erkannt worden ist, steht in einer solchen klassischen Betrachtungsweise eindeutig das Individuum im Zentrum der grundrechtsdogmatischen Aufmerksamkeit. Das erweist sich etwa an der weiterhin großen Relevanz der Statuslehre Georg Jellineks. Dabei muss diese – wie alle wissenschaftlichen Leistungen – selbstverständlich aus ihrer Entstehungsgeschichte

49 Vgl. statt vieler Thouvenin 2017.
50 BVerfGE 4, 7 (15 f.).

und ihrem historischen Hintergrund heraus gelesen werden. Sie bildet deshalb zunächst ein spezifisches, im Übergang von der Monarchie zur Demokratie entwickeltes (Grund-)Rechtsverständnis ab. Sie übernimmt die für die Rechtswissenschaft des Kaiserreichs charakteristischen Elemente der formalisierten, begriffs- und systematikfixierten Jurisprudenz.[51] Dementsprechend fokussiert und thematisiert sie den Einzelnen v.a. mit Blick auf seine Beziehung zum Staat;[52] sie vernachlässigt hingegen andere, für die moderne Gesellschaft mindestens ähnlich relevante Aspekte: Kollektive Interaktionen, insbesondere organisations- und verfahrensbezogene Grundrechtswirkungen, sind nicht ihr Thema. Mit ihrer Betonung des Individuums und seiner Stellung zum Staat steht sie vielmehr gerade in der Tradition einer Abkehr von klassischen Kollektivierungszwängen (Zünfte u.ä.), und sie liefert damit durchaus eine angemessene Grundrechtsdogmatik für die vergleichsweise stratifizierte Gesellschaftsstruktur der Jahrhundertwende. Versteht man demgegenüber Grundrechte als Teil eines sozialen Verständigungsprozesses, der gerade auch der Integration heterogen zusammengesetzter, durch plurale Zugehörigkeiten gekennzeichneter und in starkem Wandel befindlicher Gesellschaften[53] dient, dann bedarf es anstelle eines »statischen« eines stärker dynamisierten und pluralisierten, auf Wechselwirkungen und Kodependenzen eingestellten Grundrechtsverständnisses. Eine solche Konzeption könnte es auch erleichtern, intrapersonale und intertemporale Konflikte leichter zu integrieren und mit multiplen, tendenziell widersprüchlichen und unterschiedliche Reflexionsgrade abbildenden Willensäußerungen umzugehen.

Offensichtlich entspricht nämlich eine gleichermaßen individualistische wie etatistische Engführung schon lange nicht mehr der normativen wie gesellschaftlichen Bedeutung der Grundrechte: sie wirken auch als Leistungs- insbesondere Schutzansprüche, unterstützen den demokratischen Willensbildungsprozess, sichern privatrechtliche Institute (etwa die Ehe oder das Eigentum) und öffentlich-rechtliche Institutionen (wie den öffentlich-rechtlichen Rundfunk) ab und wirken zunehmend – vermittelt über Vorschriften des einfachen Gesetzesrechts – auch in Rechtsverhält-

51 Vgl. dazu, insbesondere zum Verhältnis zu Carl Friedrich v. Gerber: Kersten 2000, S. 50 ff. Zur Systemorientierung des deutschen (Verwaltungs-)Rechts aufschlussreich Hilbert 2015.

52 Deutlich Jellinek 1905, S. 82: »Ein Wesen wird zur Persönlichkeit, zum Rechtssubjekt erhoben in erster Linie dadurch, dass der Staat ihm die Fähigkeit zuerkennt, seinen Rechtsschutz wirksam anzurufen. Der Staat schafft daher die Persönlichkeit.«

53 Vgl. hierzu m.w.N. S. Augsberg 2013, S. 30 ff.

nisse zwischen Privaten ein. Grundrechte sind damit zwar in erster Linie, aber keineswegs nur in einer subjektivrechtlichen Dimension zu verstehen. Auch die Grundrechtsdogmatik hat sich in der jüngeren Vergangenheit von der starken Konzentration auf das traditionelle Staat-Bürger-Subordinationsverhältnis, also auf hoheitliche Freiheitsbeschränkungen und abwehrrechtliche Gegenreaktionen, entfernt und ist in Richtung einer umfassenderen Betrachtung der wechselseitigen Bindungen, Verfaltungen und Wechselwirkungen in einer komplexen und pluralistischen Gesellschaft weiterentwickelt worden.[54]

Folgerichtig bleiben Grundrechte nicht auf die Ebene des Individuums begrenzt, sondern lassen sich (auch) als »Phänomene kollektiver Ordnung« lesen.[55] Mit Blick auf wirtschaftliche Zusammenhänge verweist dies etwa auf die Frage, ob und inwieweit sich ein derartiges, auf Spezialisierung und Arbeitsteilung angewiesenes sowie durch zahlreiche (auch) kollektive Interdependenzen gekennzeichnetes organisiertes Wirtschaftssystem mit einem allein oder doch primär individualistisch ausgerichteten Grundrechtsverständnis verträgt bzw. ob letzteres nicht ohnehin nur um den Preis zu haben ist, bestimmte normative und faktische Realitäten auszublenden. Denn selbst dort, wo im Sinne einer *zero-contribution-thesis* kollektive Kooperationen und Ergebnisse letztlich allein auf handfeste Einzelinteressen zurückgeführt werden,[56] kann doch die Einbettung des Individuums in ein sozioökonomisches Gesamtgefüge nicht in Frage gestellt werden. Namentlich mit Blick auf das gegenwärtige, in hohem Maße arbeitsteilig organisierte Wirtschaftsleben erscheint die Existenz zahlreicher Kodependenzen[57] und die hieraus resultierende Bedeutung kollektiver Akteure und Aktionen evident. Eine deutliche Kollektivorientierung ist aber nicht nur mittels einer primär produktionsorientierten, sondern auch in einer (durchaus klassischen[58]) konsumorientierten Betrachtung zu gewinnen. Denn in marktwirtschaftlichen Konstellationen steht eben nicht der einzelne Kunde bzw. Abnehmer im Mittelpunkt, sondern die Vielzahl potentieller Konsumenten.[59] Dieses basale Verständnis der Wirtschafts- als Kollek-

54 Zu diesem polyzentrischen Ansatz und einer Kritik daran vgl. Lindner 2005, S. 430 ff.

55 So der Titel eines 2014 von Thomas Vesting, Stefan Korioth und Ino Augsberg herausgegebenen Bandes.

56 Vgl. Olson 1968, S. 18 ff.

57 Vgl. aus ökonomischer Perspektive nur Becker 1993.

58 Vgl. etwa zu Adam Smith: Streissler 2012, S. 3 ff.

59 Zu diesen siehe etwa Becker/Michael 1993.

tivordnung wird, zugegebenermaßen, im vorliegenden Zusammenhang vorausgesetzt, nicht hingegen ausführlicher begründet. Schon im Ausgangspunkt liefert es indes ein Indiz für einen gewissen Grundkonflikt: In diesem Sinne erscheint es angemessen, gängigen und vielleicht allzu eingängigen »radikalindividualistischen« Grundrechtsverständnissen[60] eine etwas anders orientierte, stärker auf (etwa) wirtschaftstypische, in den einschlägigen Verfassungsvorgaben angelegte oder doch von diesen vorausgesetzte Kollektivphänomene eingehende Perspektive entgegenzusetzen, bzw. an die Seite zu stellen.[61] Damit wird keineswegs das überkommene Modell individualbezogenen Grundrechtsschutzes schlicht überwunden. Stattdessen wird es ergänzt, bzw. es wird an eine eigentlich schon länger existierende zusätzliche Grundrechtsdimension erinnert (überindividuell, aber nicht postindividuell).

3. Anleihen beim Modell der »informationellen Freiheitsgestaltung«

Das für die datenschutzrechtlichen Stellungnahmen grundlegende Recht auf informationelle Selbstbestimmung zählt, wie erwähnt, nicht zu den klassischen Grundrechten, sondern ist eine kreative »Erfindung« des Bundesverfassungsgerichts. Hieran erweist sich die Dynamik und Innovationsfähigkeit auch dieses scheinbar besonders stabilen Rechtsbereichs. Es verdeutlicht zugleich, dass kontextbezogene Weiterentwicklungen nicht nur prinzipiell möglich, sondern sogar sinnvoll und unter Umständen nötig sind.

In diesem Sinne hat etwa der Deutsche Ethikrat 2017 in seiner Stellungnahme zu »Big Data und Gesundheit« ausdrücklich eine derartige Weiterentwicklung des Rechts auf informationelle Selbstbestimmung eingefordert: »Der Begriff der informationellen Freiheitsgestaltung entwickelt das Konzept der informationellen Selbstbestimmung weiter. Er gründet nicht in einem eigentumsanalogen Ausschlussrecht, sondern in der Befugnis, selbst zu bestimmen, mit welchen Inhalten jemand in Beziehung zu seiner Umwelt tritt. Informationelle Freiheitsgestaltung in diesem Sinne meint interaktive Persönlichkeitsentfaltung unter Wahrung von Privatheit

60 Vgl. bspw. Schäfer 2010. Von der »primären Bedeutung« der subjektiv-individualrechtlichen Grundrechtsdimension spricht etwa BVerfGE 50, 290 (337).

61 Siehe dazu näher S. Augsberg 2014.

in einer vernetzten Welt und ist gekennzeichnet durch die Möglichkeit, auf Basis persönlicher Präferenzen effektiv in den Strom persönlich relevanter Daten eingreifen zu können.«[62] Diesen Impuls zu evolutionärer Veränderung aufnehmend und weiterführend ist zu überlegen, ob nicht noch diese ihrerseits auf die individuelle Freiheitsgestaltung bezug nehmende Vorgehensweise für den konkreten Untersuchungsgegenstand zu eng ist. Denn dieser Freiheitsbezug impliziert letztlich doch wieder eine traditionelle Konzentration auf individuelle, gegenüber zumal staatlichen Begrenzungen schützenswerte Autonomieräume.[63] Letztere bleiben selbstredend wichtig. Aber ein gehaltvoller (Grund-)Rechtsschutz sollte sich nicht darin erschöpfen.

Allerdings reicht es unter Umständen nicht, in diesem Sinne lediglich die klassische datenschutzrechtliche Position evolutionär zur »Datensouveränität« fortzuschreiben.[64] Denn auch wenn man dieses Konzept gerade aufgrund seiner Vagheit und der daraus folgenden Variabilität für interessant und anschlussfähig hält,[65] handelt es im Grunde doch um eine recht konservative Position, weil und soweit sie der traditionellen Subjektorientierung verhaftet bleibt, bzw. diese Tendenz sogar eher noch verstärkt.

4. Sogenannte inpersonale Grundrechte als Inspirations- und Innovationsquelle

Will man hierüber hinausgehen, könnte ein älterer, aber keineswegs veralteter Theoriebaustein wichtige Hilfestellung leisten. Mit dem Begriff »inpersonale Grundrechte« bezeichnet *Helmut Ridder* Grundrechte, die keinen personalen Träger voraussetzen.[66] Ungeachtet der insoweit mindestens dürftigen textlichen Grundlage versteht er dieses Modell nicht als Novum. Vielmehr könne es normtextbezogen vor allem an der Sozialstaatsklausel des Grundgesetzes anknüpfen.[67] Ridder versucht darzulegen, dass und warum es sich hierbei nicht lediglich um einen Spezialfall, eine Ausnahme vom ansonsten weiterhin strikt personal gedachten Grundrechtsschutz handele.

62 Deutscher Ethikrat 2017, S. 40.
63 Vgl. dazu etwa Honneth 2013, S. 129 ff.
64 Vgl. Deutscher Ethikrat 2017.
65 Vgl. Augsberg/Gehring 2022.
66 Vgl. Ridder 1975, S. 86 f., 90. Siehe zum folgenden auch I. Augsberg 2024; Ladeur 2016b, S. 127 ff.
67 Vgl. Ridder 1975, S. 145.

Denn bei den inpersonalen Grundrechten lasse sich »leichter als bei den personalen Grundrechten erkennen, was indes in Wahrheit allen Grundrechten der Gesamtverfassung gemeinsam ist, nämlich daß sie auf die konkrete Freiheit eines sozialen Feldes durch dessen Organisation abzielen.«[68] Gerade durch die Lösung von der Person wird damit die Erkenntnis ermöglicht, dass im Mittelpunkt des Grundrechtsschutzes nicht das isolierte Individuum, sondern der Mensch als Gemeinschaftswesen steht. Ridders Konzept steht damit nicht in direkter Konkurrenz zu dem herkömmlichen, auch das deutsche Verfassungsrechtsdenken prägenden Modell primär personalindividualistischen Grundrechtsschutzes, zielt nicht auf dessen Abwicklung oder rechtspolitische Erweiterung. Stattdessen versucht er, einen blinden Fleck der traditionellen Grundrechtsdogmatik zu beschreiben und auszuleuchten. So verstanden, läßt sich *Ridders* Vorgehen durchaus produktiv auf das Problem des Datenzugangs anwenden: es verdeutlicht für dieses Beispiel, wie ungeachtet gängiger Präferenzen das Verfassungsrecht offener für Innovationen ist, als es mitunter den Anschein hat, bzw., dass Weiterentwicklungen nicht auf die verfassungsgerichtliche Entscheidungsfindung begrenzt sind.

5. Der »Personenbezug« als überdenkenswertes Merkmal

Klassische Begriffe und Schutzmechanismen des Datenschutzrechts werden durch immer weitergehende Vernetzungsmöglichkeiten, enorm gestiegene Rechenkapazitäten und damit ermöglichte Deanonymisierungstechniken unter Druck gesetzt.[69] Deutlich wird dieses Problem zumal im Kontext neuer technischer Formen, Modelle und Instrumente der Datenanalyse. Es betrifft nicht nur Einzelphänomene, sondern sogar den für das herkömmliche Datenschutzmodell nahezu konstitutiven, jedenfalls als zentrales Anwendungskriterium fungierende Personenbezug der Daten. Anstatt an dieser Stelle darauf zu beharren, in ganz anderem Kontext entwickelte Konzepte schlicht auszubauen, sollte man – durchaus im Sinne des ursprünglichen, kreativen Geists des Datenschutzrechts – nach neuen Regelungsmodi und Instrumenten suchen, die den weiterhin, bzw. gerade heute gebotenen wirksamen Schutz der mit Daten verbundenen informa-

68 Ridder 1975, S. 91.
69 Vgl. etwa Sarunski 2016.

torischen Abschirmungsinteressen mit sinnvollen Nutzungsmöglichkeiten verbinden.[70] Dabei können technische Weiterentwicklungen dazu beitragen, althergebrachte Elemente nicht nur in Frage zu stellen, sondern sie so weiterzuentwickeln, dass sich die ursprünglich mit ihnen verbundenen Intentionen reaktualisieren lassen. Das lässt sich am besten anhand eines konkreten Konzepts, nämlich der »transaktionsbasierten Datentreuhand«, veranschaulichen. Bei dieser neuen und komplexen Form gemeinsamer Datennutzung[71] stellt sich die Frage, ob überhaupt personenbezogene Datenverarbeitungen (im klassischen Sinn) stattfinden und inwieweit somit die dabei involvierten Vorgänge den traditionellen Schutzintentionen und Bindungen des Datenschutzrechts unterfallen.[72]

V. Gestaltungsverantwortung und Verantwortungsgestaltung

Ersichtlich ist damit nun die Frage, wer für die Gewährung oder Begrenzung von Datenzugängen verantwortlich zeichnen soll, nicht beantwortet. Immerhin lässt sich aber aus dem Vorgesagten doch die Einsicht ableiten, dass diese Verantwortungsdimension etwas ist, das seinerseits nicht als unverrückbar vorgegeben, sondern als Teil des gestaltbaren Gesamtrahmens einzuordnen ist. Das mit den Beiträgen dieses Bandes fortgeführte Nachdenken über Datenzugänge, ihre Voraussetzungen, Grenzen und Konsequenzen verweist damit einerseits auf über- und tiefgreifende Debatten und wird von diesen inspiriert. Es kann andererseits diese allgemeineren Überlegungen anreichern und konkretisieren.

Dabei geht es nicht um ein bloßes innerakademisches Glasperlenspiel, sondern um eine gesellschaftlich hochrelevante und aktuell brisante Fragestellung. Derzeit ist sowohl in öffentlichen Diskussionen als auch in konkreten Rechtsetzungsprojekten eine Akzentverschiebung zu beobachten: wo früher vor allem die Gefahren der Datenverbreitung betont wurden, wird jetzt vermehrt auf das produktive Potential und die ökonomischen wie sozialen Chancen der Datennutzung hingewiesen. In diesem Sinne stellt die DSGVO gewissermaßen einen letzten Höhepunkt einer traditionellen Datenschutzperspektive dar. Mit ihr war es gelungen, dem gerade

70 Ähnlich, aber mit Blick auf andere Instrumentarien Bull 2015, S. 77 ff., 113 ff.
71 Zur Funktionsweise siehe näher Buchheim/Gehring/Augsberg 2023.
72 Dazu jetzt Buchheim/Augsberg 2024, 365 ff.

in Deutschland wichtigen und stark emotional besetzten – und bisweilen, etwa im Kontext der Coronapandemie, durchaus problematisch als nahezu sakrosankt behandelten – Thema Datenschutz auch auf der europäischen Ebene noch größere Relevanz zu verschaffen. Von Anfang an wurde indes kritisiert, die DSGVO perpetuiere herkömmliche datenschutzrechtliche Prinzipien, namentlich den Grundsatz der engen Zweckbindung und der Datensparsamkeit, obwohl es angesichts der veränderten Bedingungen einer »Big-Data-Welt« nicht nur ineffektiv, sondern potentiell paralysierend und kontraproduktiv sei, diese weiterhin und weitgehend unverändert heranzuziehen. Über diese an Einzelinstrumenten ansetzende Kritik gehen indes die derzeitig insbesondere auf europäischer Ebene entwickelten Rechtsakte und Initiativen hinaus, die den Fokus nicht so sehr auf den von Datennutzung ausgehenden Gefahren, sondern auf ihr ökonomisches und soziales Potential legen. Sowohl die neuen Regelungen zur KI als auch und insbesondere der Digital Markets Act[73] sowie der Data Governance Act fokussieren eher die Chancen als die Risiken einer neuen Datenwirtschaft.[74] Ähnliches gilt bereichsbezogen für ambitionierte, in ihren konkreten Auswirkungen noch nicht abschließend einschätzbare Projekte wie den einheitlichen European Health Data Space.[75] Obwohl dabei routinemäßig hervorgehoben wird, die neuen Vorschläge entsprächen den Vorgaben der DSGVO und nutzten lediglich die Gestaltungs- und Interpretationsspielräumen, die diese bewusst enthält, ist doch unverkennbar, dass hier jedenfalls eine Schwerpunktverlagerung erfolgt.

In diese stärker chancenorientierte Richtung lässt sich auch die kürzlich von der Bundesregierung präsentierte »Digitalstrategie Deutschland« einordnen. Dieser »Wegweiser für den digitalen Aufbruch« liest sich in weiten Teilen wie ein digitales Wünsch-Dir-was. Er muss selbstredend als politisches Statement und nicht als konkretes Rechtsdokument verstanden werden. Gleichwohl fällt auf, wie sehr gerade im Bereich der Daten deren produktives Integrations- und Innovationspotential in den Vordergrund gerückt wird. So werden beispielsweise die bei Behörden vorhandenen Daten – über die bestehenden informations(weiterverwendungs)rechtlichen Vorgaben hinausgehend – im Sinne eines umfassenden, als Rechtsanspruch verstandenen Open-Data-Konzepts vorgestellt. Daten sollen zudem nicht

73 Siehe Pfeiffer in diesem Band.

74 Zu den dabei vorfindlichen Subjektvorstellungen siehe Schweitzer/Brieske in diesem Band.

75 Siehe Riechert/Böning in diesem Band. Vgl. etwa Raji 2023.

länger auf »einzelnen einsamen Dateninseln« verbleiben, sondern auf Basis einer entsprechenden Nutzungsstrategie standardisiert und miteinander verbunden werden. Praktisch bedeutsam dürfte dabei insbesondere die Weiterentwicklung der europäischen vernetzten Infrastruktur Gaia-X werden. Konkrete Relevanz erhält die Fokusverschiebung aber auch im Rahmen der rechtlichen Ausgestaltung des unionalen Data Acts, des jüngst verabschiedeten Gesundheitsdatennutzungsgesetzes und des zumindest angekündigten nationalen Forschungsdatengesetzes. Inwieweit sich diese relativ weitreichenden Pläne tatsächlich praktisch umsetzen lassen, bleibt abzuwarten. Manches stimmt skeptisch, etwa der optimistische Verweis auf Projekte wie die elektronische Patientenakte.[76] Jedenfalls aber dürften die anstehenden Veränderungen – gerade auch in ihrem Verhältnis zum klassischen Datenschutz – noch zahlreiche spannende (nicht nur) juristische Fragen aufwerfen.

Literatur

Albers, Marion (2005): *Informationelle Selbstbestimmung*, Baden-Baden.

Augsberg, Ino (2024): Was leistet das verfassungsrechtliche Konzept der »inpersonalen Grundrechte«?, in: Steffen Augsberg/Franz Reimer (Hg.): *Demokratie und Verfassung bei Helmut Ridder*, Baden-Baden [in Vorbereitung].

Augsberg, Ino (2021): *Theorien der Grund- und Menschenrechte*, Tübingen.

Augsberg, Ino (2015): GRC Art. 8, in: von der Groeben, Hans/Schwarze, Jürgen/Hatje, Armin (Hg.): *Europäisches Unionsrecht*, siebte Auflage, Baden-Baden.

Augsberg, Steffen (2022): Datenschutz, Datensouveränität, Data Governance: Überlappungen, Spannungen und mögliche Lerneffekte, in: Augsberg, Steffen/Petra Gehring (Hg.): *Datensouveränität. Positionen zur* Debatte, Frankfurt am Main, S. 121–133.

Augsberg, Steffen (2014): Das kollektive Moment der Wirtschaftsgrundrechte, in: Vesting, Thomas/ Korioth, Stefan/ Augsberg, Ino (Hg.): *Grundrechte als Phänomene kollektiver Ordnung. Zur Wiedergewinnung des Gesellschaftlichen in der Grundrechtstheorie und Grundrechtsdogmatik*, Tübingen, S. 161–182.

Augsberg, Steffen (2013): Gesellschaftlicher Wandel und Demokratie: Die Leistungsfähigkeit der parlamentarischen Demokratie unter Bedingungen komplexer Gesellschaften, in: Hans M. Heinig/Jörg P. Terhechte (Hg.): *Postnationale Demokratie, Postdemo-*

76 Dazu näher Niggemeier in diesem Band.

kratie, Neoetatismus. Wandel klassischer Demokratievorstellungen in der Rechtswissenschaft, S. 27–54.

Augsberg, Steffen/Gehring, Petra (2022): Datensouveränität als Diskursgegenstand: Ambiguität als Chance?, in: dies. (Hg.): *Datensouveränität. Positionen zur* Debatte, Frankfurt am Main, S. 7–17.

Austermühle, Gisa (2002): *Zur Entstehung und Entwicklung eines persönlichen Geheimsphärenschutzes vom Spätabsolutismus bis zur Gesetzgebung des Deutschen Reiches*, Berlin.

Barczak, Tristan (2023): Art. 2 Abs. 1, in: Dreier, Horst (Hg.): *Grundgesetz-Kommentar*, vierte Auflage, Tübingen.

Becker, Gary S. (1993): Eine Theorie sozialer Wechselwirkungen (1974), in: ders.: *Ökonomische Erklärung menschlichen Verhaltens*, zweite Auflage, S. 282–316.

Becker, Gary S./Michael, Robert T. (1993): Zur Neuen Theorie des Konsumentenverhaltens (1973), in: Gary S. Becker: *Ökonomische Erklärung menschlichen Verhaltens*, zweite Auflage, S. 145–166.

Behrendt, Svenja (2023): *Entzauberung des Rechts auf informationelle Selbstbestimmung. Eine Untersuchung zu den Grundlagen der Grundrechte*, Tübingen.

Bryde, Brun-Otto (2016): Verfassungsinterpretation und verfassungsgerichtliche Praxis, in: Franz Reimer (Hg.): *Juristische Methodenlehre aus dem Geist der Praxis?*, Baden-Baden, S. 107–116.

Buchheim, Johannes/Augsberg, Steffen (2024): Von der Verarbeitung personenbezogener Daten zur personenbezogenen Datenverarbeitung. Zugleich eine datenschutzrechtliche Erläuterung und Einordnung des Modells der transaktionsbasierten Datentreuhand, in: *Juristenzeitung* 79, Heft 9, S. 365–375.

Buchheim, Johannes/Augsberg, Steffen/Gehring, Petra (2023): Transaktionsbasierte Datentreuhand. Nutzungsszenarien, Kennzeichen und spezifische Leistungen eines neuen Modells gemeinsamer Datennutzung, in: *Juristenzeitung* 77, Heft 23, S. 1139–1147.

Bull, Hans Peter (2015): *Sinn und Unsinn des Datenschutzes. Persönlichkeitsrecht und Kommunikationsfreiheit in der digitalen Gesellschaft*, Tübingen.

Bull, Hans Peter (2011): *Informationelle Selbstbestimmung – Vision oder Illusion?*, zweite Auflage, Tübingen.

Calliess, Gralf Peter (1999): *Prozedurales Recht*, Baden-Baden.

Caspar, Johannes (2023): *Wir Datensklaven. Wege aus der digitalen Ausbeutung*, Berlin.

Cavoukian, Ann (2011): Privacy by Design: Origins, Meaning, and Prospects for Assuring Privacy and Trust in the Information Era, in: George O. M. Yee (Hg.): *Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards*, Hershey, S. 170–208.

Deutscher Ethikrat (2024): *Klimagerechtigkeit*, Berlin.

Deutscher Ethikrat (2023): *Mensch und Maschine – Herausforderungen durch Künstliche Intelligenz*, Berlin.

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

Di Martino, Alessandra (2005): *Datenschutz im europäischen Recht*, Baden-Baden.

Fischer-Lescano, Andreas/Franzki, Hannah/Horst, Johan (2018) (Hg.): *Gegenrechte. Recht jenseits des Subjekts*, Tübingen.

Flatscher, Matthias (2016): Was heißt Verantwortung? Zum alteritätsethischen Ansatz von Emmanuel Levinas und Jacques Derrida, in: *Zeitschrift für Praktische Philosophie* 3, Heft 1, S. 125–164.

Häberle, Peter (1975): Die offene Gesellschaft der Verfassungsinterpreten. Ein Beitrag zur pluralistischen und »prozessualen« Verfassungsinterpretation, in: *Juristenzeitung* 30, Heft 10, S. 297–305.

Hansen, Marit (2019): Art. 25 DSGVO, in: Simitis, Spiros/Hornung, Gerrit/Spiecker gen. Döhmann, Indra (Hg.): *Datenschutzrecht. DSGVO mit BDSG*, Baden-Baden.

Hardin, Garrett (1968): The Tragedy of the Commons, in: *Science* 162, Heft 3859, S. 1243–1248.

Heidbrink, Ludger (2003): *Kritik der Verantwortung. Zu den Grenzen verantwortlichen Handelns in komplexen Kontexten*, Weilerswist-Metternich.

Herrmann, Christoph (2010): *Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*, Lausanne.

Hesse, Konrad (1959): *Die normative Kraft der Verfassung*, Tübingen.

Hilbert, Patrick (2015): *Systemdenken in Verwaltungsrecht und Verwaltungsrechtswissenschaft*, Tübingen.

Höfling, Wolfram (1987): *Offene Grundrechtsinterpretation. Grundrechtsauslegung zwischen amtlichem Interpretationsmonopol und privater Konkretisierungskompetenz*, Berlin.

Honneth, Axel (2013): *Das Recht der Freiheit*, Frankfurt am Main.

Hornung, Gerrit/Spiecker gen. Döhmann, Indra (2019): in: Einleitung, in: Simitis, Spiros/Hornung, Gerrit/Spiecker gen. Döhmann, Indra (Hg.): *Datenschutzrecht. DSGVO mit BDSG*, Baden-Baden.

Jellinek, Georg (1905): *System der subjektiven öffentlichen Rechte*, zweite Auflage, Nachdruck 1963.

Jestaedt, Matthias (1999): *Grundrechtsentfaltung im Gesetz. Studien zur Interdependenz von Grundrechtsdogmatik und Rechtsgewinnungstheorie*, Tübingen.

Kersten, Jens (2000): *Georg Jellinek und die klassische Staatslehre*, Tübingen.

Klement, Jan Henrik (2006): *Verantwortung. Funktion und Legitimation eines Begriffs im Öffentlichen Recht*, Tübingen.

Klingbeil, Thilo/Kohm, Simon (2021): Datenschutzfreundliche Technikgestaltung und ihre vertraglichen Implikationen, in: *Multimedia und Recht* 24, Heft 1, S. 3–8.

Ladeur, Karl-Heinz (2016a): »Big Data« im Gesundheitsrecht – Ende der »Datensparsamkeit«?, in: *Datenschutz und Datensicherheit* 40, Heft 6, S. 360–364.

Ladeur, Karl-Heinz (2016b): *Recht – Wissen – Kultur. Die fragmentierte Ordnung*, Berlin.

Ladeur, Karl-Heinz (2015): Die Gesellschaft der Netzwerke und ihre Wissensordnung. Big Data, Datenschutz und die »relationale Persönlichkeit«, in: Florian Süssenguth (Hg.): *Die Gesellschaft der Daten. Über die digitale Transformation der sozialen Ordnung*, S. 225–252.

Ladeur, Karl-Heinz (2009): Das Recht auf informationelle Selbstbestimmung: Eine juristische Fehlkonstruktion?, in: *Die öffentliche Verwaltung*, Heft 2, S. 45–55.

Ladeur, Karl-Heinz (1995): *Postmoderne Rechtstheorie. Selbstreferenz – Selbstorganisation – Prozeduralisierung*, zweite Auflage, Berlin.

Lindner, Josef Franz (2005): *Theorie der Grundrechtsdogmatik*, Tübingen.

Luhmann, Niklas (1983): *Rechtssoziologie*, zweite Auflage, Opladen.

Neuroth, Benedikt Josef (2023): *Das Private in der Sicherheitsgesellschaft. Umstrittene Freiheitsrechte in den USA 1963–1977*, Paderborn.

Olson, Mancur (1968): *Die Logik des kollektiven Handelns. Kollektivgüter und die Theorie der Gruppen*, Tübingen.

Pieper, Niels (2019): *Der grundrechtliche Schutz des Kommunikationsraums. Präventive und repressive Informationseingriffe in der deliberativen Demokratie*, Baden-Baden.

Raji, Behrang (2023): Datenräume in der Europäischen Datenstrategie am Beispiel des European Health Data Space. Datenschutzrechtliche Implikationen, in: *Zeitschrift für Datenschutz* 13, Heft 1, S. 3–8.

Reimer, Franz (2020): *Juristische Methodenlehre*, zweite Auflage, Baden-Baden.

Ridder, Helmut (1975): *Die soziale Ordnung des Grundgesetzes. Leitfaden zu den Grundrechten einer demokratischen Verfassung*, Opladen.

Sarunski, Maik (2016): Big Data – Ende der Anonymität? Fragen aus Sicht der Datenschutzaufsichtsbehörde Mecklenburg-Vorpommern, in: *Datenschutz und Datensicherheit* 40, Heft 7, S. 424–427.

Schäfer, Jan Philipp (2010): Das Individuum als Grund und Grenze deutscher Staatlichkeit. Plädoyer für eine radikalindividualistische Konzeption der Menschenwürdegarantie des Grundgesetzes, in: *Archiv des öffentlichen Rechts* 135, Heft 3, S. 404–430.

Schöndorf-Haubold, Bettina (2020): *Das Recht auf Achtung des Privatlebens. Grundrechtsschutz in der Informationsgesellschaft*, München.

Steinmüller, Wilhelm (1971): *Grundfragen des Datenschutzes. Gutachten im Auftrag des Bundesministerium des Innern*, Bundestag Drucksache VI/3826, Berlin.

Streissler, Erich W. (2012): Einführung, in: Adam Smith: *Untersuchung über Wesen und Ursachen des Reichtums der Völker*, Tübingen, S. 1–31.

Thouvenin, Florent (2017): Wem gehören meine Daten? Zu Sinn und Nutzen einer Erweiterung des Eigentumsbegriffs, in: *Schweizerische Juristen-Zeitung* 113, Heft 2, S. 21–32.

Timmermann, Daniel (2019): Datenschutz im Wandel der Zeit. Eine Analyse der Entwicklung der Rechtstatsachen, des Rechtsrahmens und der Judikatur, in: *Die öffentliche Verwaltung*, Heft 7, S. 249–260.

Ulbricht, Max-R./Weber, Karsten (2017): Adieu Einwilligung? Neue Herausforderungen für die informationelle Selbstbestimmung im Angesicht von Big Data-Technologien, in: Friedewald/Lamla/Roßnagel (Hg.): *Informationelle Selbstbestimmung im digitalen Wandel*, Wiesbaden, S. 265–286.

van Rest, Jeroen/Boonstra, Daniel/Everts, Maarten/van Rijn, Martin/van Paassen, Ron (2014): Designing Privacy-by-Design, in: Bart Preneel/Demosthenes Ikonomou (Hg.): *Privacy Technologies and Policy*, Heidelberg, S. 55–72.

Vesting, Thomas (2021): *Gentleman, Manager, Homo Digitalis. Der Wandel der Rechtssubjektivität in der Moderne*, Weilerswist-Metternich.

Vesting, Thomas/ Korioth, Stefan/ Augsberg, Ino (2014) (Hg.): *Phänomene kollektiver Ordnung. Zur Wiedergewinnung des Gesellschaftlichen in der Grundrechtstheorie und Grundrechtsdogmatik*, Tübingen.

Waldman, Ari Ezra (2020): Data Protection by Design? A Critique of Article 25 of the GDPR, in: *Cornell International Law Journal* 53, Heft 1, S. 147–167.

Warren, Samuel D./Brandeis, Louis (1890): The Right to Privacy, in: *Harvard Law Review* 4, Heft 5, S. 193–220.

Westin, Alan (1967): *Privacy and Freedom*, New York.

Zimmermann, Sören (2021): *Datenschutz und Demokratie. Überlegungen zu einem reziproken Bedingungszusammenhang*, Baden-Baden.

Ausblick: Datenzugangsregulierung

Offene Wissenschaft versus Zeitenwende: Neue Dilemmata in Sachen (Forschungs)Datenzugang

Petra Gehring und Daniel Lambach

»Cyberspace consists of transactions, relationships, and thought itself, arrayed like a standing wave in the web of our communications« (Barlow 1996) – so hieß es im berühmten *Internet Manifesto*, das vor fast dreißig Jahren den digitalen Raum als eine Art körperloses, einer Regierung nicht bedürftiges Reich der Gedankenfreiheit entwarf. Tatsächlich haben Bildung und Wissenschaft sich dieses Ideal zu eigen gemacht. Sie stellten in den letzten Jahrzehnten geradezu *das* Paradigma für eine nach dem Willen (fast) aller Beteiligten weltweit »offene« Datennutzung dar.[1] Dank Digitalität schien ein zuvor unbekanntes Maß an niedrigschwellig zugänglichem, fairem und demokratischem Austausch zu entstehen. Global gemeinsame – und wohlmöglich sogar kostenlos zugängliche – Wissensräume schienen möglich zu werden. Vielleicht handelt es sich sogar um *das* Versprechen des Internetzeitalters: Menschen teilen künftig Informationen und Wissen als würde die ganze Menschheit in die Kollegialität innerwissenschaftlichen Kommunizierens integriert. Programmatiken wie *Open Access*, *Open Education*, *Open Science* und *Open Data* unterstreichen diese Gleichung: Digitale Wissenschaft und ihre Datenströme sind »offen« bzw. sollten bald- und weitestmöglich offen sein. Nicht nur Verlage, Lizenzierungen und die Publikationsfinanzierung stellen sich entsprechend um, sondern auch der Umgang mit Forschungsdaten folgt dem Leitbild der »Öffnung«.[2] Daten als Ressourcen der Forschungsprozesse selbst sollen also zugänglich gemacht werden – sei es als *Open Data*, sei es im

1 Die Interessen der Anbieter proprietärer Softwareprodukte sowie inzwischen damit verschmolzener Publikationsdienstleister zielen freilich auf eine Produktform sowohl von Content als auch von Code. Solche Anbieter haben sich auf das Thema »Offenheit« auf ihre ganz eigene Weise eingestellt, bleiben aber mindestens ein Thema für sich. Sie vermarkten inzwischen bei hinreichender Subventionierung Content als »offen« und haben die Gewinnung von Nutzungsdaten zum Zusatz- oder sogar Hauptgeschäft gemacht.

2 Vgl. den Beitrag von Petra Gehring zu Open Science in diesem Band.

Rahmen von stärker auf die Bedarfe wirtschaftlicher Sektoren zugeschnittenen sogenannten »Datenräumen«.[3]

Nicht erst seit der 2022 unter dem Schlagwort der »Zeitenwende« zusammengefassten globalen Polykrise haben sich die Töne in der Digitalpolitik nun aber verändert, und dies gerade auch dort, wo es um Wissenschaft geht. Stellungnahmen bringen zum Ausdruck, dass der russische Angriffskrieg in der Ukraine, die aggressive Außen- und Wirtschafspolitik seitens China sowie ein eskalierender Nahost-Konflikt, der in sich gespaltene muslimische Öffentlichkeiten und »den Westen« auseinandertreibt, auf neuartige Weise auch Grenzen für das Teilen von Daten erzwingt. Eine Semantik der »Verantwortung« und des Auswählens konditioniert oder konterkariert vielleicht sogar diejenige von Offenheit im Sinne von weltweiter Kooperation und digitaler Allmende.

Zur Polykrise also eine neue Polyphonie datenpolitischer Signale? Wir versuchen uns hierzu an einem Lagebild. Im Fokus sind dabei die Diskurse – also programmatische Steuerungsversuche. Zu diesem Zweck nehmen wir neuere Verlautbarungen aus der deutschen Wissenschafts- und Datenpolitik in den Blick, wobei vor allem deren vage Terminologie und geringe Konsistenz kritisch reflektiert werden sollen. Ebenso möchten wir die potenziell weitreichenden Ansprüche aufzeigen, die man unter dem Vorzeichen der Verantwortung nun (neu) an die Wissenschaft stellt. Unser Ziel ist es, eine öffentlich bislang eher raunend adressierte Problemstellung und die darin sich abzeichnende Zielkonflikte klarer herauszustellen. Lösungen haben wir nicht. Stattdessen versuchen wir in eher allgemeiner Form die Situation zu umreißen, in welche die transnationale Wissenschaft in einer Lage der »Post-Globalisierung«, also einer Welt härter werdender Interessensblöcke und neuer Abschottungsprozesse, geraten ist.

3 Es sind EU-Staaten bzw. die EU als ganze, die im Rahmen mehrerer Förderinitiativen seit einiger Zeit »Datenräume« aufbauen (vgl. Europäische Kommission 2023a). Hier geht es nicht primär um Offenheit als vielmehr um ein vertrauensbasiertes (und zugunsten der jeweiligen Geschäftsmodelle auch hinreichend »geschütztes«) Teilen von Daten. Dieses soll Vermarktung gerade auch kritischer Daten erleichtern. Stichworte lauten GAIA-X oder auch (ebenfalls schon recht weit entworfen) European Health Data Space. – Auch Datenräume sind allerdings, unter Wahrung eines KYC-Prozesses und der jeweiligen Regeln, als global niedrigschwellig zugänglich gedacht.

1. Papiere zur Wende

Im März 2022 hat die DFG die Förderung von wissenschaftlichen Kooperationen mit Russland ausgesetzt (vgl. DFG 2022), im deutschen Wissenschaftssystem wurden institutionelle Beziehungen »eingefroren« – als Maßnahmen, die der durch Kanzler Scholz am 27. Februar 2022 in einer Sondersitzung des Bundestages als »Zeitenwende« titulierten Situation Rechnung tragen. Ein gutes Jahr später und das Thema verallgemeinernd hat der Deutsche Hochschulverband mit einer Stellungnahme zu »*Science Diplomacy« nach der Zeitwende* hierauf reagiert. »Russlands brutaler Überfall« auf die Ukraine« wird deutlich verurteilt: an »Kipppunkten« müsse »auch die Wissenschaft« »Haltung beweisen und Position beziehen« (DHV 2023, S. 1 f.). Das Papier fasst auch ins Auge, dass sich die außenpolitische Lage auf Dauer auf die deutsche Wissenschaft verhaltensprägend auswirken werden wird: »Stärker als bisher« seien autokratische Staaten »mal als Partner, mal als Herausforderer oder auch Gegner« wahrzunehmen (vgl. DHV 2023, S. 2). Der Wissenschaftsaustausch mit autoritären Staaten sei »ein schwieriger Balanceakt«, müsse reflektiert und auch mit der »wertstiftende(n) Bedeutung der Freiheit der Wissenschaft« als »Eckpfeiler« erfolgen. Dennoch wirbt der Verband auch für die Chancen der Fortführung von Kooperationen »auf persönlicher Ebene«:

> »Auch dieser Weg ist keinesfalls risikofrei, weil gute persönliche Kontakte blenden können. Die historischen Erfahrungen können jedoch ermutigen: […] Vertiefte Kenntnisse des Gegenübers schaffen Verständnis und Vertrauen und eröffnen allen Beteiligten Einblicke in neue Welten. Langer Atem zahlt sich aus: Eine freie Wissenschaft kann positiv auf geschlossene Gesellschaften ausstrahlen und potentielle Reformkräfte dort stärken oder entstehen lassen. Eine an unbequeme außenpolitische Realitäten angepasste ›Science Diplomacy‹ bleibt deshalb wichtig und richtig.« (DHV 2023, S. 3)

Diese Sichtweise zielt erkennbar nicht nur auf den Umgang mit Russland, sondern ist auch zugeschnitten auf die im Papier neben Iran und der Türkei »vor allem« (DHV 2023, S. 1) angesprochene Volksrepublik China (hierzu inzwischen auch DAAD 2024).

Wenig später, nämlich am 20. August 2023, meldete sich die Bundesforschungsministerin mit einem Gastbeitrag in der FAZ zu Wort, welcher ebenfalls die »Zeitenwende« zum Ausgangspunkt nimmt, um nun vor allem den »kritischen Blick auf China« zu thematisieren: Es bedürfe erstens einer Bremse des »ungewollte[n] Abfluss[es] von Know How und Technologie«; insbesondere »der Dual-Use-Aspekt« sei dabei mitzudenken. Zweitens

müssten »wir noch verantwortungsbewusster mit der Wissenschaftsfreiheit umgehen« – nämlich »bei sicherheitsrelevanter Forschung und erkennbaren Dual-Use-Risiken« hinsichtlich der Einladung bzw. Mitarbeit ausländischer Wissenschaftler »besonders sensibel handeln«. Und drittens sei »die strikte Trennung zwischen ziviler und militärischer Forschung« zu hinterfragen, da diese »mit dem technologischen Fortschritt« zunehmend verschwimme. Die Zeitenwende rücke überdies Zivilklauseln in ein verändertes Licht, es sei fraglich, ob diese noch zeitgemäß seien. »Zivilklauseln sollten daher zumindest so ausgestaltet sein, dass Wissenschaftler ihrer Verantwortung im Interesse unseres Landes gerecht werden können« (vgl. Stark-Watzinger 2023).

Als ein drittes Papier, das die Zeitenwende zwar nicht im Titel trägt, aber ihr sogar mittels der Empfehlung von »Prüf- und Reflexionsschritten« gerecht zu werden sucht, die Wissenschaftlerinnen und Wissenschaftlern angeraten werden, ist eine im September 2023 publizierte Stellungnahme der DFG zu nennen. Auf sechs Seiten geht es hier im Rahmen einer »auf geopolitische Veränderungen reagierenden Forschungskultur« (DFG 2023, S. 1) um den Umgang mit Risiken in internationalen Kooperationen. Verwiesen wird auf Außenwirtschaftsrecht und Außenwirtschaftsverordnung, auf die EU Dual-Use-Verordnung sowie die »Ethik sicherheitsrelevanter Forschung«, für welche das deutsche Wissenschaftssystem seit einigen Jahren auf freiwilliger Basis spezifische Gremien, die sogenannten Kommissionen für Ethik sicherheitsrelevanter Forschung (KEF), besitzt.[4]

Die DFG kündigt nun an, im Rahmen von DFG-Förderanträgen sei künftig unter dem Punkt »… zu möglichen Sicherheitsrelevanten Aspekten« die Vertretbarkeit eines Forschungsprojektes »schon beim Anschein des Vorliegens eines Risikos« (DFG 2023, S. 3) im Antragstext obligatorisch zu erläutern. Ebenso müssten Gutachtende sowie die DFG-Fachkollegien »von der Vertretbarkeit der Durchführung des Projektes überzeugt sein«, sonst sei es nicht zu bewilligen; und »in der Gesamtbetrachtung« sei die Reflexion auch danach nicht abgeschlossen, sondern bleibe »eine kontinuierliche Aufgabe in der Leitung von Forschungsprojekten […], nicht zuletzt, weil sich die politischen Rahmenbedingungen in Partnerländern über die Zeit verändern und eine Neubewertung erforderlich sein kann.« (DFG 2023, S. 4)

4 Die Leopoldina besitzt hierzu ein Dachgremium und ist zuständig für das Monitoring und die Vernetzung solcher dezentraler Kommissionen.

»Erkannte Risiken«, »Prüfschritte« und »Gesamtschau«: Die DFG listet hierzu Punkte zum Forschungsgegenstand (u.a. »Missbrauch« von Wissen durch Dritte) sowie zu den Forschungsbedingungen (Dual-Use, aber auch Rechtstaatlichkeit, Publikationseinschränkungen und mehr) auf, macht aber auch deutlich, dass es sich sowohl bei verantwortlicher Projektplanung als auch bei der Partnerwahl um eine umfassende, auch beratungsbedürftige und das persönliche Engagement der Forschenden dauerhaft fordernde Angelegenheit handelt. »Zu einem verantwortlichen Umgang mit Risiken«, heißt es abschließend durchaus ein wenig kryptisch, »gehört auch die Anerkennung der Komplexität der wissenschaftlichen und außerwissenschaftlichen Welt« (DFG 2023, S. 6).

Schließlich sei noch der Wissenschaftsrat zitiert, der im Oktober 2023 – nun als erster auch mit Blick auf die Datenströme und digitale Prozesse – im Rahmen umfassender Empfehlungen zu Digitaler Souveränität und Sicherheit, allerdings vage, anmerkte:

»Vor allem beim Teilen und gemeinsamen Nutzen von digitalen Objekten ergeben sich verschiedene Herausforderungen, die bisher oft noch zu wenig bedacht werden. Zu denken ist unter anderem an eine mögliche Preisgabe von Forschungsdaten in nicht kontrollierbaren digitalen Umgebungen, an die Nutzung von Soft- und Hardware, die unter Sicherheits- und Datenschutzgesichtspunkten zu beanstanden ist, oder auch an etwaige Einfallstore für Wissenschaftsspionage, gerade wenn es sich um Kooperationspartner aus autoritären Staaten handelt. Die zunehmenden geopolitischen Spannungen, die sich auch auf die internationale Wissenschaftskooperation auswirken, verstärken dieses Gefahrenpotenzial zusätzlich und rücken Fragen bezüglich wirtschaftlicher und technologischer Abhängigkeiten weiter in den Fokus.« (WR 2023, S. 23)

2. Gedanken zu den Papieren

Es ist plausibel, dass mit einem offenen Angriffskrieg in Europa sowie mehreren militärischen Drohszenarien und Erklärungen von Weltmächten wie China und die USA, die an eine »Blockkonfrontation« denken lassen, außenpolitisch motivierte Fragestellungen auch an das Wissenschaftssystem herangetragen werden. Forschung bewegt sich nicht in einem (und schafft auch keinen) politikfreien Raum. Wissenschaft muss zudem selbst die Integrität ihrer Prozesse schützen. Ein Wissenschaftssystem kann nicht offen zutage liegende Mechanismen ignorieren, mittels welche autokratische oder terroristische Regime Forschung oder auch Lehre instrumentalisieren. Insofern

muss man die Bereitschaft der Politik begrüßen, unangenehme Wahrheiten auszusprechen. Ebenso ist es viel verlangt, von deutschen politischen Ressorts sowie von wissenschaftlichen Beratungsgremien sofort klare Strategien in einer unklaren Lage zu fordern.

Dennoch führt – nach inzwischen anderthalb Jahren Waffengang in der Ukraine, Abbruch der Beziehungen zu Russland sowie Handelskonflikten und einem neuen Sinn für technologische Abhängigkeiten Europas – die Durchmusterung der wissenschaftspolitischen Aussagen (oder Ansagen?) in Sachen Zeitenwende zu einigen Fragen.

Zunächst fällt die Unterschiedlichkeit der Themen auf, von (a) dem Transfer militärisch relevanten Wissens (»dual use«, »sicherheitspolitische Interessen«), (b) dem Schutz von Geschäftsgeheimnissen zur Sicherung eines Technologievorsprungs, (c) der Minderung einer zu großen technologischen Abhängigkeit von bestimmten Ländern, (d) dem Problem des Missbrauchs von Wissen oder Kooperationsbeziehungen zu politisch bedenklichen, etwa undemokratischen Zwecken (»Wahrung zentraler, durch das Grundgesetz geschützter Güter«, DFG 2023: 1) sowie (e) dem allgemeinen Bild einer globalen »systemischen Rivalität« (Stark-Watzinger 2023), die Parteinahme erfordert. Eigentlich handelt es sich sogar schon auf der abstrakten Ebene um nahezu unverbundene Punkte – und forschungspraktisch gilt dies auch.

So ist das naheliegende Thema der absehbaren oder absehbar möglichen militärischen Nutzung von Forschungsergebnissen (a) alles andere als neu, auch wenn das deutsche Wissenschaftssystem hierzu erst seit einigen Jahren flächendeckend beratende Angebote anstrebt. Neu und bis zu einem gewissen Grad verständlich wird nun allerdings schärfer unterschieden zwischen einem Transfer von Wissen ins Ausland, der unter Dual Use-Aspekten unerwünscht ist, und einer Kritik an Zivilklauseln im Inland, welche die Ministerin in die Formel kleidet, solche Klauseln sollten »zumindest so ausgestaltet sein«, dass Wissenschaftler »im Interesse unseres Landes« agieren (vgl. Stark-Watzinger 2023) – soll heißen: wenn es um die richtige Seite geht, auch *für* Rüstungszwecke forschen.

Ob (und welches) Militär von Forschung profitieren soll – diese Frage hat zweifellos im Kontext »Zeitenwende« ihren Platz. Für den Schutz des Wissens von Unternehmen zugunsten von deren Marktposition (b) gilt dies hingegen in keiner Weise. Im Gegenteil – es muss überraschen, wie nonchalant der Zeitenwende-Diskurs die Entfernung zwischen Krieg und Handelskrieg verkürzt oder genauer gesagt sogar nur den Schutz von Marktpositionen in

denselben Kontext rückt. Insofern wird man es im Grunde für eine Kategorienfehler halten müssen, wenn die Ministerin den »ungewollten Abfluss von Know-How und Technologie ins Ausland« (s.o.) zu den »Risiken« für die deutsche Forschung zählt oder sogar zur Frage der »Sicherheit unserer Forschung« (ebd.) hochstilisiert. Denn für wie immer wichtig man deutsches Know-How und dessen Vermarktung hält: Forschung wird gewiss nicht unsicherer oder schlechter dadurch, dass erfolgreiche deutsche Unternehmen ihre Geschäftsgeheimnisse nicht schützen (können).

Bei der Vermeidung oder dem Rückbau von volkswirtschaftlichen Abhängigkeiten (c) handelt es sich demgegenüber um ein politisches Ziel im engeren Sinne – und auch eines, das die Allgemeinheit angeht und betrifft. Für den Digitalbereich wird dieses Thema seit einigen Jahren unter dem Stichwort der »digitalen Souveränität« diskutiert – wobei es oft die Wissenschaft selbst ist, der diese Souveränität (etwa was Software oder auch Großrechner angeht) fehlt. Sogenannte Lock-In-Situationen hat die öffentliche Hand in einigen Bereichen sogar sehenden Auges zugelassen (man denke an die Abhängigkeit von Produkten aus den Häusern Microsoft oder Adobe). Das Problem ist kein wissenschaftsspezifisches, vielmehr fehlen der Wissenschaft (allem voran im Hochschulbereich) im vollen Wortsinn die Mittel, um sich von hegemonialen Anbietern zu lösen. Lautet die Botschaft aus der Politik nun, solchen Abhängigkeiten sei entgegenzuwirken, handelt es sich – was die Wissenschaft angeht – im Grunde um ein fehladressiertes Signal. Denn zur Veränderung der Infrastruktursituation läge, umgekehrt, gerade für die durch die öffentliche Hand finanzierten Akteure das Momentum einer Zeitenwende eindeutig auf Seiten der Politik.

Der politische Missbrauch von Kooperationsbeziehungen, bemessen am deutschen Verfassungsverständnis, etwa an den Grund-, Menschen- und Freiheitsrechten, (d) eröffnet ein viertes, nicht nur rechtlich, sondern auch moralisch weites Feld. So muss sicher inzwischen nicht nur den Lebensverhältnissen einer Zivilgesellschaft in einem Partnerland, sondern auch dem Thema »Nachhaltigkeit« Verfassungsrang zugebilligt werden. Soll Forschungs- und Wissenschaftsaußenpolitik diesbezüglich tatsächlich künftig mittels der Messlatte hochstehender Verfassungsnormen erst einmal evaluieren, bevor man forschen darf? Die Gefahr wäre groß, gerade über politisch ungute Weltgegenden nur noch wenig (empirisch) zu wissen, würden beispielsweise die Klima-, die Wirtschafts- und Sozialwissenschaften oder auch die Altertumswissenschaften so verfahren. Vor allem aber hat diese Fragestellung wiederum wenig mit der jüngst so genannten »Zeiten-

wende« im engeren Sinne zu tun. Die Vermischung dieses Punktes mit etwa den Punkten (a) und (c) oder auch überhaupt die Verbindung der genannten Stichworte in einer Art atmosphärischen Gesamtdiagnose muss befremden.

3. Raunen oder aber neue Maximen?

Das DFG-Papier bietet »ausgehend« von »Erwägungen zur Dual Use-Problematik« eine Liste von »Anhaltspunkte[n] zu empfohlenen Prüf- und Reflexionsaspekten, die kontinuierlich weiterentwickelt werden« – wobei extra auch nochmals die Liste als »nicht abschließend« bezeichnet wird (vgl. DFG 2023, S. 5). Man soll sich beraten lassen, sich seiner Verantwortung bewusst sein, kontinuierlich aufmerksam bleiben: angesichts einer unabgeschlossenen Liste von eher formalen, man könnte sagen: rechtsstaatlichen Mängeln einer Kooperationsbeziehung bleibt da Andeutungshaftes im Raum stehen. Die geforderten Reflexionen haben über Recht ja gerade hinauszugehen (vgl. DFG 2023, S. 1). In welchem Sinne sind überdies die »ethische und rechtliche Bewertung sicherheitsrelevanter Forschung« sowie ein entsprechend richtiges Verhalten eine Sache von langjähriger Erfahrung (der zuständigen »Kommissionen und Beauftragten«), wie die DFG abschließend nahelegt? Geht es hier also um wissenschaftsexterne Bewertungen oder nicht doch gerade um den Sinn fürs genuin Wissenschaftliche (und dessen Grenzen)?

Fast raunend äußert sich die Ministerin. Man wolle »Information und Sensibilisierung« verstärken, Forschende sollten selbst »besonders sensibel handeln« und dann eben, wie schon zitiert, »ihrer Verantwortung im Interesse unseres Landes« gerecht werden, denn richtig sei – gewagter Komparativ – ein »strategischerer Ansatz in Wissenschaft und Forschung« (vgl. Stark-Watzinger 2023). »Umdenken« und »Freiheit zur Verantwortung« sowie »Ethik« sind weitere Stichworte.[5]

Relativ knackig fallen demgegenüber die Leitlinien des DHV aus. Er fordert »Kooperationsvereinbarungen«, die »Vereinnahmungen und un-

5 Das DAAD-Papier zu China – angelegt als »an den Chancen der Zusammenarbeit […] orientierte[r] Ansatz« (vgl. DAAD 2024: 5) – bringt die, jedenfalls im fraglichen Zusammenhang, ebenfalls opake Dimension der »Chinakompetenz« oder sogar »interdisziplinären Chinakompetenz« (DAAD 2024, S. 17 ff.) ins Spiel: Kooperationen seien nicht nur interessenorientiert und risikoreflexiv, sondern auch »kompetenzbasiert« anzulegen – was immer das in normativer Hinsicht heißen mag.

erwünschte Abhängigkeiten abwehren« (DHV 2023, S. 3). Werde »Freiheit mit Füßen getreten«, seien Kooperationen zu beenden. Auch hier wünschte man sich freilich Fallbeispiele, denn die Freiheit »mit Füßen« zu treten bleibt letztlich eben doch ein Sprachbild, das sich schwer in empirische Indikatoren, geschweige denn Handlungsmaximen umsetzen lässt. Verlasse ich das Konsortium, weil man sich auf die Nutzung einer Software verständigt, deren Hersteller auch autokratische Regierungen beliefert? Verwehre ich der belarussischen Stipendiatin ein Empfehlungsschreiben, weil ich nicht weiß, auf welche Positionen sie sich unter seiner Vorlage bewerben wird? Lehne ich ab und trete die Rückreise an, wenn man mir bei der Einreise nach China ein staatliches Mobiltelefon aushändigt und mich verpflichtet, es bei mir zu führen?

Was also wäre »Zeitenwende« im Digitalen? Wie globale Datenströme, das Internet und die jahrelang als umfassende Vernetzung gefeierte Entwicklung für die Wissenschaft im Rahmen jenes geforderten Umdenkens zu bewerten sind, ist besonders dann eine schwierige Frage, wenn man sich klarmacht, dass die Offenheitssemantik rund um Open Science ja fortbesteht. Wo soll nun plötzlich die Forderung nach nur mehr begrenzten Datenzugängen ihre Anhaltspunkte finden? Und mittels welcher Infrastrukturdispositive wäre nun in Sachen Datenzugang oder auch Datenpublikation weiter zu verfahren? Lediglich das DFG-Papier spricht die Gefahr eines »systematischen Abgreifens von Forschungsdaten« (DFG 2023, S. 5) bisher an. Wie jedoch beugt man dem auf offenen Plattformen wirksam vor? Bislang jedenfalls hat man schon dem Tracking, Tracing, dem Datenhandel durch Großverlage und ihre Intermediäre wenig entgegengesetzt. Sieht man die Wissenschaft nun in der Lage, Datenraub, Tracking oder auch Datensabotage durch militärische Gegner zu verhindern?

Und auch das Schicksal der Maxime des »Teilens« und der Offenheit, die Forschung im Digitalzeitalter doch gerade ja auszeichnen soll, wäre von Interesse. Denn eine Semantik der Privilegierung und des selektiven Zulassens von Zugang zu digitalen Ressourcen lassen die Bildungs- und Wissenschaftsvorstellungen der 2000er Jahre bisher kaum zu. Dies gilt namentlich für die durch die UNESCO vorangetriebene und ebenfalls global angelegte Programmatik »Open Science«.[6] Bislang werden »Zeitenwende« und die

6 Vgl. zum gerade auch in Europa mit Macht erfolgten Umsteuern in Richtung »Openness« von wissenschaftlichen Publikationen, aber auch Forschungsdaten, den Beitrag von Petra Gehring in diesem Band.

Standards digitaler Transparenzgebote sowie Zeitenwende und »Open Science« auch noch nicht ins Verhältnis zueinander gebracht. Wir laufen also, so scheint es, in eine Zeit des neuen Nachdenkens über mögliche Abstufungen des Datenzugangs und auch des Anerkennens real existierender Konflikte rund um Forschungsdaten hinein. Dass das Bundesforschungsministerium inzwischen hat wissen lassen, dass in Deutschland künftig, die zivile und die militärische Forschung stärker kooperieren sollten (BMBF 2024, S. 8 f.), kommt zu diesem Befund hinzu. Denn sicher wird man die bisherigen Schutzgrade militärischer Forschungsgeheimnisse nicht absenken wollen. Somit kommen auch hierüber potenziell neue Verschwiegenheitspflichten und also Grenzen für das globale oder auch nur wissenschaftsweite Teilen von Daten auf die öffentliche Forschung zu.

4. Daten als umkämpftes Gut in der Post-Globalisierung

»Wir erleben eine Zeitenwende. Und das bedeutet: Die Welt danach ist nicht mehr dieselbe wie die Welt davor« (Scholz 2022, S. 8). Das oben schon erwähnte Zitat von Bundeskanzler Olaf Scholz aus der Regierungserklärung nach der russischen Invasion der Ukraine Ende Februar 2022 wurde auch für umfassendere politische Diagnosen zum geflügelten Wort. Im engeren Sinne beschreibt es nur die Erschütterung der europäischen Sicherheitsordnung, dennoch fing es auch darüber hinaus den Zeitgeist ein. Wie ein Brennglas bündelt sich im Begriff der Zeitenwende ein generelles Unbehagen an der Welt, wie wir sie heute erleben: eine Welt, in welcher kein »weiter so« möglich erscheint. Hierzu einige abschließende Überlegungen. Sie setzen genereller an, nehmen aber wiederum die Wissenschaft in den Blick.

Die große Resonanz des Zeitenwende-Begriffes kann man nur dadurch erklären, dass es eben keine Momentaufnahme war, auch wenn es in der Regierungserklärung um einen konkreten Anlass ging. Mit anderen Worten: Die Zeitenwende geschah nicht im Februar 2022, sondern wurde damals nur in einem griffigen Wort ausgedrückt. Stattdessen fasst dieser Begriff mehrere Trends zusammen, die sich in den Jahren und Jahrzehnten zuvor entfalteten und jetzt kulminieren. Diese Entwicklung enthält einen Umbruch, eine Verschiebung von der Globalisierung zur Post-Globalisierung (vgl. ausführlich dazu Lambach/Hofferberth 2024).

Die Globalisierung, einstmals derart hegemonial im Diskurs, dass sie der frühere UN-Generalsekretär Kofi Annan mit der Schwerkraft verglich

(Annan 2002), ist im letzten Jahrzehnt zunehmend in einer ideellen Krise. Statt von Interdependenz und Integration ist gegenwärtig von »Deglobalisierung« (*deglobalisation*) und »Entkopplung« (*decoupling*) die Rede (Schirm u.a. 2022). Die Hegemonie der Globalisierung starb den sprichwörtlichen *death by a thousand cuts*. Jeder dieser Schnitte ging tief:

- Brexit und die »take back control«-Kampagne in Großbritannien,
- der Wahlsieg von Donald Trump im Zeichen von »America First«, welcher Handelskriege als probates Mittel der Staatskunst verstand und Allianzen einer Kosten-Nutzen-Kalkulation unterzog,
- die zunehmend belasteten Beziehungen zwischen China und den USA, welche vielerorts bereits als neuer »Kalter Krieg« gedeutet werden,
- die Covid 19-Pandemie und die damit verbundenen Schließungen von Grenzen, Disruptionen von Handlungsketten, und der alsbald einsetzende Impfstoff- und Handelsnationalismus,
- der russische Einmarsch in der Ukraine.

Der militärische Konflikt im Nahen Osten kommt seit neuestem hinzu. Diese Ereignisse sind Indizien für den Übergang in die Epoche der Post-Globalisierung. Gemeint ist damit nicht die Rückabwicklung der Globalisierung, sondern ein Infragestellen der mit der Globalisierung verknüpften Versprechungen von Prosperität, Frieden und Kooperation. Interdependenz war unter Befürworterinnen und Befürwortern der Globalisierung der Ausgangspunkt von Kooperation und Integration. Heute mehren sich die Gegenstimmen, die – geprägt von den Erfahrungen des letzten Jahrzehnts – Interdependenz auch als Quelle von Verwundbarkeit interpretieren.

Geopolitik ist heute immer auch Datenpolitik, in eigener Sache macht sich die Wissenschaft das bislang nicht in hinreichender Weise klar. Technologische Innovationskapazität ist in der Post-Globalisierung zu einem zentralen Indikator für Resilienz, Sicherheit und Zukunftsfähigkeit geworden. Für den Nationalen Sicherheitsberater der US-Regierung Jake Sullivan ist technologische Innovation »poised to define the geopolitical landscape of the 21st century« und »a national security imperative« (The White House 2022). Auch die Europäische Union spricht von einer entstehenden »geopolitical, economic, and technological global rivalry« (Europäische Kommission 2023b, S. 2), welche EU-Kommissar Julian King schon vor Jahren als die »geotech world« bezeichnete (King 2019). Dies sind Denkweisen einer sich entfaltenden systemischen Rivalität, derer sich auch die Bundesforschungsministerin bedient – siehe Punkt e) in unserer obigen Aufzählung.

So haben Regierungen diesen Wandel keineswegs untätig über sich ergehen lassen, sondern eine Vielzahl politischer Strategien und rechtlicher Innovationen entwickelt, die ihre Position in dieser neuen Weltordnung sichern sollen. Daten- und digitalpolitisch gehören dazu zum Beispiel Gesetze zur Datenlokalisierung, Sorgen um Dual Use-Kapazitäten digitaler Technologie (z.B. auch Künstlicher Intelligenz) sowie Diskussionen um digitale bzw. technologische Souveränität (Lambach/Oppermann 2023, Monsees/Lambach 2022). Im weiteren Sinne gehören dazu auch Diskussionen um den Schutz geistigen Eigentums und von wirtschaftlichen Innovationskapazitäten, die z.B. stärkere Eingriffsmöglichkeiten gegen ausländische Unternehmensübernahmen schufen, um den Abfluss von Technologie zu unterbinden.

Exemplarisch kann man diese Diskussion am Thema KI-Trainingsdaten sehen, die heute beinahe wie Staatsschätze behandelt werden. Entsprechend eng greifen in vielen Staaten wissenschaftliches Arbeiten und wirtschaftliche Innovationssysteme im Big Data- und KI-Bereich ineinander. Große Plattformen sammeln gigantische Datensätze an, die als eine der zentralen Ressourcen für die neue KI-Anwendungen gelten, vor allem in den Bereichen Text und Bild. Der Hype um Generative KI und Große Sprachmodelle ist seit 2022 so groß, dass sie als nationale Prioritäten im globalen »AI Race« behandelt werden, obwohl ihre Wirkung auf nationale Sicherheit eher als gering einzustufen wäre. In einem Zeitungsbericht wird der Wettlauf aus chinesischer Sicht so beschrieben: »China wants its own intelligent natural language systems for reasons that range from language and the need for Chinese language systems to keep up with English and other global languages, to purely political reasons relating to its goals as a global science and technology power« (Sharma 2023). Neben diesen politischen Erwägungen gibt es auch für Unternehmen keinen Anlass ihre Trainingsdaten mit irgendwem zu teilen – damit gäben sie einen wichtigen Teil ihrer Wertschöpfung preis.

5. Fazit: Transnationale Wissenschaft in der Post-Globalisierung

Die geschilderten Entwicklungen und Überlegungen betreffen auch die Wissenschaften, wie oben ausgeführt. Während die einen Daten einsammeln, sollen die anderen Daten teilen. Wobei die Frage, mit wem sie teilen dür-

fen, nun ebenfalls kritisch wird. Genau wie Handel und Technologie wird so auch die Forschung einem Prozess der Geopolitisierung unterworfen, in der internationales Handeln zunehmend unter der Frage bewertet wird, inwieweit es staatliche Interessen berührt. Auch hier kann die KI-Forschung als Beispiel herangezogen werden, die seit jeher transnational organisiert ist. Teams aus verschiedenen Ländern arbeiten an gemeinsamen Publikationen, Firmen vergeben Forschungsaufträge an internationale Subunternehmen (World Intellectual Property Organization 2019). Und alle Akteure profitieren von den global vernetzten Infrastrukturen des Internets, die die massenhafte Sammlung von Text-, Bild- und Videodaten ermöglichen. Hier wird das Spannungsfeld deutlich, in dem transnational-kollaborative Wissenschaftspraktiken mit nationalem Konkurrenz- und Prestigedenken stehen.

Ähnliche Spannungen und Verschiebungen zeichnen sich auch im Umgang mit Forschungsdaten und transnationaler wissenschaftlicher Kooperation generell ab. Das lange herrschende Paradigma einer weitestmöglichen Offenheit verschiebt sich hin zu einer stärker selektiven Offenheit mit mehr Vorbehalten, allerdings nicht zu einer Schließung. Ein Blick in die Geschichte mag hier etwas Hoffnung geben. Selbst in den schwierigsten Phasen des Kalten Kriegs, als andere Formen der Zusammenarbeit stärker eingeschränkt oder gar ganz unmöglich waren, war wissenschaftliche Kooperation zwischen West- und Ostblock möglich. Das Internationale Geophysikalische Jahr 1957–58 ist hierfür ein Paradebeispiel (Collis/Dodds 2008). Man sollte den Vergleich allerdings nicht überstrapazieren. Europa befindet sich heute noch nicht in einem neuen Kalten Krieg mit China, auch wenn diese Phrase manchmal leichtfertig herausgekramt wird.

Gleichwohl bleiben die geopolitischen Spannungen nicht folgenlos für Forschung und Wissenschaft, insbesondere bei politisch sensiblen Technologien und Wissenschaften. Zwar bewegt sich Wissenschaft heute nicht in abgeschotteten Blöcken. Und sie kann ein Grenzen übergreifendes Eigenleben auch verteidigen. Das historische Beispiel des Ost-West-Konflikts zeigt, dass selbst in schwierigen politischen Lagen Systeme oder »Blöcke« übergreifende wissenschaftliche Kooperation zumindest ansatzweise möglich bleibt. Wissenschaftsdiplomatie und wissenschaftliche Kooperation haben auch in der Post-Globalisierung noch ihren Platz. Gleichwohl muss man sich der Frage stellen, wie denn nun mit den Datenströmen umzugehen ist, ob die paradoxe Doppelforderung nach einerseits Offenheit, andererseits Ab- und Ausgrenzung für die Wissenschaft überhaupt in ein reales Daten- und

Infrastrukturhandeln übersetzbar ist und wohin die gute wissenschaftliche Praxis driftet, wenn die Antwort auf komplexe Interessenslagen immer wieder lediglich darin besteht, den Wissenschaftlerinnen und Wissenschaftlern noch mehr »Verantwortung« aufzubürden. Wenn nun hierfür – das Teilen und das Nicht-Teilen – Leitmaximen neu ausgehandelt werden, kann und wird der oben geschilderte, pauschale Zeitenwende-Reflex jedenfalls nicht die letzte Antwort bleiben.

Anzuerkennen, wie umkämpft Forschungsdaten wirklich sind, beinhaltet für niemanden eine angenehme Einsicht. Sollte die Post-Globalisierung nun tatsächlich auch zu einer Zeit der »Post-Openness« in der Forschungsdatenpolitik führen, stellt sich einmal mehr die Frage, die schon zuvor womöglich nicht immer im Blick gehalten wurde: die Frage danach nämlich, was denn nun eigentlich im Interesse der Wissenschaft ist.

Literatur

Annan, Kofi (2002): *Secretary-General, Accepting Moscow Award, Says Strength of Russian Spirit ›Is Your Country's Greatest Natural Asset‹*, United Nations Press Release SG/SM/8262, 5.5.2002, https://press.un.org/en/2002/sgsm8262.doc.htm [23.3.204].

Barlow, John Perry (1996): *A Declaration of the Independence of Cyberspace. Electronic Frontier Foundation*, https://www.eff.org/cyberspace-independence [23.3.204].

BMBF [= Bundesministerium für Bildung und Forschung] (2004): *Positionspapier des Bundesministeriums für Bildung und Forschung zur Forschungssicherheit im Lichte der Zeitenwende*, https://www.bmbf.de/bmbf/shareddocs/kurzmeldungen/de/2024/03/240311-positionspapier-forschungssicherheit.html [23.3.2024].

Collis, Christy/Dodds, Klaus (2008): Assault on the unknown: the historical and political geographies of the International Geophysical Year (1957–8), in: *Journal of Historical Geography* 34, Heft 4, S. 555–573.

DAAD [= Deutscher akademischer Austauschdienst] (2024): *Die akademische Zusammenarbeit mit China realistisch gestalten. Handlungsempfehlungen des DAAD für deutsche Hochschulen*, Januar 2024, https://static.daad.de/media/daad_de/der-daad/kommunikation-publikationen/presse/daad_perspektive_china_de_240112.pdf [23.3.2024].

DFG [= Deutsche Forschungsgemeinschaft] (2023): *Umgang mit Risiken in internationalen Kooperationen. Empfehlungen der Deutschen Forschungsgemeinschaft (DFG)*, September 2023, https://www.dfg.de/download/pdf/dfg_im_profil/geschaeftsstelle/publikationen/stellungnahmen_papiere/2023/risiken_int_kooperationen_de.pdf [23.3.2024].

DFG (2022): *Hinweise für deutsch-russische Anträge und Kooperationsprojekte*, Information für die Wissenschaft Nr. 22, 8.3.2022, https://www.dfg.de/foerderung/info_wissenschaft/2022/info_wissenschaft_22_22/index.html [23.3.2024].

DHV [= Deutscher Hochschulverband] (2023): »Science Diplomacy« nach der Zeitwende. Leitlinien des Deutschen Hochschulverbandes zum Wissenschaftsaustausch mit autoritären Staaten, Berlin, 4.4.2023, https://www.hochschulverband.de/fileadmin/redaktion/download/pdf/resolutionen/Resolution-ScienceDiplomacy.pdf [23.3.2024].

Europäische Kommission [= European Commission, Joint Research Centre, Farrell, E., Minghini, M., Kotsev, A. u.a.] (2023a): *European data spaces – Scientific insights into data sharing and utilisation at scale*, Publications Office of the European Union, https://data.europa.eu/doi/10.2760/400188 [23.3.2024].

Europäische Kommission (2023b): *2023 Strategic Foresight Report: Sustainability and people's wellbeing at the heart of Europe's Open Strategic Autonomy*, COM (2023) 376 final, Brüssel, 6.7.2023, https://commission.europa.eu/strategy-and-policy/strategic-planning/strategic-foresight/2023-strategic-foresight-report_en [23.3.2024].

King, Julian (2019): *Commissioner King's remarks at the 2019 Digital Resilience Summit of the Lisbon Council*, Brüssel, 24.9.2019, https://ec.europa.eu/commission/presscorner/detail/en/speech_19_7261 [23.3.2024].

Lambach, Daniel/Hofferberth, Matthias (2024): Post-Globalisierung: Konturen eines Epochenbruchs, in: *Leviathan* 52, Heft 1, S. 93–118.

Lambach, Daniel/Oppermann, Kai (2023): Narratives of digital sovereignty in German political discourse, in: *Governance* 36, Heft 3, S. 693–709.

Monsees, Linda/Lambach, Daniel (2022): Digital sovereignty, geopolitical imaginaries, and the reproduction of European identity, in: *European Security* 31, Heft 3, S. 377–394.

Schirm, Stefan A./Busch, Andreas/Lütz, Susanne/Walter, Stefanie/Zimmermann, Hubert (Hg.) (2022): *De-Globalisierung: Forschungsstand und Perspektiven*, Wiesbaden.

Scholz, Olaf (2022): Regierungserklärung von Bundeskanzler Olaf Scholz am 27. Februar 2022, in: Bundesregierung (Hg.): *Reden zur Zeitenwende*, Berlin, September 2022, https://www.bundesregierung.de/resource/blob/992814/2131062/78d39dda6647d7 f835bbe76713d30c31/bundeskanzler-olaf-scholz-reden-zur-zeitenwende-download-bpa-data.pdf [23.3.2024].

Sharma, Yojana (2023): *China seeks AI ›catch-up‹ by creating its own ChatGPT-like tools*, University World News, 10.3.2023, https://www.universityworldnews.com/post.php?story=20230309103200913 [23.3.2024].

Stark-Watzinger, Bettina (2023): Wir müssen unsere Forschung besser vor China schützen, in: *Frankfurter Allgemeine*, 21.8.2023, https://www.faz.net/aktuell/politik/inland/stark-watzinger-wir-muessen-unsere-forschung-vor-china-schuetzen-19116350.html [23.3.2024].

The White House (2022): Remarks by National Security Advisor Jake Sullivan at the Special Competitive Studies Project Global Emerging Technologies Summit, 16.9.2022, https://www.whitehouse.gov/briefing-room/speeches-remarks/

2022/09/16/remarks-by-national-security-advisor-jake-sullivan-at-the-special-competitive-studies-project-global-emerging-technologies-summit/ [23.3.2024].

World Intellectual Property Organization (2019): *WIPO Technology Trends 2019: Artificial Intelligence*, Genf, https://www.wipo.int/publications/en/details.jsp?id=4386 [23.3.2024].

WR [= Wissenschaftsrat] (2023): *Empfehlungen zur Souveränität und Sicherheit im digitalen Raum*, Köln, https://www.wissenschaftsrat.de/download/2023/1580-23.html [23.3.2024].

Datenzugangsregeln als Aufgabe

Steffen Augsberg und Marcus Düwell

Schon aus der schieren Vielzahl der in den vorstehenden Beiträgen angesprochenen, auf unterschiedlichen Reflexions- und Handlungsebenen angesiedelten Herausforderungen erhellt, dass eine einfache *conclusio* unterkomplex und dem Thema unangemessen wäre. Im Folgenden soll daher weder eine klare Prognose über die Zukunft der Datenzugangsregeln abgegeben noch sollen eindeutige Empfehlungen ausgesprochen werden. Intendiert ist kein Abschluss, sondern eher ein zukunftsoffener Anschluss an das Vorgesagte. Damit geht es zunächst primär darum zu fragen, wie weitergehende Diskussionen aussehen könnten, die die in diesem Band versammelten Überlegungen integrieren. Dabei sind inhaltliche wie formale und institutionelle, tatsächliche wie normative Elemente in den Blick zu nehmen. Das kann hier nicht im Detail ausgeführt werden, lässt sich aber zumindest in Grundzügen skizzieren:

Den Ausgangspunkt liefert insoweit die basale, auch in zahlreichen Beiträgen dieses Bandes bestätigte Erkenntnis, dass sich die herkömmlichen Regeln zum Datenzugang zwar in der Vergangenheit prinzipiell bewährt haben, aber zugleich schon jetzt aufgrund veränderter technischer, gesellschaftlicher und politischer Rahmenbedingungen Friktionen und Dysfunktionalitäten hervorrufen. Es dürfte deutlich geworden sein, dass diese Regeln unter den Bedingungen einer »datafizierten« Netzwerkgesellschaft und intrikat verschränkten Plattformökonomie(n) nicht nachhaltig erfolgreich sein werden. Deshalb bedarf es einer konsequenten und kontinuierlichen Weiterentwicklung – das ist im Sinne eines »lernenden Systems« zunächst einmal eine bare Selbstverständlichkeit (oder sollte es sein), gewinnt aber vor dem Hintergrund der spezifischen Entwicklungsgeschwindigkeit und zahlreicher externer, nur teilweise berechenbarer Einflussfaktoren eine besondere Relevanz. Losgelöst von konkreten Regulierungsinhalten dürfte diese anpassungsorientierte Dimension eine der

wichtigsten Folgerungen aus der hier unternommenen multidisziplinären und übergreifenden Problemanalyse sein: zukünftige Gestaltungsoptionen sind so auszuwählen, dass sie noch nicht einmal den Anspruch erheben oder den Anschein erwecken, dauerhafte und abschließende Lösungen zu präsentieren. Stattdessen geht es um fortgesetztes *training on the job*, um eine bewusst etablierte Regelungsdynamik, in der sich eine gegebene Regulierungskonstellation nicht als Endpunkt, sondern immer nur als Teil einer fortlaufenden Evolution versteht und die eigenen Vorschläge folglich immer wieder in Frage gestellt und nachgebessert werden. Zugleich erfordert das Gewicht der hier zu beobachtenden Veränderungen, dass ihr Impact auf die Regulierung bzw. die Möglichkeit der Regulierbarkeit Gegenstand eines gründlichen und längerfristigen Diskussionsprozesses sein muss, um zumindest mittelfristig effektivere, gegebenenfalls auch kurzfristig anpassbare Regulierungen zu ermöglichen. Der Komplexität datafizierter Gesellschaften Rechnung zu tragen, bedeutet dann primär, die wissenschaftlichen und praktischen Fähigkeiten zu entwickeln, um diesen regulatorischen Lernprozess adäquat gestalten zu können.

Vor diesem Hintergrund sind Zweifel angebracht, ob und inwieweit der bislang statisch gedachte Fokus auf das datengebende Subjekt und auf den Personenbezug der Daten einer dynamischen Weiterentwicklung des Schutzkonzepts nicht eher im Wege steht. Die historisch plausible Ausrichtung auf den unterschiedlichen Grundrechtsstatus des Einzelnen und die unhintergehbare Wertschätzung des Individuums sollte auch weiterhin nicht zur Disposition stehen; es darf also keinesfalls darum gehen, diesen normativ zentralen Orientierungspunkt pauschal zu ersetzen oder aufzugeben. Angesichts der mit entsprechenden Experimenten in der Vergangenheit verbundenen Schrecken muss selbstredend der Versuchung widerstanden werden, neokollektivistische Herrschaftskonstrukte und hierauf basierende Datenzugangsmodelle zu etablieren. Das Individuum bleibt Kern und Ziel unserer normativen Ordnung; der pauschalen Berufung auf angeblich übergeordnete Ziele des Gemeinwohls (und erst recht des »Staatswohls«) ist deshalb stets mit großer Skepsis zu begegnen.

Allerdings ist einzugestehen, dass unter den beschriebenen Bedingungen der »Datafizierung« aus verschiedenen Gründen das bisherige Verständnis der (Schutz-)Position des Einzelnen ein Problem darstellt. Zum einen sind bestimmte Schutzinstrumente, wie ein Zustimmungserfordernis, bisweilen weder sinnvoll möglich noch dem Individualschutz wirklich förderlich. Zum anderen scheinen viele Regelungen davon auszugehen,

dass man den Einzelnen primär als selbständiges und tendenziell isoliertes Wesen anzuerkennen habe. Damit wird aber verkannt, dass die menschliche Existenz zu einem beträchtlichen Teil von vielfältigen personalen und institutionellen Interdependenzen gekennzeichnet ist. Es sind aber gerade diese Gestaltungen der menschlichen Relationalität, die sich im Zuge der Digitalisierung teilweise erheblich wandeln. Diese Wandlungen sind nun für den Einzelnen tendenziell nicht durchschaubar, weshalb die Gefahr besteht, dass Datenzugangsregelungen das Subjekt mit Erwartungen konfrontieren, denen es im Normalfall nicht gewachsen ist oder sein kann. Interdependenz und Relationalität müssen aber nicht prinzipiell als Bedrohung erfahren werden, sondern sie sind konstitutives Element der *conditio humana*. Regelungen müssten nun fragen, wie diese Interdependenzen produktiv gestaltet werden können. Diese Frage wird in der Zukunft noch wichtiger werden, insofern die rasanten Fortentwicklungen im Bereich der Künstlichen Intelligenz die Unterscheidung von (rechtlichen wie moralischen) Subjekten und Objekten verwischt. Damit stellt sich eine zumindest dreifache Aufgabe: Zum ersten sollte im Hinblick auf die *Konsumenten* gefragt werden, wie die Digitalisierung so gestaltet werden kann, dass den menschlichen Bedürfnissen, zu deren Realisierung sie entwickelt wird, auch wirklich gedient ist. Zum zweiten sollten mit Blick auf die *Rechtssubjekte* Regulierungen so gestaltet werden, dass ein Schutz des Einzelnen effektiv möglich ist, ohne das Subjekt permanent zu überfordern und damit letztlich dem Konzept des subjektiven Rechts zu schaden. Zum dritten sollten Individuen als *Bürgerinnen und Bürger* in die Lage versetzt werden, an der Gestaltung und Weiterentwicklung des Regulierungsregimes effektiv mitzuwirken.

Eine entsprechende, der besonderen Volatilität des Regelungsgegenstands angemessene adaptive Regelungsstrategie bedeutet zumal, *trial-and-error*-Prozesse zuzulassen bzw. sogar bewusst zu initiieren. Angesichts des rechtsstaatlich gebotenen Mindestmaßes an Stabilität, aber auch aus pragmatischen Gründen heraus, impliziert das keine grenzenlose Freiheit zu mehr oder weniger willkürlichen Veränderungen. Primär sollten vielmehr Anstrengungen unternommen werden, in konsistenter Weise vorhandene Lösungen weiterzuentwickeln und zu verbessern. Allerdings sind deutlichere Abweichungen von ausgetretenen Pfaden vorstellbar und gegebenenfalls sogar geboten, wenn erkenn- oder vorstellbar ist, dass vorgegebene Ziele so besser zu erreichen sind. Wichtig ist hierbei die Einsicht, dass entsprechende Versuche in der Regelungspraxis bereits stattfinden; das zeigen

insbesondere die Ausführungen von *Brieske/Schweizer* zu den unterschiedlichen Subjektvorstellungen, die der neueren unionalen Rechtsetzung im Datennutzungsbereich zugrunde liegen. Ähnliches lässt sich indes auch für die nationalen Anstrengungen, zumal im Gesundheitssektor, erkennen. Es geht also nicht so sehr darum, innovative Ansätze überhaupt erst auszulösen. Stattdessen ist auf eine erhöhte Transparenz und eine verbesserte Systematisierung zu achten – auch, weil sich nur dann die Vorzüge und Nachteile divergierender Alternativen sinnvoll erfassen und vergleichen lassen. Daraus folgt eine institutionelle Daueraufgabe: erforderlich ist ein fortlaufender Prozess der (Selbst- und Fremd-)Beobachtung, der unterschiedliche Elemente umfassen kann und sich beispielsweise auch als eine spezifische Funktion der wissenschaftlichen Begleitung entsprechender Prozesse erweist.

Das damit schon angedeutete Moment der Verantwortung verdient es, grundlegender betrachtet zu werden. In Anbetracht der Vielfalt von Beteiligten ist offensichtlich, dass es einer umfassenderen Einbeziehung unterschiedlicher individueller wie kollektiver Akteure bedarf. Gleichzeitig genügt es nicht, sich pauschal auf eine in sich intransparente und potentiell intransigente Multiakteursverantwortung zu berufen. Der eigentliche regulatorische Witz der Verantwortungsdimension besteht vielmehr in der Aufgabe, einerseits möglichst genaue Rollendefinitionen vorzunehmen und konkrete Handlungsbeiträge herauszupräparieren, andererseits aber auch offen zu bekennen, wo genau dies nicht (mehr) möglich ist. Verantwortung ist somit kein *catch-all*-Begriff, sondern ein Differenzierungsgebot. Zwei Beispiele mögen dies verdeutlichen:

Zum einen ist die *Wissenschaft* in unterschiedlichen Wirk- und Werkdimensionen betroffen: sie ist Datengeber, Datennutzer, Datenproduzent und Datenallokator; sie reguliert Datennutzungsprozesse und ist zugleich selbst regulatorischen Eingriffen ausgesetzt. Darüber hinaus ist die genuin wissenschaftliche Perspektive aber in mehrfacher Hinsicht relevant: Wissenschaft ist ein wesentlicher Motor der Entwicklung von Datennutzungsmöglichkeiten, Wissenschaft beobachtet den Prozess der zunehmenden Datendurchdringung der Gesellschaft, und Wissenschaft kritisiert Entwicklungen und Fehlentwicklungen im Umgang mit Daten. In dieser Hinsicht unterstützt sie gesellschaftliche, rechtliche wie politische Kontrollfunktionen. Offensichtlich stellen sich dabei je nach Handlungsbeitrag unterschiedliche Verantwortungsfragen; offensichtlich handelt es sich indes auch um in sich dynamische, durch Überlappungen gekennzeichnete

Prozesse. Jedenfalls wäre die Wissenschaft gut beraten, ihre besondere Rolle im Kontext der Datennutzung noch intensiver intern zu debattieren und nach Möglichkeit nach außen eine zumindest einigermaßen einheitliche und konsistente Position zu vertreten. Besonders realistisch erscheint diese Hoffnung angesichts stark divergierender Interessen indes nicht, in diese Richtung zu arbeiten wäre aber eine primäre Aufgabe der Wissenschaft.

Zum anderen sollte das Augenmerk verstärkt auf die *Infrastrukturverantwortung* gelegt werden. Sie betrifft zunächst und vor allem ein Bewusstsein für die Bedeutung übergeordneter Zugangseröffnungen, die ihrerseits eine grundsätzlich gut funktionierende und nicht einfach korrumpierbare Infrastruktur voraussetzen. Das verweist zugleich, ohne damit in übertrieben nationalistische bzw. regionalistische Züge zu verfallen, auf die Gefahren fehlender Autarkie bzw. »digitaler Souveränität«. Infrastrukturverantwortung betrifft damit nicht nur das, was ist, sondern umfasst gerade die infrastrukturell erst ermöglichten künftigen Entwicklungen. Wenn einzelne subjektive Verantwortlichkeiten zugunsten stärker objektivierter Kontroll- und Verteilungsaufgaben zurückgedrängt werden, muss darüber hinaus gewährleistet sein, dass hiermit keine inakzeptable Missbrauchsgefahren einhergehen. Individuellen Kontrollverlusten sollten damit infrastrukturelle Kontrollzugewinne korrespondieren, die dann im Rahmen rechtsstaatlicher und demokratischer Prozesse gestaltet werden können. Hierauf ist bei der Fortführung der existierenden Dateninfrastruktur, namentlich auch bei der Gründung entsprechender Kontrollzentren und -institute, besonderer Wert zu legen.

Eine zentrale Rolle bei der Entwicklung entsprechend adaptiver Regelungsmechanismen spielt schließlich die frühzeitige und konsequente Verbindung regulatorischer und technischer Aspekte. Über die klassische Konzeption »technikneutraler« Regulierung und auch die Idee der *privacy by design* hinausgehend bedeutet dies *idealiter* eine Herangehensweise, die Regulierungen zum Schutz des Einzelnen so gestaltet, dass die Chancen technischer Innovationen genutzt werden können. Die Überlegungen dieses Bandes haben gezeigt, mit wieviel Gesichtspunkten Datenzugangsregeln verbunden sind. Regulierungen der Zukunft sollten diesem Komplexitätsniveau Rechnung tragen.

Autorinnen und Autoren

Dr. Steffen Augsberg ist Professor für Öffentliches Recht an der Justus-Liebig-Universität Gießen.

Fabiola Böning ist wissenschaftliche Mitarbeiterin am Fachgebiet für Öffentliches Recht, IT-Recht und Umweltrecht (Prof. Dr. Gerrit Hornung, LL.M.) sowie am Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG) der Universität Kassel.

Jasmin Brieske ist wissenschaftliche Mitarbeiterin und Doktorandin an der Goethe-Universität Frankfurt am Main sowie Rechtsreferendarin am Landgericht Frankfurt am Main.

Dr. Marcus Düwell lehrt Philosophie an der TU Darmstadt.

Dr. Petra Gehring ist Professorin für Philosophie an der TU Darmstadt.

Dr. Malte-C. Gruber ist Professor für Bürgerliches Recht und Rechtsphilosophie an der Justus-Liebig-Universität Gießen.

Dr. Philipp Kellmeyer ist Juniorprofessor für Responsible AI and Digital Health an der Universität Mannheim. Zudem arbeitet er als Neurologe und klinischer Forscher an der Klinik für Neurochirurgie des Universitätsklinikums Freiburg.

Dr. Daniel Lambach ist Privatdozent für Politikwissenschaft an der Universität Duisburg-Essen.

Benjamin Müller ist wissenschaftlicher Mitarbeiter in der ZEVEDI-Projektgruppe »Datenzugangsregeln". Er promoviert in Philosophie über Freiheit im Ausgang von Hegel und Schelling.

Dr. Frank Niggemeier wurde mit einer Arbeit über Hans Jonas' Ethik für die technologische Zivilisation promoviert und arbeitet freiberuflich zu Fragen der Praktischen Philosophie. Hauptberuflich leitet er das Referat »Ethik im Gesundheitswesen, Sachverständigenrat Gesundheit und Pflege« im Bundesgesundheitsministerium sowie die Geschäftsstelle des Sachverständigenrats Gesundheit & Pflege.

Lars Pfeiffer ist wissenschaftlicher Mitarbeiter am Fachgebiet für Öffentliches Recht, IT-Recht und Umweltrecht (Prof. Dr. Gerrit Hornung, LL.M.) sowie am Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG) der Universität Kassel.

Dr. Anne Riechert ist Forschungsdirektorin für KI und Digitalisierung am Institut für Finanzleistungen e.V. (iff).

Dr. Doris Schweitzer ist Professorin für Soziologie mit dem Schwerpunkt Soziologische Theorie und Theoriegeschichte an der Goethe-Universität Frankfurt am Main.

Zaira Zihlmann arbeitet seit 2019 als wissenschaftliche Assistentin von Prof. Dr. iur. Mira Burri am Lehrstuhl für Internationales Wirtschafts- und Internetrecht an der Rechtswissenschaftlichen Fakultät der Universität Luzern.