ePA, DiGA, SaMD & Co. – Regulatorische Trends und Entwicklungen einer datengetriebenen Medizin*

Von *Michael Kolain* und *Jonas Lange*

I. Einleitung

1. Einführung in die Welt der datengetriebenen Medizin

Bei der Bewertung des Potentials einer „datengetriebenen Medizin" scheiden sich seit jeher die Geister – der Forderung „die Chancen des digitalen Wandels [zu] ergreifen"[1] stehen zahlreiche ungeklärte ethische, rechtliche und gesellschaftspolitische Fragen gegenüber[2]. Es ist Aufgabe einer integrierten Rechtsetzung im Bereich der Digital- und Gesundheitspolitik, die widerstreitenden Interessen und Perspektiven in einen konstruktiven Ausgleich zu bringen und bis auf die technische Umsetzungsebene rechtssicher durchzudeklinieren. Wissenschaft und Gesetzgebung sind dazu aufgerufen, dem öffentlichen Gut der Gesundheit – auf dem, frei nach Arthur Schopenhauer, immerhin „neun Zehntel unseres Glückes" beruhen – auch im digitalen Zeitalter den passenden rechtlichen und technologischen Rahmen zur Seite zu stellen.

Übergreifende Zielvorstellung im Bereich eHealth ist es, die vorhandenen Datenpunkte im Gesundheitswesen besser zusammenführen und neue Informationen über die individuelle sowie kollektive Gesundheit mithilfe komplexer Softwareanwendungen ergebnisorientiert aufbereiten zu können. In Deutschland liegen Gesund-

* Stand dieses Beitrags ist der 5. November 2023.

[1] https://www.bundesgesundheitsministerium.de/ministerium/meldungen/2019/gesundheitsministerkonferenz.html [Abruf: 21. 2. 2023].

[2] Siehe beispielsweise die Begleitung des LfDI Rheinland-Pfalz im Bereich der Telemedizin mit der Grundaussage „Aus datenschutzrechtlicher Sicht stehen der Nutzung telemedizinischer Anwendungen im Bereich Gesundheit und Pflege grundsätzlich keine Bedenken entgegen, sofern dabei das informationelle Selbstbestimmungsrecht der Betroffenen angemessen berücksichtigt wird.", https://www.datenschutz.rlp.de/de/themenfelder-themen/telemedizin/ [Abruf: 21. 2. 2023]. In der Zwischenzeit hat die Bundesregierung zwei Gesetzesentwürfe aus dem BMG beschlossen und in das parlamentarische Verfahren überführt: Das Digitalgesetz (DigiG) soll u. a. die Vorgaben zur elektronischen Patientenakte (ePA) reformieren, während das Gesundheitsdatennutzungsgesetz (GDNG) den Fokus auf die Weiterverarbeitung (anonymisierter) Gesundheitsdaten durch die Forschung legt, siehe https://www.bundesgesundheitsministerium.de/presse/pressemitteilungen/bundeskabinett-beschliesst-digitalgesetze-fuer-bessere-versorgung-und-forschung-im-gesundheitswesen.

heitsdaten einzelner Patient:innen und die Auswertungen der behandelnden Ärzt:innen bislang weitgehend in digitalen Silos verteilt: als Behandlungsdokumentation in den Aktenschränken verschiedener Arztpraxen und in Arztbriefen, als Abrechnungsdaten bei den Krankenkassen oder aggregiert in medizinischen Studien von Forschungseinrichtungen und der Industrie. Was aus Sicht des Persönlichkeitsschutzes der behandelten Menschen durchaus sachgerecht erschien[3], erweist sich in einer digitalen Lebenswelt mit mannigfaltigen Datenpunkten über die menschliche Gesundheit möglicherweise als Bremsklotz für eine passgenaue individuelle Gesundheitsvorsorge und eine evidenzbasierte Gesundheitspolitik. Nicht nur die globale Covid-19-Pandemie, in der die Bewertung komplexer Messwerte und Kennzahlen fast zum Volkssport mutierte, sondern auch die Fortschritte im Bereich lernfähiger Softwareanwendungen, die ein Stück weit selbsttätig aus riesigen Datensätzen neue Erkenntnisse über medizinische Wirkungszusammenhänge und Heilungsmöglichkeiten extrahieren können, machen deutlich: Auf dem Weg in eine „datengetriebene Medizin" müssen Gesellschaft, Wissenschaft und Politik vielfältige Herausforderungen passgenau bewältigen und einen am Gemeinwohl orientierten Kompromiss zwischen den verschiedenen Interessen und Perspektiven finden.

In das allenfalls unscharf umrissene, weite Feld der „datengetriebenen Medizin" lassen sich vielfältige rechts- und digitalpolitische Entwicklungen einordnen, die in Deutschland und der EU in den letzten Jahren im Bereich eHealth eine zentrale Rolle gespielt haben. Sie reichen von der 2021 in Deutschland gestarteten elektronischen Patientenakte (ePA),[4] über die unter dem Schlagwort „Apps auf Rezept" bekannt gewordenen und seit 2020 gesetzlich verankerten „Digitalen Gesundheitsanwendungen" (DiGAs), bis hin zu in Krankenhäusern eingesetzter Diagnose-Software (Software as a Medical Device, SaMD), erstrecken sich aber auch auf vernetzte softwaregetriebene Produkte, wie Fitnessarmbänder, oder Implantate, wie mit dem Smartphone verbundene „smarte" Herzschrittmacher[5].

Viele der Software- und Hardwareanwendungen im Bereich der datengetriebenen Medizin zeichnen sich dadurch aus, dass sie zum einen in der Phase der Produktentwicklung und -anpassung auf vielfältige Gesundheitsdaten angewiesen sind, um einen bestmöglichen Output für die medizinische Versorgung zu gewährleisten. Zum anderen generieren solche Anwendungen im klinischen Einsatz oder Heimge-

[3] Immerhin war in Zeiten der medizinischen „Zettelwirtschaft" klar vorgezeichnet, welche:r Akteur:in über welches Wissen verfügt und es lag großteils in der Hand des Einzelnen, individuell Verschwiegenheitspflichten für eine Weitergabe aufzuheben oder eigene Dokumente an Leistungserbringer:innen weiterzugeben.

[4] Das Bundesgesundheitsministerium (BMG) hat dazu eine neue Digitalstrategie vorgestellt und plant auch Änderungen an Konzept und Ausrollen der ePA, siehe https://www.bundesgesundheitsministerium.de/presse/pressemitteilungen/digitalisierungsstrategie-vorgelegt-09-03-2023.html [Abruf: 1. 4. 2023].

[5] Ähnlich einem Herzschrittmacher können etwa auch stimulierende Gehirn-Computer-Schnittstellen elektronische Impulse setzen, um Symptome von Krankheiten wie Parkinson oder Epilepsie zu lindern, vgl. *Mario Martini/Carolin Kemper*, Cybersicherheit von Gehirn-Computer-Schnittstellen, Int. Cybersecur. Law Rev. 3 (2022), S. 191 (196).

brauch wiederum selbst neue Gesundheitsdatensätze, die – jedenfalls theoretisch – gleichsam erneut als Forschungs- oder Trainingsdaten zur Entwicklung neuer medizinischer Software Verwendung finden können. Um die Feinheiten technischer Innovationen im Bereich eHealth sachgerecht zu strukturieren, sind Gesundheits-, Technologie- und Datenrecht nicht nur rechtssystematisch gemeinsam zu betrachten, um rechtsdogmatische Widersprüche zu vermeiden, sondern sie müssen zugleich auch die interdisziplinären Grundlagen und Implikationen reflektieren, um den technischen Fortschritt gleichsam in ihr Normprogramm aufzusaugen.

Abb. 1: Kreislauf der datengetriebenen Medizin.

2. Kreislauf der datengetriebenen Medizin

Der Verarbeitungszyklus von Gesundheitsdaten lässt sich unter den (Ideal-)Bedingungen einer datenzentrierten Medizin plastisch als eine Art „Datenkreislauf" umschreiben. Der „Kreislauf der datengetriebenen Medizin" lässt sich in fünf wesentliche Phasen der Datennutzung unterteilen. Zunächst erfolgt die Erhebung eines Datums[6] im gesundheitlichen Kontext, etwa im Rahmen einer ärztlichen Behandlung oder bei Verwendung einer digitalen Gesundheitsanwendung (II.). Dieses Datum wird anschließend in einem IT-System (etwa in der ePA des Patienten oder durch die Praxissoftware der Leistungserbringerin) gespeichert (III.). Von dort aus lassen sich die Daten einer Person gemeinsam mit anderen Datensätzen für andere Zwecke als die individuelle Behandlung, etwa für Forschungszwecke, akkumulieren (IV.). Mithilfe großer Datensätze mit gesundheitlichen Informationen vieler Menschen lassen sich dann im besten Fall neue Diagnose- und Therapieansätze entwi-

[6] Zum Begriff des „Datums" und seinem Verhältnis zu „Informationen" siehe *Martini/Michael Kolain et al.*, Datenhoheit – Annäherung an einen offenen Leitbegriff, MMR-Beil. 6/2021, S. 3 (3 f.) m. w. N.

ckeln (V.). Diese fließen ggf. in die Entwicklung softwarebasierter Produkte ein, die später auf dem Markt erscheinen und sich für die Anwendung am jeweiligen Patienten personalisieren (VI.) lassen. Die (personalisierten) Apps ermöglichen es wiederum, neue Gesundheitsdaten zu gewinnen: Der Kreislauf schließt sich und beginnt von vorn.

Freilich durchläuft nicht jedes Gesundheitsdatum – selbst wenn die technischen und rechtlichen Voraussetzungen gegeben sind – exakt diese fünf Phasen der Datennutzung.[7] Gerade im System der gesetzlichen (geschweige denn privaten) Krankenversicherung mit unterschiedlichen Akteuren, rechtlichen Vorgaben und institutionellen Zuständigkeiten ergeben sich zahlreiche Eigenheiten. Das Bild des „Datenkreislaufs" dient vor diesem Hintergrund also in erster Linie der Versinnbildlichung, welche Formen der Verarbeitung das Schlagwort der „datenzentrierten Medizin" beispielhaft unter seinem terminologischen Dach vereint und wie diese zueinander in Verbindung stehen (können). Letztlich dient er dem Beitrag als Richtschnur, um die verschiedenen rechtlichen und regulatorischen Themenbereiche zu strukturieren.

Dem Gesetzgeber kann diese Struktur eine Grundlage dafür bieten, um Regulierungsbedarfe zu erkennen und einzelne Maßnahmen systematisch aufeinander abzustimmen. Denn ein „Regulierungswildwuchs", wie er zurzeit schon im Bereich des – zudem unionsrechtlich überspannten – Sozial(datenschutz)rechts zu beobachten ist, konterkariert im schlimmsten Fall den Versuch, den Bereich einer „datengetriebenen Medizin" durch klare und praxistaugliche Vorgaben rechtlich einzuhegen.

3. Zielsetzung und Fokus des Beitrags

Die fünf Verarbeitungsszenarien eines „Kreislaufs der datengetriebenen Medizin" (Abb. 1) nimmt der Beitrag als Ausgangspunkt, um einen Überblick über die unterschiedlichen gesetzlichen Vorgaben an eine Datenverarbeitung im Gesundheitskontext zu vermitteln. Der Beitrag nähert sich der Frage an, welche rechtlichen, organisatorischen und technischen Hürden die medizinische Praxis nehmen muss, um die digitalen Erkenntnisse aus ePA, DiGA und sonstigen Medizinprodukten interessengerecht und zielgerichtet in Diagnostik und Forschung zu nutzen.

Bei der Suche nach Antworten gehen wir sowohl auf geltendes Recht – wie die DSGVO oder den Data Governance Act – ein, stellen aber auch die vielfältigen Neuerungen vor, die sich pro futuro aus aktuellen Reformvorschlägen der EU-Kommission für Digitalgesetze (u. a. KI-Verordnung, Data Act, European Health Data Space) abzeichnen. Welche Anforderungen gibt das Recht für elektronische Patientenakten, digitale Gesundheitsanwendungen, softwaregestützte Medizinprodukte, Datenintermediäre sowie europäische Datenräume vor? Neben der systematischen

[7] Es lassen sich sicherlich auch weitere Formen der Datenverarbeitung dem Kontext der „datengetriebenen Medizin" zuordnen. Die Aufzählung erhebt insoweit keinen Anspruch auf Vollständigkeit, sondern dient in erster Linie dazu, die unterschiedlichen Rechtsfragen und Regulierungsansätze zu strukturieren.

Darstellung des Regelungsinhalts der einzelnen Gesetzgebungsvorhaben mit Bezug zur datengetriebenen Medizin nehmen wir die Frage in den Fokus, wie sich die unterschiedlichen Rechtsgebiete, die jeweils einzelne Aspekte der datengetriebenen Medizin regeln, systematisch zusammendenken und in einen kohärenten Rechtsrahmen überführen lassen.

So viel vorweg: Dieses Unterfangen wird sich als herausfordernd erweisen, da die einzelnen Rechtsakte unterschiedliche rechtsdogmatische, terminologische und systematische Ansatzpunkte wählen. Für Normadressat:innen erweist es sich deshalb als große Herausforderung, die rechtlichen Vorgaben für ihre Produkte, Verarbeitungsvorgänge und Dienstleistungen zu verstehen und umzusetzen.

Als Ausweg aus dem unklaren Verhältnis zwischen den einzelnen Rechtsakten, deren Schnittmengen, Reichweiten und Anwendungsbereiche nicht trennscharf sind, schlagen wir eine „Systematisierung von unten" vor – und zwar über die technische Standardisierung. Über das Regelungsinstrument der „harmonisierten Standards", das sich als Ausdruck des *New Legislative Frameworks* in vielen der Rechtsakte der EU wiederfindet, lassen sich die rechtlichen Vorgaben bis hin zu Designstandards für Produkte und Dienstleistungen herunterbrechen. Bei der Überführung der harmonisierten Standards in konkrete technische Lösungen wirken oftmals Expert:innen aus den Unternehmen und externe Dritte mit, die Recht, Standards und Technik überblicken. Als Ausdruck einer „Systematisierung von unten" entstehen im Zusammenspiel der unterschiedlichen gesetzlichen Domänen des Produkt-, Infrastruktur- und Daten(raum)rechts kohärente technische Standards, die im Ergebnis rechtskonforme Geschäftsmodelle begünstigen. Dafür bedarf es aber sowohl Anpassungen im Prozess und Selbstverständnis der Legistik, als auch im Umgang der EU-Kommission und der zuständigen Aufsichtsbehörden mit den Regulierungsinstrumenten der harmonisierten Standards und gemeinsamen Spezifikationen.

Im Bereich der Datenerhebung (II.) beleuchtet der Beitrag zunächst die allgemeinen datenschutzrechtlichen Voraussetzungen, um Gesundheitsdaten zu erheben und zu analysieren (II. 1.). Ein Anwendungsfall sind medizinische Apps, die Patienten zur Diagnose und Therapie einsetzen. Den Rechtsrahmen für solche digitalen Gesundheitsanwendungen bilden die sozialrechtlichen Vorgaben für DiGAs (II. 2.) ebenso wie das Medizinprodukterecht (II. 3.). Nutzen App-Entwickler:innen maschinelles Lernen oder andere Formen der Künstlichen Intelligenz, müssen sie pro futuro auch die europäische KI-Verordnung berücksichtigen (II. 4.). Eine dauerhafte Speicherung bereits erhobener Patientendaten (III.) erfolgt etwa in der elektronischen Patientenakte (III. 1.). Ferner hat die Europäische Union mit dem Data Governance Act (DGA) Voraussetzungen für Datenvermittlungsdienste geschaffen (III. 2.). Der Beitrag geht der Frage nach, ob die deutsche ePA einen Datenvermittlungsdienst im Sinne des DGA darstellt (III. 3.).

Einen rechtlichen Rahmen für die Akkumulation medizinischer Datenbestände (IV.) könnten einerseits die sozialrechtlichen Datentransparenzvorschriften bieten (IV. 1.), die die Weitergabe von Daten aus der ePA an die Forschung regeln. Ande-

rerseits könnte eine wirksame Anonymisierung (IV. 2.) die rechtskonforme Sammlung von medizinischen Daten für verschiedenste Zwecke erlauben. Der Beitrag beschreibt die Hürden, die einer wirksamen Anonymisierung im Gesundheitsbereich derzeit noch im Wege stehen. Anschließend widmet sich die Untersuchung den nationalen und unionalen Gesetzesvorhaben (V.), welche Forscher:innen die datengetriebene medizinische Forschung erleichtern sollen. Auf nationaler Ebene sind dies insbesondere die Pläne für ein Forschungsdatengesetz und ein Gesundheitsdatennutzungsgesetz (V. 1.). Die Kommission hat darüber hinaus Entwürfe eines Datengesetzes (V. 2. a)) und einer Verordnung für den Europäischen Gesundheitsdatenraum (EHDS-E, V. 2. b)) vorgelegt. Der EHDS-E sieht erste Regeln für die Datennutzung zur Personalisierung (VI.) vor, die der Beitrag kurz aufzeigt. Abschließend legen wir unser Konzept einer „Systematisierung von unten" näher dar (VII.), das darauf abzielt, Datennutzern im Medizinsektor pro futuro das rechtssichere Navigieren durch den Normendschungel zu erleichtern.

II. Datenerhebung im gesundheitlichen Kontext

Ob beim Arztbesuch oder bei der Selbstvermessung per Gesundheits-App: Tagtäglich erheben Leistungserbringer:innen im Gesundheitswesen oder Patient:innen selbst Daten, aus denen sich Informationen über den individuellen Gesundheitszustand herleiten lassen. Die Verarbeitung dieser Gesundheitsdaten muss dabei stets auf einer datenschutzrechtlichen Grundlage erfolgen, die sich insbesondere aus den Bestimmungen der DSGVO ergeben kann (1.). Setzen Ärzt:innen bzw. Patient:innen für die Diagnose oder Therapie auf softwarebasierte Produkte, sind die Anforderungen an digitale Gesundheitsanwendungen (2.) zu erfüllen, um in das Regime der Abrechnung mit gesetzlichen Krankenkassen zu fallen; soweit es sich etwa um eine Gesundheits-App handelt, sind grundsätzlich auch die Regeln des Medizinprodukterechts (3.) einzuhalten. Produkte, die lernfähige Softwareanwendungen implementieren, sollen nach dem Willen der Kommission künftig auch einer spezifischen KI-Regulierung unterfallen (4.).

1. Erlaubnis zur Verarbeitung personenbezogener Gesundheitsdaten

Erfassen Ärzt:innen Informationen über ihrer Patient:innen in Form von (digitalen) Daten, kann sich eine Pflicht zur Verarbeitung von Patientendaten aus vertraglichen oder versicherungsrechtlichen Dokumentationspflichten ergeben. So sehen etwa die Vorschriften über den Behandlungsvertrag (§ 630a Abs. 1 BGB) – Patient:innen und Behandelnde schließen ihn in aller Regel konkludent durch das Begeben in die Praxis und den folgenden Behandlungsbeginn ab[8] – vor, dass die Dokumentation der Behandlung in einer Patientenakte erfolgt (§ 630 f BGB).

[8] *Volker Lipp*, in: Adolf Laufs/Christian Katzenmeier/ders. (Hrsg.), Arztrecht, 8. Aufl. 2021, III. Rn. 20.

Zwar *verpflichtet* die Norm die behandelnde Person, die Dokumentation durchzuführen. Eine *Befugnis* zur Datenverarbeitung ergibt sich aus ihr selbst aber nicht.[9] Da es sich bei den Patient:innendaten regelmäßig um personenbezogene Daten (Art. 4 Nr. 1 DSGVO) handelt, bedarf es vielmehr einer Verarbeitungsbefugnis auf Grundlage der horizontalen Vorschriften der in Deutschland unmittelbar geltenden DSGVO.[10] So gestattet Art. 6 Abs. 1 lit. b DSGVO etwa, personenbezogene Daten zu verarbeiten, sofern dies erforderlich ist, um den Vertrag durchzuführen. Auch eine zur Durchführung des Behandlungsvertrags erforderliche Verarbeitung lässt sich im Grundsatz auf diese Vorschrift stützen.

Möchte eine im Gesundheitswesen beschäftigte Person aber besonders sensible Daten, wie etwa Gesundheits- oder genetische Daten, verarbeiten, richtet sich die Frage, ob eine Verarbeitung erlaubt ist, nach Art. 9 DSGVO: Nach dessen Abs. 1 ist die Verarbeitung sensibler Daten grundsätzlich verboten, in den Fällen des Abs. 2 aber ausnahmsweise nicht untersagt. Für Gesundheitsdaten gelten also strengere Regelungen für eine Verarbeitung durch verantwortliche Stellen. Die DSGVO definiert Gesundheitsdaten als Daten, die sich auf die körperliche oder geistige Gesundheit beziehen (Art. 4 Nr. 15 DSGVO). Der Terminus ist dabei im Grundsatz weit zu verstehen, sodass auch körperliche Leistungsdaten wie Puls- und Blutdruckwerte mit einzubeziehen sind.[11] Unabhängig davon, ob Ärzt:innen bzw. das Pflegepersonal Blutdruckwerte klassisch mit einem manuellen Messgerät erfassen und händisch in die ePA eintragen oder ob Radiolog:innen Röntgen- bzw. CT-Aufnahmen des Brustkorbs mittels KI-Anwendungen etwa auf durch Covid-19 hervorgerufene Lungenläsionen[12] untersuchen: Wann immer Leistungserbringer:innen Gesundheitsdaten von Patient:innen verarbeiten, bedürfen sie dazu einer Verarbeitungserlaubnis aus Art. 9 Abs. 2 DSGVO.

Eine Datenanalyse u. a. zur Gesundheitsvorsorge, der medizinischen Diagnostik und der Behandlung im Gesundheitsbereich gestattet Art. 9 Abs. 2 lit. h DSGVO, so-

[9] Vgl. etwa *Carsten Dochow*, in: ders./Bert-Sebastian Dörfer/Bernd Halbe et al. (Hrsg.), Datenschutz in der ärztlichen Praxis, 2019, S. 35.

[10] Die DSGVO verfolgt das Prinzip des Verbots mit Erlaubnisvorbehalt, sodass die Verarbeitung personenbezogener Daten grundsätzlich verboten ist, es sei denn sie ist ausdrücklich erlaubt (Art. 6 Abs. 1 DSGVO), *Benedikt Buchner/Thomas Petri*, in: Jürgen Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 3. Aufl. 2020, Art. 6 DSGVO Rn. 11; *Albert Ingold*, in: Gernot Sydow/Nikolaus Marsch (Hrsg.), DS-GVO/BDSG, 3. Aufl. 2022, Art. 7 DSGVO Rn. 8. Den Begriff des „Verbots mit Erlaubnisvorbehalt" für die vorliegende Konstellation, in der nicht eine administrative Stelle die Erlaubnis in wenigen Fällen gesondert erteilt, (dogmatisch) ablehnend *Marion Albers/Raoul-Darius Veit*, in: Heinrich Amadeus Wolff/Stefan Brink/Antje von Ungern-Sternberg (Hrsg.), BeckOK Datenschutzrecht, Stand: 1. 8. 2023, Art. 6 DSGVO Rn. 11.

[11] *Eike Michael Frenzel*, in: Boris P. Paal/Daniel A. Pauly (Hrsg.), DS-GVO/BDSG, 3. Aufl. 2021, Art. 9 DSGVO Rn. 15.

[12] *Stephanie Harmon/Thomas Sanford et al.*, Artificial Intelligence for the detection of COVID-19 pneumonia on chest CT using multinational datasets, Nat Commun 11 (2020), 4080; *Annette Feldmann*, Dortmunder Ärzte spüren mit KI Lungenschäden durch Covid-19 auf, RuhrNachrichten.de vom 20. 12. 2020.

weit die Verarbeitung für diese Zwecke erforderlich ist. Die Verarbeitung kann eine verantwortliche Stelle aber nicht unmittelbar auf Art. 9 Abs. 2 lit. h DSGVO stützen. Denn zum einen beinhaltet die Norm eine Öffnungsklausel, die der deutsche Gesetzgeber etwa allgemein mit § 22 Abs. 1 Nr. 1 lit. b BDSG, aber auch mit spezifischen datenschutzrechtlichen Regelungen der Sozialgesetzbücher ausgefüllt hat: So lassen sich bspw. die Regelungen, wonach Vertragsärzte der gesetzlichen Krankenversicherung verpflichtet sind, für die Abrechnung relevante Leistungsdaten aufzuzeichnen (§ 294 SGB V) und an die Krankenversicherungen zu übermitteln (§ 295 Abs. 1 SGB V), auf diese Öffnungsklausel stützen.[13] Zum anderen gestattet es Art. 9 Abs. 2 lit. h DSGVO, personenbezogene Daten auf Grundlage „eines Vertrags mit einem Angehörigen eines Gesundheitsberuf" zu verarbeiten: Sofern ein Behandlungsvertrag zustande gekommen ist, können Ärzt:innen Gesundheitsdaten auch direkt unter Rückgriff auf diese Variante des Erlaubnistatbestands verarbeiten.[14]

Sollen Patientendaten über die ärztliche Individualversorgung hinaus indes (auch) anderen Zwecken zugutekommen, bedarf es dafür spezifischer Erlaubnistatbestände. Weitere Ausnahmen vom grundsätzlichen Verarbeitungsverbot für Gesundheitsdaten greifen etwa bei öffentlichen Gesundheitsbelangen (Art. 9 Abs. 2 lit. i DSGVO)[15], bei wissenschaftlicher Forschung und statistischen Zwecken (Art. 9 Abs. 2 lit. j DSGVO)[16] oder im Falle einer ausdrücklichen Einwilligung der betroffenen Person (Art. 9 Abs. 2 lit. a DSGVO)[17].

Unabhängig von der Art der Verarbeitung sind zusätzlich immer die Grundsätze des Art. 5 DSGVO zu beachten. So legt etwa der Zweckbindungsgrundsatz (Art. 5 Abs. 1 lit. b DSGVO) fest, dass der Verantwortliche einzelne Daten in der Regel nur zu einem anderen Zweck, der mit dem ursprünglichen Erhebungszweck vereinbar ist, weiterverarbeiten darf.[18] Der Grundsatz der Speicherbegrenzung (Art. 5

[13] Vgl. *Thilo Weichert*, in: Kühling/Buchner (Fn. 10), Art. 9 DSGVO, Rn. 60.

[14] *Marian Arning/Tobias Born*, in: Nikolaus Forgó/Marcus Helfrich/Jochen Schneider (Hrsg.), Betrieblicher Datenschutz, 3. Aufl. 2019, Kap. 2 Rn. 34.

[15] Anders als bei Art. 9 Abs. 2 lit. h DSGVO setzt lit. i ein öffentliches Interesse an der Verarbeitung der Gesundheitsdaten voraus.

[16] Der Unionsgesetzgeber möchte den Forschungsbegriff der DSGVO weit verstanden wissen (ErwGrd. 159 S. 2 DSGVO). Nach Stimmen in der Literatur soll dieser auch privat finanzierte Forschung einbeziehen, sofern diese sich nach wesentlichen Grundsätzen freier wissenschaftlicher Methodik richtet, vgl. *Martini/Matthias Hohmann*, Der gläserne Patient: Dystopie oder Zukunftsrealität?, NJW 2020, S. 3573 (3576). Wissenschaftliche Forschung könnte aber dann nicht (mehr) vorliegen, wenn der Erkenntnisgewinn wirtschaftlichen Interessen untergeordnet ist, wie etwa bei der bloßen unternehmerischen Produktentwicklung, vgl. *Weichert*, Die Forschungsprivilegierung in der DS-GVO, ZD 2020, S. 18 (19).

[17] Die Einwilligung in die Verarbeitung ist nicht deckungsgleich mit der Einwilligung in die Behandlung i. S. d. § 630d BGB. Sollen beide Einwilligungen mithilfe eines Schriftstücks erfolgen, muss die Formulierung so gewählt sein, dass die beiden Einwilligungssachverhalte klar voneinander getrennt sind (Art. 7 Abs. 2 S. 1 DSGVO).

[18] Vgl. dazu umfassend *Gabriele Buchholtz/Rainer Stentzel*, in: Sibylle Gierschmann/Katharina Schlender/Stentzel et al. (Hrsg.), DSGVO, 2018, Art. 5 Rn. 31 ff.

Abs. 1 lit. e DSGVO) begrenzt die Dauer, während der die verarbeitende Person die Daten speichern darf: Speichern darf er oder sie nur, solange dies erforderlich ist, um den konkreten Erhebungszweck zu erreichen. Allerdings sehen beide Grundsätze Ausnahmen für wissenschaftliche Forschungszwecke vor: Der Unionsgesetzgeber hat die Weiternutzung von Daten, die ein Verantwortlicher im Behandlungskontext erhoben hat, für Forschungszwecke bewusst privilegiert.[19]

Einen möglichen Ansatzpunkt, um konkret nachzuweisen, dass eine Gesundheitsanwendung die datenschutzrechtlichen Anforderungen der DSGVO einhält, böten die Vorschriften über die Zertifizierung (Art. 42 DSGVO). Konkret enthält Art. 42 Abs. 1 DSGVO eine Aufforderung u. a. an Mitgliedstaaten, Aufsichtsbehörden und EU-Kommission, die Entwicklung datenschutzspezifischer Zertifizierungsverfahren und von Datenschutzsiegeln zu fördern. Solche Auditverfahren gehen für Verarbeiter mit dem Vorteil einher, ihre Datenverarbeitungsregime von unabhängigen Stellen überprüfen zu lassen und so etwa Haftungsgefahren zu verringern.[20] Für Hersteller:innen und Anbieter:innen verbindet sich mit einer Zertifizierung der Anreiz, mit der – wenn auch nur indiziell wirkenden – Bestätigung der Datenschutzkonformität ihrer Produkte werben zu können; Kund:innen, welche die Software erwerben, könnten durch die unabhängige Bestätigung der Konformität ihre Haftungsrisiken minimieren.[21] Trotz großen Interesses aus der unternehmerischen Praxis ist die Entwicklung und Genehmigung von Zertifizierungsstandards zuletzt nur langsam vorangeschritten.[22] Für den Bereich der Auftragsdatenverarbeitung hat die Landesbeauftragte für Datenschutz und Informationsfreiheit NRW jüngst erstmals in Deutschland und der EU einem privaten Unternehmen Kriterien für die Datenschutz-Zertifizierung genehmigt.[23] Im Bereich der datengetriebenen Medizin gibt es indes noch keine Datenschutzsiegel oder -zertifikate, auf die sich Verantwortliche stützen könnten. Die datenschutzrechtliche Praxis wäre gut beraten, die zu Verfügung stehenden Instrumente in interdisziplinären Kraftakten staatlicher und privater Akteure künftig stärker mit Leben zu füllen.

[19] Ebd., Art. 5 Rn. 34; *Martini/Hohmann* (Fn. 16), S. 3576.

[20] *Nicolas Raschauer*, in: Sydow/Marsch (Fn. 10), Art. 42 DSGVO Rn. 2 ff.

[21] *Matthias Bergt/Paulina Pesch*, in: Kühling/Buchner (Fn. 10), Art. 42 DSGVO Rn. 4.

[22] Vgl. *Frederick Richter*, Zertifizierung unter der DS-GVO, ZD 2020, S. 84 (86 f.).

[23] *LDI NRW*, LDI NRW genehmigt erste deutsche Kriterien für Datenschutz-Zertifizierung, https://www.ldi.nrw.de/ldi-nrw-genehmigt-erste-deutsche-kriterien-fuer-datenschutz-zertifizierung [Abruf: 29. 11. 2022]; siehe auch *EuroPriSe*, EuroPriSe Cert GmbH is the first private company in the EU with certification criteria approved by the competent supervisory authority, https://www.euprivacyseal.com/EPS-en/news/n/12278/europrise-cert-gmbh-is-the-first-private-company-in-the-eu-with-certification-criteria-approved-by-the-competent-supervisory-authority [Abruf: 29. 11. 2022].

2. Digitale Gesundheitsanwendungen

Um digitale Gesundheitsanwendungen (sog. DiGAs) in den Leistungskatalog der gesetzlichen Krankenversicherungen aufzunehmen, hat das Digitale-Versorgung-Gesetz (DVG)[24] Sonderregelungen für die DiGA in das SGB V eingeführt. Der Gesetzgeber hat u. a. ein Anspruch der Versicherten auf Versorgung mit DiGAs (§ 33a Abs. 1 SGB V) geschaffen, der unter dem Schlagwort „Apps auf Rezept" eine gewisse mediale Verbreitung gefunden hat.[25] Spezialregelungen für die – notwendigerweise stattfindende – Verarbeitung personenbezogener Daten durch DiGAs hat das DVG indes nicht statuiert.

DiGA definiert der Gesetzgeber als jedes Medizinprodukt der Risikoklassen I oder IIa[26], dessen Hauptfunktion auf digitalen Technologien beruht und das u. a. dazu dient, Krankheiten zu erkennen, zu überwachen, zu behandeln oder zu lindern (§ 33a Abs. 1 S. 1 SGB V).[27] Patient:innen können den Anspruch auf eine DiGA gegenüber ihrer Versicherung geltend machen, wenn die gewünschte DiGA im DiGA-Verzeichnis des Bundesinstituts für Arzneimittel und Medizinprodukte (BfArM)[28] geführt ist und die Verwendung entweder ärztlich angeordnet oder von der Krankenkasse genehmigt ist (§ 33a Abs. 1 S. 2 SGB V). Um eine App in das DiGA-Verzeichnis aufnehmen zu lassen, muss der Hersteller u. a. nachweisen, dass Sicherheits-, Funktionstauglichkeits- und Qualitätsanforderungen für Medizinprodukte erfüllt sind, aber auch, dass Anforderungen an Datenschutz und Datensicherheit gewährleistet sind und dass die DiGA positive Versorgungseffekte generiert (§ 139e Abs. 2 S. 2 SGB V).

Die Regelungen des SGB V zu DiGAs und DiGA-Verzeichnis konkretisiert die Digitale Gesundheitsanwendungen-Verordnung (DiGAV) des Bundesgesundheitsministeriums.[29] So enthält etwa § 3 Abs. 1 DiGAV eine Verschränkung zum Rechtsgebiet der Medizinprodukte (dazu sogleich III.): Eine medizinproduktrechtliche CE-Kennzeichnung gilt grundsätzlich als Nachweis dafür, dass eine Anwendung die erforderlichen Sicherheits- und Funktionstauglichkeitserfordernisse erfüllt. In der DiGAV finden sich auch besondere datenschutzrechtliche Bestimmungen: § 4 DiGAV gestattet die Verarbeitung durch DiGAs nur auf Grundlage einer Einwilli-

[24] Gesetz für eine bessere Versorgung durch Digitalisierung und Innovation (Digitale-Versorgung-Gesetz – DVG) vom 9. 12. 2019, BGBl. I S. 2562.

[25] Vgl. etwa *Britta Beeger/Thiemo Heeg*, Holpriger Start für die „Apps auf Rezept", FAZ vom 29. 7. 2021, S. 25.

[26] § 33a Abs. 2 SGB V, vgl. zu den Risikoklassen die Ausführungen unten unter 3.

[27] Neben dem Hauptanwendungsfeld Gesundheits-Apps sind somit grundsätzlich auch andere Formen von Software umfasst, vgl. auch *Alexandra Jorzig/Lukas Kellermeier*, Besondere datenschutzrechtliche Anforderungen an Gesundheitsapps auf Rezept (DiGA), MedR 2021, S. 976 (976).

[28] Vgl. dazu § 139e SGB V und die konkretisierenden Vorschriften der § 20 ff. DiGAV.

[29] Digitale Gesundheitsanwendungen-Verordnung vom 8. 4. 2020 (BGBl. I S. 768), die zuletzt durch Artikel 3 des Gesetzes vom 20. 12. 2022 (BGBl. I S. 2793) geändert worden ist. Eine entsprechende Verordnungsermächtigung findet sich in § 139e Abs. 9 SGB V.

gung und nur zu bestimmten Zwecken (§ 4 Abs. 1 S. 1 DiGAV). Neben dem bestimmungsgemäßen Gebrauch und dem Nachweis positiver Versorgungseffekte ist die Verarbeitung etwa in engen Grenzen[30] auch zur Weiterentwicklung der App erlaubt.[31]

Als Hemmschuh eines hohen Schutzniveaus der Nutzer:innen einer DiGA erweist es sich indes, dass ein Verstoß gegen die Vorgaben des § 4 DiGAV für sich genommen keinen Datenschutzverstoß darstellt, sondern lediglich die Aufnahme in das DiGA-Verzeichnis hindert.[32] Denn der Verordnungsgeber wollte mit § 4 Abs. 2 DiGAV gerade keinen besonderen Erlaubnistatbestand i. S. d. Art. 9 Abs. 2 lit. h DSGVO schaffen, sondern primär für verschreibungsfähige DiGA die zulässige Datenverarbeitung auf die ausdrückliche Einwilligung des Art. 9 Abs. 2 lit. a DSGVO beschränken.[33] Dies ist gesetzessystematisch konsequent, stellt die Vollzugspraxis zwischen den unterschiedlichen Aufsichtsbehörden aber vor erhebliche Herausforderungen. Denn sofern klare Spezifikationen für Gesundheits-Apps bereits auf der Grundlage der DSGVO fehlen, drohen die Vorgaben im Bereich des Medizinprodukterechts und aus der DiGAV die Komplexität – und damit Rechtsunsicherheit – in der Praxis weiter zu erhöhen.

3. Medizinprodukterecht

Die Medizinprodukte-Verordnung[34] etabliert nicht nur für digitale Gesundheitsanwendungen, sondern für alle Medizinprodukte Regelungen zum Inverkehrbringen, der Bereitstellung auf dem Markt und der Inbetriebnahme (Art. 1 Abs. 1 MP-VO). Unter den weiten Produktbegriff des Medizinprodukterechts fallen (neben sämtlichen Instrumenten, Apparaten etc.) auch Softwareanwendungen. Ob es sich bei einem konkreten Produkt auch um ein *Medizin*produkt handelt, hängt maßgeblich von der Zweckbestimmung des Herstellers ab: Erklärt etwa der Anbieter eines Fitnessarmbands, dass das Produkt für Menschen bestimmt ist und den in Art. 2 Nr. 1 MP-VO genannten Zwecken dienen soll, zu denen u. a. der Diagnose, Verhütung, Überwachung, Vorhersage, Prognose und Behandlung von Krankheiten zählen, liegt ein Medizinprodukt vor – sonst nicht.[35] Daneben sind bestimmte Anwendungen vom Anwendungsbereich der MP-VO vollständig ausgenommen, insbesondere Arz-

[30] So muss die darauf bezogene Einwilligung gesondert erfolgen (§ 4. Abs. 2 S. 2 DiGAV).

[31] Es gilt insoweit das Kopplungsverbot des Art. 7 Abs. 4 DSGVO, vgl. dazu *Jorzig/Kellermeier* (Fn. 27), S. 982.

[32] *Jorzig/Kellermeier* (Fn. 27), S. 982 f.

[33] *Kristina Schreiber/Bernadette Gottwald*, Gesundheits-Apps auf Rezept, Die neue Datenschutzprüfung im Digitale-Versorgung-Gesetz, ZD 2020, S. 385 (388).

[34] Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates vom 5. April 2017 über Medizinprodukte, zur Änderung der Richtlinie 2001/83/EG, der Verordnung (EG) Nr. 1223/2009 und zur Aufhebung der Richtlinien 90/385/EWG und 93/42/EWG des Rates, ABl. L 117/1 (im Folgenden: MP-VO).

[35] Die Rechtsprechung sieht aber eine Willkürkontrolle vor, vgl. BGH, MPR 2014, S. 60 (61).

neimittel sowie In-vitro-Diagnostika, welche die eigenständige In-vitro-Diagnostika-Verordnung (VO 2017/746) reguliert.[36]

Datenverarbeitende Software kann im Medizinproduktekontext in drei Facetten eine Rolle spielen. Sie ist entweder Bestandteil eines medizinischen Apparats (sog. *embedded software*). Als Beispiel kann eine Software dienen, die fest in einem CT-Gerät verbaut ist, Informationen verarbeitet und auf dem integrierten Bildschirm des Geräts darstellt. Software kann ein Hersteller aber auch alleinstehend ohne Hardware (sog. *standalone software*) ausliefern. Für solche alleinstehende Medizinprodukte-Software hat sich der Terminus *Software as a Medical Device* (SaMD) herauskristallisiert. Darunter fallen etwa medizinische Bildauswertungsprogramme, die sich auf Praxisrechnern installieren lassen, aber auch eine DiGA, etwa zur Behandlung depressiver Erkrankungen. Drittens kann Software im Medizinproduktekontext auch bloßes Zubehör zu einem Medizinprodukt sein.[37] Eine solche Zubehör-Software kann etwa Software sein, die lediglich die Hardware eines Produkts steuert (etwa das Display einer elektrischen Waage) und weder einen medizinischen Zweck erfüllt noch selbst Informationen generiert.[38]

Für sämtliche Softwaretypen gelten sowohl die materiellen Anforderungen, welche die MP-VO allgemein für „Produkte“[39] aufstellt, als auch die softwarespezifischen Sicherheits- und Leistungsanforderungen, die sich aus Art. 5 Abs. 2 i. V. m. Anhang I Abschnitt 17 MP-VO ergeben. So muss Software nicht nur zu wiederholbaren und zuverlässigen Ergebnissen kommen, sondern auch eine Leistung entsprechend ihrer bestimmungsgemäßen Verwendung gewährleisten (Anhang I Abschnitt 17.1 MP-VO) und nach dem Stand der Technik entwickelt sein (Anhang I Abschnitt 17.2 MP-VO).

Die MP-VO fußt gesetzesdogmatisch auf einem risikobasierten Ansatz. Die Regelungsdichte orientiert sich dabei jeweils an den möglichen Folgen potenziell risikoreicher Handlungen – die konkreten, ausdifferenzierten Vorgaben an ein Produkt hat der Gesetzgeber an das konkret vermutete Risiko angepasst.[40] Die MP-VO kategorisiert Medizinprodukte vor diesem Hintergrund in vier Risikoklassen (I, IIa, IIb, III) mit jeweils aufsteigendem Risiko, an die sie unterschiedliche Anforderungen

[36] Vgl. Art. 1 Abs. 6 MP-VO.

[37] Zubehör ist jeder Gegenstand, der bestimmungsgemäß zusammen mit einem Medizinprodukt Verwendung findet und entweder dessen Zweckbestimmung ermöglicht oder die medizinische Funktion gezielt unterstützt (Art. 2 Nr. 2 MDR).

[38] *Medical Device Coordination Group*, MDCG 2019 – 11 – Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR, 2019, S. 5.

[39] Unter dem Sammelbegriff „Produkte“ fasst die MP-VO u. a. Medizinprodukte und Zubehör zusammen (Art. 1 Abs. 4 MP-VO).

[40] *Ulrich Gassner*, Dimensionen der Risikoregulierung im Medizinproduktrecht, MPR 2020, S. 162 (167).

knüpft. So fällt Software[41], die zur Unterstützung bei Diagnose- und Therapieentscheidungen dient oder physiologische Prozesse überwachen soll, grundsätzlich in die Klasse IIa. Droht bei Parameteränderung eine Gesundheitsverschlechterung bzw. unmittelbare Gefahr, ist die Klasse IIb einschlägig. Kann die Entscheidung der Software gar den Tod oder eine irreversible Gesundheitsverschlechterung verursachen, ist das Produkt in die Klasse III einzuordnen (Anhang VIII Regel 11 MP-VO).

Die risikobasierte Klassifizierung hat u. a. Auswirkungen auf das Konformitätsbewertungsverfahren, das Hersteller durchführen müssen, bevor sie ihr Produkt in den Verkehr bringen (Art. 52 MP-VO). Mit diesem Instrument bewertet grundsätzlich der Hersteller selbst, also in einem rein internen Compliance-Verfahren, ob sein Produkt mit den Vorschriften der MP-VO übereinstimmt. Bei den Klassen IIa, IIb und III ist hingegen stets die Mitwirkung einer staatlichen autorisierten Prüforganisation erforderlich, der sog. Benannten Stelle.[42] Sobald das herstellende Unternehmen das Konformitätsbewertungsverfahren erfolgreich durchgeführt hat, darf es das Produkt mit einem CE-Zertifikat versehen. Allerdings muss es dann auch sicherstellen, dass es neben der MP-VO auch andere Vorschriften, die die CE-Kennzeichnung vorsehen, erfüllt (Art. 20 Abs. 6 MP-VO). In der Praxis verbinden sich damit erhebliche Herausforderungen, insbesondere für kleine und mittlere Unternehmen.

Die Konformität mit den Anforderungen der MP-VO muss der Hersteller aber weder gleichsam aus dem hohlen Bauch noch notwendigerweise unter kostspieliger Mitwirkung externer Beratungsfirmen bewerten, sondern kann sich für den Nachweis auch auf technische Standards berufen. Bei den sog. harmonisierten Normen i. S. d. Art. 8 Abs. 1 UAbs. 1 MP-VO handelt es sich um Europäische Normen (EN), auf deren Fundstelle ein entsprechender Eintrag im Amtsblatt der Europäischen Union verweist. Sie stimmen inhaltlich regelmäßig auch mit korrespondierenden ISO- und DIN-Normen überein.[43] Erfüllt das Produkt einen technischen Stan-

[41] Zu beachten ist aber Anhang VIII Abschnitt 3.3 S. 1 MP-VO, wonach Software, die ein Produkt steuert oder dessen Anwendung beeinflusst, derselben Klasse zugerechnet wird wie das Produkt. Für solche abhängige Software können daher auch weitere Klassifizierungsregeln maßgeblich sein.

[42] Bei der Klasse I kann der Hersteller in der Regel selbst die Konformität erklären; bei sterilen Produkten, wiederverwendbaren chirurgischen Instrumenten und Geräten mit Messfunktion ist aber ebenfalls die Mitwirkung der Benannten Stelle (Art. 53 ff. MP-VO) in begrenztem Maße erforderlich (Art. 52 Abs. 7 MP-VO). In diesem Rahmen hat der Hersteller der Benannten Stelle etwa sämtliche Informationen, die diese zur Durchführung der Konformitätsbewertung benötigt, auf Verlangen zur Verfügung zu stellen (Art. 53 Abs. 4 MP-VO). Nach Abschluss des Verfahrens stellt die Benannte Stelle eine Konformitätsbescheinigung aus (Art. 56 MP-VO). Die Benannte Stelle kann dabei etwa die Zweckbestimmung auf bestimmte Patientengruppen beschränken oder den Hersteller zur Durchführung von Studien über die klinische Nachbeobachtung verpflichten (Art. 56 Abs. 3 MP-VO).

[43] So übernimmt etwa die DIN unverändert sämtliche EN, während die ISO und das CEN parallel über die Einführung als EN- und ISO-Norm abstimmen, vgl. *Deutsches Institut für Normung*, Europäische Normen, https://www.din.de/de/din-und-seine-partner/din-in-der-welt/din-in-europa/europaeische-normen [Abruf: 30. 11. 2022].

dard, der im Amtsblatt veröffentlicht ist (harmonisierte Norm), wird die Konformität des Produkts mit den Anforderungen der MP-VO vermutet. Ferner kann die Kommission auch eigene sog. gemeinsame Spezifikationen erlassen, wenn es keine geeigneten harmonisierten Normen gibt (Art. 9 MP-VO) – sie muss dafür dann selbst die notwendige Übersetzungsleistung zwischen gesetzlichen Vorgaben und technischen Designentscheidungen übernehmen oder beauftragen.

4. KI-Regulierung

Mit dem Entwurf eines Gesetzes über Künstliche Intelligenz (engl. Artificial Intelligence Act – im Folgenden: KI-VO-E)[44] hat die Kommission eine weitere produktbezogene Regulierung vorgeschlagen. Ihre Vorgaben werden auch Auswirkungen auf KI-basierte Medizinprodukte zeitigen.

Auch der KI-VO-E folgt im Grundsatz einem risikobasierten Ansatz. Er unterscheidet im Wesentlichen zwischen gänzlich verbotenen KI-Anwendungen (Art. 5 KI-VO-E), Hochrisiko-KI-Systemen, die einem Konformitätsbewertungsverfahren unterfallen (Art. 6 KI-VO-E) und KI-Systemen, die Transparenzanforderungen erfüllen müssen. Nicht erfasste risikoarme KI-Systeme unterfallen grundsätzlich nicht der KI-Regulierung.[45]

Doch welche Technologien künftig als „System der Künstlichen Intelligenz" in den Anwendungsbereich der Verordnung fallen sollen, ist noch nicht ausgemacht. Die terminologischen Schwierigkeiten beruhen insbesondere darauf, dass weder in Wissenschaft noch Legistik bislang eine allgemeingültige, disziplinübergreifende Definition für KI-Systeme existiert.[46] Grob umreißen lässt sich Künstliche Intelligenz allenfalls als diejenige Disziplin der Informatik, die versucht, Computern menschenähnliche Fähigkeiten beizubringen.[47] Der Kommissionsentwurf hat unter „Systeme der Künstlichen Intelligenz" neben Konzepten maschinellen Lernens auch „Logik- und wissensgestützte Konzepte" und „statistische Ansätze" gefasst (Art. 3 Abs. 1 i. V. m. Anhang I KI-VO-E). Kritiker bemängeln, dass die Definition aufgrund dieser weitreichenden Formulierung zu umfassend und damit nicht sachgerecht sein könnte, da logische Konzepte nahezu jedem – auch händisch programmiertem – Computerprogramm zugrunde liegen:[48] Statt einer KI-Regulierung käme es zu

[44] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (Gesetz über Künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union, COM(2021) 206 final. Das Trilog-Verfahren läuft – Stand November 2023 – auf Hochtouren und wird voraussichtlich bis Anfang 2024 abgeschlossen sein.

[45] *Hanna Hoffmann*, Regulierung der Künstlichen Intelligenz, K&R 2021, S. 369 (370).

[46] Zum Vorschlag „lernfähige Softwarenanwendungen" als rechtlichen Grundterminus vorzusehen, siehe *Martini*, Blackbox Algorithmus, 2019, S. 113 ff.

[47] Vgl. ähnlich *Elaine Rich*, Artificial Intelligence, 1983, S. 1.

[48] *David Bomhard/Marieke Merkle*, Europäische KI-Verordnung – Der aktuelle Kommissionsentwurf und praktische Auswirkungen, RDi 2021, S. 276 (277); ähnlich *Gerald Spindler*,

horizontalen Vorschriften für jegliche Softwareanwendungen.[49] Der Rat hat diese Kritik in Teilen aufgenommen und den Anwendungsbereich in seinem Kompromissvorschlag (KI-VO-E-Rat)[50] ausschließlich auf Anwendungen mit gewissem Grad an selbstständiger Weiterentwicklung verengt: Umfasst sein sollten explizit nur Techniken des maschinellen Lernens sowie logik- und wissensgestützte Komponenten, sofern diese als Output Vorhersagen, Empfehlungen oder Entscheidungen generieren, die den Bereich, mit dem die KI interagiert, beeinflussen (Art. 3 Abs. 1 KI-VO-E-Rat). ErwGrd. 6 KI-VO-E-Rat stellt überdies klar, dass Systeme, die ausschließlich von Menschen programmierte Wenn-Dann-Regeln nutzen, nicht als KI-System gelten sollen. Das EU-Parlament hat sich für seine Definition weitgehend auf die Vorarbeiten der OECD gestützt.[51]

Den KI-VO-E-Rat dürften Stimmen, die bei einem weitgefassten *scope* der KI-Regulierung vor allem Innovations- und Wettbewerbsnachteile fürchten, im Hinblick auf die Beschränkung des Anwendungsbereichs begrüßen. Hält man sich indes vor Augen, dass auch von klassischer Software wie einem Betriebssystem teilweise erhebliche Risiken für die Privatsphäre der Nutzer:innen ausgehen können, stellt sich die Frage, ob anstelle der Beschränkung der Regulierung auf besondere Technologien nicht grundsätzlich eine über KI-Systeme hinausgehende, technologieneutrale, risikobasierte IT-Regulierung sinnvoll sein könnte.[52] Der risikobasierte Ansatz lässt es regulatorisch durchaus zu, die niedrigste Stufe weitgehend von regulatorischen Vorgaben freizuhalten, und dann nach Risikograd – und unabhängig von der konkreten Form der Programmierung, Lernfähigkeit oder Modellierung – zu differenzieren. Ein weiter Anwendungsbereich vermeidet jedenfalls tendenziell, dass findige Rechtsberater:innen und Legal Teams großer IT-Konzerne Schlupflöcher finden, um potenziell riskante Anwendungen aus dem Anwendungsbereich der KI-VO zu befreien, während kleine und mittlere Unternehmen (KMU) und Start-ups, die mit innovativen KI-Methoden arbeiten, mit der vollen Regulierungsbandbreite konfrontiert wären.

Der Vorschlag der EU-Kommission für eine Verordnung zur Regulierung der Künstlichen Intelligenz (KI-VO-E), CR 2021, S. 361 (363).

[49] Vgl. zu der Frage, ob eine horizontale Regulierung für IT-Systeme vor dem Hintergrund tradierter Marktzulassungsregimes sinnvoll sein könnte, *Kolain*, Zulassungsverfahren für Künstliche Intelligenz: Über IT-Regulierung, Impfstoffe und Covid-Tests, netzpolitik.org vom 27. 4. 2021, abrufbar unter https://netzpolitik.org/2021/zulassungsverfahren-fuer-kuenstliche-intelligenz-ueber-it-regulierung-impfstoffe-und-covid-tests/ [Abruf: 26. 7. 2023].

[50] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union – Allgemeine Ausrichtung vom 25. 11. 2022, Dok.-Nr. 14954/22.

[51] Vgl. *Luca Bertuzzi*, KI-Gesetz: Parlament einigt sich auf OECD-Definition, https://www.euractiv.de/section/digitale-agenda/news/ki-gesetz-parlament-einigt-sich-auf-oecd-definition/ [Abruf: 1. 4. 2023].

[52] Vgl. *Kolain* (Fn. 49); vgl. zur Möglichkeit, den Entwurf als „Software-Verordnung" zu verstehen, auch *Bomhard/Merkle* (Fn. 48), S. 277. Zum sog. Hiroshima AI Process der G7 Staaten für einen internationalen Code of Conduct für KI-Entwickelnde https://digital-strategy.ec.europa.eu/en/library/g7-leaders-statement-hiroshima-ai-process [Abruf: 5. 11. 2023].

Ob der Unionsgesetzgeber die vom Rat vorgeschlagene Beschränkung der KI-System-Definition umsetzt, wird gleichwohl erst der Abschluss der Trilog-Verhandlung zeigen.

Sofern Medizinprodukte aufgrund der eingesetzten Techniken dem Anwendungsbereich der Verordnung unterfallen, gelten sie grundsätzlich als Hochrisiko-KI. Denn wenn sie nach der MP-VO ein Konformitätsbewertungsverfahren unter Beteiligung einer Benannten Stelle durchlaufen müssen, gelten sie schon qua des Verweises auf die MP-VO in Anhang II Nr. 11 KI-VO-E als Hochrisiko-KI i. S. d. Art. 6 Abs. 1 KI-VO-E.

Materiell müssen Hochrisiko-KI-Systeme verschiedene Anforderungen erfüllen, z. B. ein Risikomanagementsystem vorhalten und Regelungen zu Daten-Governance und Transparenz erfüllen (Art. 8 ff. KI-VO-E). In formeller Hinsicht müssen Hersteller von Risiko-KI – ähnlich wie im Medizinprodukterecht – ein Konformitätsbewertungsverfahren (Art. 19, 43 KI-VO-E) durchlaufen, bevor sie ihr System in Betrieb nehmen. Dieser Prüfprozess ist grundsätzlich wie in der MP-VO entweder als interne Kontrolle oder unter Beteiligung einer staatlich autorisierten Organisation ausgestaltet – letztere bezeichnet der KI-VO-E als „notifizierte Stelle".

Bei KI-Medizinprodukten, die schon aufgrund ihrer Regulierung durch die MP-VO als Hochrisiko-KI gelten, müssen Hersteller[53] die besonderen Anforderungen des KI-VO-E in dem nach der MP-VO erforderlichen Konformitätsbewertungsverfahren mitprüfen (Art. 24, 43 Abs. 3 KI-VO-E). Dies bietet Anbietern von KI-Medizinprodukten zwar in verfahrensformeller Hinsicht Erleichterungen bei der Zertifizierung. Da MP-VO und KI-VO-E aber in materieller Hinsicht nicht hinreichend klar erkennbar aufeinander abgestimmt sind, sind Widersprüchlichkeiten nicht ausgeschlossen und Doppelprüfungen vorgezeichnet.[54]

Dass der Anwender nach Abschluss des Verfahrens eine CE-Kennzeichnung anbringen[55] darf, sieht auch der KI-VO-E vor (Art. 49 KI-VO-E). Ebenso verschränkt die KI-VO – im Einklang mit dem sog. New Legislative Approach der EU[56] – die

[53] Der KI-VO-E kennt grundsätzlich den Terminus des „Anbieters" (Art. 3 Nr. 2 KI-VO-E). Art. 24 KI-VO-E stellt klar, dass Hersteller von Medizinprodukten, wenn diese eine Hochrisiko-KI gemeinsam mit dem Medizinprodukt in Verkehr bringen, dieselben Pflichten treffen, die die KI-VO-E dem Anbieter auferlegt.

[54] Vgl. dazu etwa *Maria Heil*, Die neue KI-Verordnung (E) – Regulatorische Herausforderungen für KI-basierte Medizinprodukte-Software, MPR 2022, S. 1 (8 ff.).

[55] Bei Software kann die CE-Kennzeichnung etwa im Startscreen, im Hilfe-Bereich der Software oder in der mitgelieferten Gebrauchsanweisung erfolgen, vgl. für Medizinprodukte *Astrid Schulze*, Schritte zum CE-Zeichen für Medizinprodukte, johner-institut.de vom 17. 7. 2019, abrufbar unter https://www.johner-institut.de/blog/regulatory-affairs/ce-zeichen-so-bestehen-sie-das-ce-audit/ [Abruf: 1. 3. 2023].

[56] Dazu *Martin Ebers*, Standardisierung Künstlicher Intelligenz und KI-Verordnungsvorschlag, RDi 2021, S. 588; *Kolain/Gergana Baeva/Katharina Buchsbaum*, Wie können Regulierung und Standards zu vertrauenswürdiger KI beitragen?, ZVKI-Fachinformation vom

Sphären der Rechtsetzung und Standardisierung strukturell: Eine Konformitätsvermutung sieht der KI-VO-E im Gleichklang mit der MP-VO bei harmonisierten Normen (Art. 40 KI-VO-E) und gemeinsamen Spezifikationen (Art. 41 KI-VO-E) vor.

III. Dauerhafte Datenspeicherung

Regelungen zur dauerhaften Speicherung von Gesundheitsdaten finden sich auf nationaler Ebene etwa in den Vorschriften über die ePA sowie auf unionaler Ebene im Data Governance Act (DGA).

1. Elektronische Patientenakte

Mit dem Patientendatenschutzgesetz (PDSG)[57] hat der Bundesgesetzgeber im Herbst 2020 Regelungen über die ePA in das SGB V eingefügt und damit der dauerhaften elektronischen Speicherung von „Informationen, insbesondere zu Befunden, Diagnosen, durchgeführten und geplanten Therapiemaßnahmen sowie zu Behandlungsberichten" (§ 341 Abs. 1 S. 3 SGB V) den regulatorischen Boden bereitet. Die Einrichtung der digitalen Akte ist für Versicherte gleichwohl nicht verpflichtend: Sie wird nur auf freiwilligen Antrag des Versicherten von der Krankenkasse bereitgestellt (§ 341 Abs. 1 S. 1 und 2 SGB V). Als Beweggrund für die dauerhafte Speicherung nennt das Gesetz insbesondere „Zwecke der Gesundheitsversorgung, insbesondere zur gezielten Unterstützung von Anamnese und Befunderhebung" (§ 341 Abs. 1 S. 3 SGB V). Darüber lassen sich als Ziele definieren, die „Qualität, Wirtschaftlichkeit und Transparenz sowie die Qualitätskontrolle der Behandlung zu verbessern und zu ermöglichen, dass es leichter fällt, auf die Krankenhistorie des Patienten zuzugreifen, als im analogen Zeitalter der Aktenordner und Faxgeräte"[58]. Damit eine ePA dem Leitbild der „Souveränität" der Patient:innen über eigene Gesundheitsdaten entspricht, sollte es möglich sein, „bestimmte Dokumente an[zu]fordern und Zugangsrechte beschränken"[59] zu können.

Mit dem Digitalgesetz (DigiG), dessen Entwurf das das Kabinett am 30. August 2023 beschlossen hat, will die Bundesregierung die Nutzung der ePA als „Austauschplattform zwischen Leistungserbringern und dem Versicherten" (vgl. BT-Drs. 20/9048, S. 2) ab 2025 nicht mehr allein der aktiven Entscheidung der Patient:innen überlassen – sondern auf ein Opt-Out-Modell umsteigen. Wer der ePA-Nutzung nicht aktiv widerspricht, für den richtet die gesetzliche Krankenkasse eine ePA ein, in die bestimmte Datenkategorien – etwa Medikationsdaten oder Laborbefunde –

28. 7. 2022, S. 6 ff., abrufbar unter https://www.zvki.de/storage/ publications/Essay_Regulierung+Standards_ZVKI.pdf [Abruf: 1. 3. 2023].

[57] Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz – PDSG) vom 14. 10. 2022, BGBl. I S. 2115.

[58] *Kolain/Ramak Molavi*, Zukunft Gesundheitsdaten, 2019, S. 22.

[59] Ebd.

automatisiert einfließen, sofern die Versicherten auch hiergegen keinen Widerspruch eingelegt haben. Weitere „Informationsobjekte und andere Daten", die automatisiert in die ePA einfließen müssen, sofern kein Widerspruch erfolgt ist, soll das BMG per Rechtsverordnung mit Zustimmung des Bundesrats erweitern können (§ 342 Abs. 2c SGB V-E, BT-Drs. 20/9048, S. 25). Die finale Fassung des DigiG wird freilich erst nach Ende des parlamentarischen Verfahrens im Deutschen Bundestag feststehen.

2. Data Governance Act

Der Unionsgesetzgeber hat den Data Governance Act[60] aus der Taufe gehoben, um den unionsweiten Datenaustausch zu erleichtern und das Vertrauen in die gemeinsame Datennutzung zu stärken. Die Verordnung ist bereits in Kraft getreten und gilt ab dem 24. September 2023 (Art. 38 DGA), ein nationales Umsetzungsgesetz befindet sich derzeit (Stand: Anfang November 2023) noch in der Ressortabstimmung (offen ist insbesondere noch die nationale Aufsichtsstruktur). Der DGA ist gleichsam eine Reaktion der Union auf das „Marktversagen" der Datenmärkte, welches sich aus dem relativ geringen Transaktionsvolumen ablesen lässt.[61] Der DGA soll dabei helfen, Netzwerkeffekten und der Monopolisierung auf dem Datenmarkt entgegenzuwirken.[62]

Als eine mögliche Lösung, um Vertrauen in neue Formen des Datenaustausches zu schaffen, hat der Gesetzgeber sog. Datenintermediäre ausgemacht:[63] Bei solchen (in der Terminologie des DGA „Datenvermittlungsdienst"[64] genannten) Mittlern handelt es sich um Dienste, mit deren Hilfe „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 […] zu ermöglichen" (Art. 2 Nr. 11 DGA). Kernaufgabe der Dienste ist also die Vermittlung zwischen Dateninhabern und Datenempfängern.[65] Der Datenvermittlungsdienst ist lediglich ein neutraler Intermediär, der zwar die technische Infrastruktur zur Verfügung stellt, die Daten aber nicht zu eigenen Zwecken nutzt (ErwGrd. 33 S. 3 DGA). Die im DSA

[60] 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), ABl. L 152/1.

[61] *Moritz Hennemann/Lukas von Ditfurth*, Datenintermediäre und Data Governance Act, NJW 2022, S. 1905 (1906). Kritisch zur aktuellen Regulierung des „Datenmarkts" durch die EU etwa *Malte Engeler*, Der Konflikt zwischen Datenmarkt und Datenschutz, NJW 2022, S. 3398 ff.

[62] Ebd.

[63] Vgl. dazu auch die Ausführungen von *Brauneck/Schmalhorst* in diesem Werk.

[64] Die engl. Sprachfassung spricht von „data intermediation service".

[65] Deshalb sind Dienste, die Daten sammeln, um selbst Lizenzen für die gesammelten Datensätze zu vergeben, ohne dass ein Vertrag zwischen Dateninhaber und Datennutzer zustande kommt, von der Definition explizit ausgenommen, Art. 2 Nr. 11 lit. a DGA.

etablierte Rolle lässt sich daher als eine als eine gesetzliche Annäherung an das in Deutschland diskutierte Modell der Datentreuhänder einstufen.[66]

Aus der regulatorischen Vogelperspektive betrachtet will der Unionsgesetzgeber mit dem DGA eine Infrastrukturschicht in die europäische Datenökonomie einziehen, die bislang noch fehlt: Datenintermediäre, die kein Eigeninteresse an den gesammelten Informationen haben dürfen, sollen sich auf dem Markt herausbilden und dadurch einen Anreiz und das notwendige Vertrauen für Bürger:innen und Unternehmen schaffen, ihre Datenbestände freigiebiger mit anderen Akteuren zu teilen. Durch das Einziehen einer neutralen, unabhängigen und klar regulierten institutionellen Schicht zwischen denjenigen, die Daten bereitstellen und erlangen wollen, will die EU implizit auch die Macht großer Internetplattformen gegenüber anderen Marktakteuren und strukturell unterlegenen Verbraucher:innen beschränken. Ob dies in der Praxis aber tatsächlich gelingt und gleichsam Datenintermediäre wie Pilze aus dem Boden schießen, ist derzeit noch offen. Es muss sich erst noch zeigen, ob der DGA eine solche Entwicklung befeuert oder am Ende ein zu starres Raster etabliert hat, das im Ergebnis aufgrund des Aufwands in der Praxis weitgehend ungenutzt bleibt.

Wer Datenvermittlungsdienste nach dem DGA anbietet, unterliegt einem formellen Anmeldeverfahren bei der zuständigen Behörde des Mitgliedstaats ihrer (Haupt-) Niederlassung (Art. 11 Abs. 1, 2 DGA). Jede An- und Abmeldung registriert die Kommission in einem öffentlichen Register der Anbieter von Datenvermittlungsdiensten (Art. 11 Abs. 10, 14 DGA). Ferner sieht Art. 12 DGA weitere materielle Anforderungen vor, die u. a. die Zweckbestimmung oder aber Maßnahmen zur Verhinderung rechtswidriger Übertragungen betreffen.[67]

Das Kapitel IV regelt hingegen den sog. Datenaltruismus, worunter der Gesetzgeber die „freiwillige gemeinsame Nutzung von Daten auf der Grundlage der Einwilligung betroffener Personen zur Verarbeitung der sie betreffenden personenbezogenen Daten oder [die] Erlaubnis anderer Dateninhaber zur Nutzung ihrer nicht personenbezogenen Daten, ohne hierfür ein Entgelt zu fordern oder zu erhalten (…) für Ziele von allgemeinem Interesse gemäß dem nationalen Recht“ versteht (Art. 2 Nr. 16 DGA). Auch beim Datenaltruismus gibt es Regelungen für Intermediäre: Juristische Personen, die sich der Förderung von Zielen von allgemeinem Interesse verschrieben haben, können sich unter gewissen Voraussetzungen als anerkannte datenaltruistische Organisation eintragen lassen (Art. 18 ff. DGA). Dies hat u. a. zur Folge, dass die Organisation von den Anforderungen an Datenvermittlungsdienste befreit ist. Die Regelungen zum Datenaltruismus sollen also letztlich sog. Datenspenden

[66] *Daniel Tolks*, Die finale Fassung des Data Governance Act – Erste Schritte in Richtung einer europäischen Datenwirtschaft, MMR 2022, S. 444 (446); jedenfalls als „Unterfall solcher Dienste“ erachten die Datentreuhand *Louisa Specht-Riemenschneider/Aline Blankertz et al.*, Die Datentreuhand – Ein Beitrag zur Modellbildung und rechtlichen Strukturierung zwecks Identifizierung der Regulierungserfordernisse für Datentreuhandmodelle, MMR-Beil. 6/2021, S. 25 (32).

[67] *Tolks* (Fn. 66), S. 446.

ohne kommerzielles Interesse erleichtern. Im Gesundheitskontext ist es dann etwa möglich, dass gemeinnützige Organisationen proaktiv Daten sammeln, um die Forschung an bestimmten seltenen Krankheiten voranzutreiben.

Neben den Regelungen für Datenintermediäre und Datenaltruismus sieht der DGA in Kapitel II zusätzlich Bestimmungen zur Weiterverwendung geschützter Daten öffentlicher Stellen vor. Ähnlich wie bei „offenen Daten", deren Verwendung bereits die Open-Data-Richtlinie[68] regelt, will der Unionsgesetzgeber damit auch die Rahmenbedingungen für die Weiterverwendung solcher Daten schaffen, die mithilfe öffentlicher Gelder generiert oder gesammelt wurden und die aus verschiedenen Gründen geschützt sind.[69]

3. ePA-Anbieter als Datenvermittlungsdienst?

Anbieter der ePA sind strukturell betrachtet ebenfalls eine Art Datenintermediär und könnten als solcher unter die Bestimmungen des Data Governance Acts fallen. Bei der Einstufung als Datenvermittlungsdienst nach dem DGA ist aber bereits zweifelhaft, ob der ePA-Anbieter tatsächlich Geschäftsbeziehungen[70] zwischen Patient:innen als Dateninhaber:innen und Ärzt:innen als Datennutzer:innen „herstellt" oder ob diese sich nicht vielmehr – vergleichbar mit einer Cloud-Lösung – *inter alia* auf die gemeinsame Nutzung der ePA im Rahmen bereits bestehender Behandlungsverträge verständigen. Denn wer nur technische Werkzeuge zur gemeinsamen Datennutzung bereitstellt, die nicht der Herstellung geschäftlicher Beziehungen dienen, stellt ausdrücklich keinen Datenvermittlungsdienst dar (ErwGrd. 28 DGA). Darüber hinaus stellt Art. 2 Nr. 11 lit. d DGA klar, dass Datenvermittlungsdienste von öffentlichen Stellen, zu denen auch die gesetzlichen Krankenkassen als Körperschaften des öffentlichen Rechts gehören, keine Datenvermittlungsdienste sind, sofern diese sie ohne die Absicht anbieten, Geschäftsbeziehungen herzustellen. Im Ergebnis fallen die Grundfunktionen der ePA, welche die gesetzlichen Krankenkassen bereitstellen und faktisch von IT-Dienstleistern einkaufen, nicht in den Anwendungsbereich des DGA für Datenvermittlungsdienste.

Allerdings sieht § 363 Abs. 1 SGB V für Patient:innen die Möglichkeit vor, die Daten aus ihrer elektronischen Gesundheitsakte für Forschungszwecke freizugeben.

---

[68] Richtlinie (EU) 2019/1024 des Europäischen Parlaments und des Rates vom 20. Juni 2019 über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors, ABl. L 172/56.

[69] *Tolks* (Fn. 66), S. 445. Vgl. zum Spannungsfeld zwischen Open Data und finanziellen Zwängen der Kommunen *Martini/David Wagner/Dietrich Haußecker*, Das Datennutzungsgesetz als digitalpolitischer Ordnungsrahmen für die Monetarisierung kommunaler Daten, NVwZ-Extra 11/2022, S. 1, 2 f.

[70] Der Terminus *commercial relationship* der englischen Fassung ist überdies ein Indiz, dass der Gesetzgeber vor allem ökonomisch motivierte Datennutzungsverträge im Sinn hatte. Bei der ePA in der derzeitigen Ausgestaltung dürfte demgegenüber primär der Austausch von Daten für individuelle Gesundheitszwecke im Vordergrund stehen.

Diese Regelung zur „Datenspende“ ist somit eine nationale Regelung, die im Wesentlichen dem Konzept des Datenaltruismus entspricht.[71] Sollte eine ePA-Anbieterin sich als anerkannte datenaltruistische Organisation eintragen wollen, müsste diese u. a. ohne Erwerbszweck handeln und die Datenaltruismus-Tätigkeiten funktionell getrennt von sonstigen Aufgaben ausführen. Einer näheren Betrachtung bedürfte in dem Zusammenhang auch die Rolle des Forschungsdatenzentrums nach § 303d SGV als öffentliche Stelle, die als Dreh- und Angelpunkt zwischen Gesundheitssystem und Forschungseinrichtungen fungieren soll (dazu sogleich IV. 1.).

Festhalten lässt sich jedoch, dass die ePA samt Möglichkeit zur „Datenspende“ an die Forschung, nicht dem Idealtypus der im DGA vorgezeichneten Akteur:innen entspricht und deshalb nicht in den Anwendungsbereich der Verordnung fallen.

IV. Datenakkumulation

Eng verknüpft mit der dauerhaften Datenspeicherung mittels App oder ePA ist die Datenakkumulation, also der strukturierte Prozess, um verschiedene Einzelinformationen zu einem großen Datensatz zusammenzufügen. Solche Datensätze sind für die medizinische Forschung sehr wertvoll, da sich aus ihnen etwa bislang unbekannte statistische Korrelationen, etwa durch KI-gestützte Mustererkennung, ziehen lassen.[72] Soweit Verarbeiter personenbezogene Gesundheitsdaten akkumulieren möchten, bedürfen sie dazu einer datenschutzrechtlichen Erlaubnis auf Grundlage des Art. 9 Abs. 2 DSGVO. Auf Basis der Öffnungsklauseln hat der Bundesgesetzgeber Vorschriften zur „forschungskompatiblen ePA“ (I.) in §§ 303a ff. SGB V eingefügt. Je nach Kontext der Verarbeitung lassen sich die Vorschriften etwa auf Art. 9 Abs. 2 lit. h DSGVO, der die individuelle Gesundheitsversorgung und damit zusammenhängende Systeme im Gesundheitsbereich wie die ePA betrifft, sowie auf Art. 9 Abs. 2 lit. j i. V. m. Art. 89 DSGVO, der die Forschung mit Gesundheitsdaten betrifft, stützen.[73] Sind Gesundheitsdaten jedoch anfänglich anonym oder erfolgreich anonymisiert (II.) und weisen somit keinen Personenbezug auf, findet die DSGVO *a priori* keine Anwendung, sodass Forscher für das Sammeln dieser Daten keiner datenschutzrechtlichen Erlaubnis bedürfen.

1. Forschungskompatible ePA

Mit dem Digitale-Versorgung-Gesetz (DVG) hat der Gesetzgeber nicht nur Regelungen für die DiGA eingeführt, sondern auch weitere Reformen angestoßen. Dar-

[71] *Tolks* (Fn. 66), S. 447.

[72] Vgl. etwa *Yannick Frost*, Künstliche Intelligenz in Medizinprodukten und damit verbundene medizinprodukte- und datenschutzrechtliche Herausforderungen, MPR 2019, S. 117 (118).

[73] *Kühling/Roman Schildbach*, Die Reform der Datentransparenzvorschriften im SGB V, NZS 2020, S. 41 (45).

unter fällt etwa eine grundlegende Reform der Datentransparenzvorschriften in §§ 303a ff. SGB V, die Regelungen zur Weitergabe von Datenbeständen der Krankenkassen an die Forschung vorsehen.[74] Mit dem Entwurf für ein Gesundheitsdatennutzungsgesetz (GDNG) will die Bundesregierung nun weitere Reformschritte vornehmen, insbesondere auf ein Opt-Out-Modell bei der Weitergabe an die Forschung umstellen (vgl. BT-Drs. 20/9046).

Sollen gewisse Daten nach Maßgabe des § 363 Abs. 1 SGB V für Forschungszwecke freigegeben werden, setzt das verschiedene Abläufe in Gang. Zunächst pseudonymisiert die Krankenkasse die freigegebenen Daten und versieht sie mit einer Arbeitsnummer. In einem zweiten Schritt übermittelt sie die pseudonymisierten Daten samt Arbeitsnummer an das Forschungsdatenzentrum[75] nach § 303d SGB V sowie die Arbeitsnummer und das Lieferpseudonym an die Vertrauensstelle[76] nach § 303c SGB V.[77] Die Vertrauensstelle erstellt aus den Lieferpseudonymen periodenübergreifende Pseudonyme (also für das Lieferpseudonym jeder Person periodenübergreifend stets ein gleichbleibendes Pseudonym), aus dem sich semantisch weder auf das Lieferpseudonym noch auf die Identität der Person schließen lässt (§ 303c Abs. 2 SGB V). Die periodenübergreifenden Pseudonyme und dazugehörigen Arbeitsnummern übermittelt die Vertrauensstelle dann wiederum an das Forschungsdatenzentrum, sodass dieses die freigegebenen Daten stets mit zuvor übermittelten Daten verknüpfen, aufbereiten und an antragsberechtigte Stellen weiterleiten kann. Die Vertrauensstelle löscht sodann die Daten, die zu einer Re-Identifikation führen können.[78] § 363 Abs. 8 SGB V stellt überdies klar, dass neben dem aufgezeigten Weg der „Datenspende" über das Datentransparenzverfahren Patient:innen ihre Daten auch auf der „alleinigen Grundlage einer informierten Einwilligung" der Forschung zur Verfügung stellen können.[79]

Doch auch ohne ausdrückliche Erklärung sieht § 303b Abs. 1 SGB V die Übermittlung spezifischer Daten, etwa Alter, Geschlecht, Wohnort, Kosten- und Leistungsdaten oder Vitalstatus, für begünstigte Zwecke (wie etwa der Forschung, § 303e Abs. 2 Nr. 4 SGB V) vor. Ähnlich wie bei der Datenspende sieht das Gesetz auch in diesem Fall die Übertragung – vermittelt durch den Spitzenverband Bund der Krankenkassen – von pseudonymisierten Daten an das Forschungsdatenzentrum

[74] Vgl. dazu etwa *Kolain/Molavi* (Fn. 58), S. 36 ff.; *Kühling/Schildbach* (Fn. 73), S. 41; *Weichert*, „Datentransparenz" und Datenschutz, MedR 2020, S. 539.

[75] Die Aufgaben des Forschungsdatenzentrums nimmt das BfArM wahr (§ 2 Abs. 2 DaTraV).

[76] Die Vertrauensstelle ist beim Robert-Koch-Institut angesiedelt und räumlich, technisch, organisatorisch und personell vom Forschungsdatenzentrum getrennt (§ 2 Abs. 1 DaTraV).

[77] Vgl. § 363 Abs. 3 SGB V.

[78] *Kolain/Molavi* (Fn. 58), S. 37, vgl. zu den Komplikationen effektiver Pseudonymisierung ebd. S. 54 ff.

[79] Vgl. dazu und zur Problematik der „breiten Einwilligung" in ganze Forschungsbereiche *Johannes Buchheim*, Die elektronische Patientenakte als Datenfundus für Pharmaindustrie und Gesundheitssektor, PharmR 2022, S. 546 (552).

sowie von Lieferpseudonymen an die Vertrauensstelle vor (§ 303b Abs. 3 SGB V). Gegen diese Form der Übermittlung wenden sich zwei von der Gesellschaft für Freiheitsrechte (GFF) unterstützte Eilanträge bzw. Klagen vor den Sozialgerichten Berlin und Frankfurt:[80] Die Kläger:innen kritisieren, dass die vorgesehene Form der Pseudonymisierung keinen ausreichenden Schutz vor der Reidentifizierung böte und das Gesetz überdies keine Widerspruchsmöglichkeit vorsehe.[81] Das SG Frankfurt hat der betreffenden Krankenkasse die Übermittlung der Daten des Antragstellers im Eilverfahren vorläufig untersagt.[82]

Das Forschungsdatenzentrum, das bei dem BfArM organisatorisch angegliedert ist, erweist sich bei näherem Hinsehen – trotz des Vermittlungszwecks zwischen Bereitstellenden und Forschung – nicht als Datenvermittlungsdienst im Sinne des DGA. Denn als Dienst einer öffentlichen Stelle, der nicht die Herstellung von Geschäftsbeziehungen zum Zweck hat, fällt es aus der Definition des Art. 2 Nr. 11 DGA heraus. Das Konzept des Forschungsdatenzentrums (FDZ), das neben dem FDZ für Gesundheitsdaten beim Robert-Koch-Institut etwa auch beim FDZ der Statistischen Ämter der Länder oder beim Forschungsdaten- und Servicezentrum der Bundesbank Anwendung findet, stand gleichwohl Pate für einen anderen Regelungsbereich des DGA: Die Bestimmungen zur Weiterverwendung geschützter Daten im Besitz öffentlicher Stellen des Kapitel II des DGA haben sich die deutschen Forschungsdatenzentren als bewährtes Beispiel für eine solche Regelung ausdrücklich zum Vorbild genommen.[83]

2. Anonymisierung

Neben der Pseudonymisierung, wie sie bei den Regeln zum Forschungsdatenzentrum zum Einsatz kommt, kommt auch die vollständige Anonymisierung von personenbezogenen Daten als möglicher Weg zur Datenakkumulation in Betracht. Die Anonymisierung bietet gegenüber der Pseudonymisierung den Vorteil, dass erfolgreich anonymisierte Daten, aus denen sich keine Informationen zu einer bestimmten oder bestimmbaren natürlichen Person mehr herleiten lassen, als Daten ohne Personenbe-

[80] Die Verfahren werden bei dem SG Frankfurt a. M. unter den Az. S 25 KR 932/22 ER (Eilverfahren) und S 25 KR 1222/22 DS (Hauptsacheverfahren) sowie bei dem SG Berlin unter den Az. S 220 SF 12/22 DS ER (Eilverfahren) und S 220 SF 13/22 DS (Hauptsacheverfahren) geführt.

[81] Siehe https://freiheitsrechte.org/ueber-die-gff/presse/pressemitteilungen-der-gesellschaft-fur-freiheitsrechte/pm-gesundheitsdaten [Abruf: 21. 2. 2023]. Vgl. aber zur Möglichkeit eines Widerspruchs auf Grundlage der DSGVO *Martini/Hohmann et al.*, Digitale-Versorgung-Gesetz – Widerspruch nicht ganz ausgeschlossen, netzpolitik.org vom 3. 12. 2019, abrufbar unter https://netzpolitik.org/2019/ein-bisschen-widerspruch-digitale-versorgung-gesundheitsdaten/ [Abruf: 21. 2. 2023].

[82] SG Frankfurt a. M., ZD 2023, S. 167 m. Anm. *Luisa Lorenz/Hans-Hermann Schild.*

[83] *Andreas Hartl/Anna Ludin*, Recht der Datenzugänge – Was die Datenstrategien der EU sowie der Bundesregierung für die Gesetzgebung erwarten lassen, MMR 2021, S. 534 (535); *Europäische Kommission*, Impact Assessment Report, SWD(2020), 25. 11. 2020, S. 13.

zug nicht der DSGVO unterliegen.[84] Da beim Anonymisieren die Verzweigungen der Originaldatensätze bewusst „getrimmt" werden, geht damit in aller Regel auch ein Verlust an Aussagekraft einher.

Ob der Anonymisierungsprozess als solcher, der ja im Ausgangsstadium personenbezogene Daten nutzt, aus denen er sodann die Informationen mit Personenbezug herausfiltert, eine Verarbeitung im Sinne des Art. 4 Nr. 2 DSGVO handelt, ist gleichwohl umstritten.[85] Da der Verarbeitungsbegriff der DSGVO jeglichen Umgang mit personenbezogenen Daten erfasst und die Anonymisierung eine Veränderung dieser Daten darstellt, spricht indes viel dafür, dass der Prozess der Anonymisierung einer Rechtsgrundlage bedarf.[86]

Schwierigkeiten bereitet überdies die Frage, wie sich eine rechtssichere dauerhafte Anonymisierung ohne jede Reidentifikationsgefahr technisch in einer Organisation umsetzen lässt, die vielfältige Datenbestände verarbeitet. Denn ein Personenbezug kann nach Maßgabe der DSGVO bereits dann bestehen, wenn ein Dritter über das notwendige Wissen verfügt, das die Gefahr der Identifizierung des Betroffenen mit verhältnismäßigem Aufwand wahrscheinlich macht.[87] Gerade Gesundheitsinformationen sind häufig so individuell, dass insbesondere bei Verknüpfung mit Big-Data-Datensätzen stets mit Rückschlüssen auf die betroffene Person zu rechnen ist.[88] Aus diesem Grund lässt sich aus der technischen Durchführung der Anonymisierung nicht stets auf die rechtliche Einstufung als „anonymes Datum" schließen.[89]

Weder der Unionsgesetzgeber der DSGVO noch die Aufsichtsbehörden haben bislang konkrete Vorgaben dazu gemacht, welche technischen oder organisatorischen Maßnahmen genügen, damit eine Deanonymisierung durch einen konkreten Verantwortlichen unverhältnismäßig oder ausgeschlossen ist. Es bleibt deshalb ein offenes Rätsel des Datenschutzrechts, was ein Verantwortlicher konkret tun muss, um zu gewährleisten, dass bei ihm kein personenbezogenes Datum (mehr) vorliegt. Dadurch entsteht ein enormes Maß an Rechtsunsicherheit.

Eine Möglichkeit, Daten auf hinreichende Anonymität zu prüfen, zeichnet das zweigeteilte Anyonymitätsbewertungsverfahren (*Anonymity Assessment)* von *Ko-*

[84] Vgl. ErwGrd. 26 S. 5, 6 DSGVO. Pseudonymisierte Daten gelten demgegenüber als personenbezogene Daten, da sie sich durch Verknüpfung mit zusätzlichen Informationen wieder einer natürlichen Person zuordnen lassen (ErwGrd. 26 S. 3 DSGVO).

[85] Vgl. zum Meinungsstand *Gierschmann*, Gestaltungsmöglichkeiten durch systematisches und risikobasiertes Vorgehen – Was ist schon anonym?, ZD 2021, S. 482 (484).

[86] So auch der *BfDI*, Positionspapier zur Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche, 29. 6. 2020, S. 5.

[87] *Martini/Hohmann* (Fn. 16), S. 3574 weisen darauf hin, dass Verantwortliche bei der Bewertung des Reidentifikationsrisikos womöglich auch Hackerangriffe berücksichtigen müssen.

[88] Ebd.

[89] *Kolain/Christian Grafenauer/Ebers*, Anonymity Assessment – A Universal Tool for Measuring Anonymity of Data Sets Under the GDPR with a Special Focus on Smart Robotics, 2021, S. 29.

lain/Grafenauer/Ebers vor.[90] Dieses sieht sowohl eine objektive Anonymitätsbewertung (*Objective Anonymity Score*), die das objektive Restrisiko einer Identifizierung mit statistischen Mitteln nach dem derzeitigen Stand der Technik erfasst, als auch eine subjektive Anonymitätsbewertung (*Subjective Anonymity Score*) vor, die wiederum individuelle Kriterien wie Zeit und Kosten der Deanonymisierung mit einbezieht.[91] Auch die *Stiftung Datenschutz* hat jüngst einen Praxisleitfaden und Ansatzpunkte für *Codes of Conducts* (Art. 40 DSGVO) im Bereich der Anonymisierung vorgestellt.[92] Ohne eine klare Positionierung der Aufsichtsbehörden zu den Schwellenwerten einer erfolgreichen Anonymisierung – etwa operationalisiert durch einen Zertifizierungsmechanismus nach Art. 42 DSGVO[93] – oder eine Entscheidung des Europäischen Gerichtshofs (EuGH), ist jedoch fraglich, ob die Methodiken aus der Wissenschaft den Praxistest bestehen und die Rechtsunsicherheit beseitigen können.

V. Datenauswertung im Forschungskontext

Große Datensätze, die qualitativ hochwertige Patientendaten aggregieren, könnten der medizinischen Forschung etwa dabei helfen, durch lernfähige Softwareanwendungen bislang unbekannte Korrelationen zu entschlüsseln. So ließen sich neuartige Zusammenhänge in der Diagnostik und bislang unbekannte Behandlungsmethoden entdecken. Denn Gesundheitsdatensätze lassen sich etwa auch dazu nutzen, Nebenwirkungen von Medikamenten aufzuspüren.[94] Auch wenn in der Medizin seit jeher in großer Vielzahl Daten erhoben werden, wie etwa Röntgenaufnahmen und Blutbilder, haben Forscher bislang selten hinreichenden Zugriff auf Datensätze in der Größenordnung, die sie für repräsentative Studien benötigen.[95] Um diesen Zustand zu bessern, bestehen sowohl auf nationaler Ebene (1.) als auch auf Unionsebene (2.) Pläne, den Datenzugang für Forschende zu vereinfachen.

[90] Vgl. ebd., S. 8 ff.

[91] Ebd., S. 29.

[92] https://stiftungdatenschutz.org/praxisthemen/anonymisierung [Abruf: 21. 2. 2023].

[93] *Kolain/Grafenauer/Ebers* (Fn. 89), S. 30.

[94] *Specht-Riemenschneider/Alexander Wehde*, Forschungsdatenzugang – Rahmenbedingungen, Prinzipien und Leitlinien für einen privilegierten Zugang zu Daten für Forschung und Wissenschaft, ZGI 2022, S. 3.

[95] Zwar sieht etwa die Öffnungsklausel des Art. 9 Abs. 2 lit. j DSGVO datenschutzrechtliche Privilegien für die wissenschaftliche Forschung vor, von der der Bundesgesetzgeber mit § 27 BDSG auch Gebrauch gemacht hat. Es finden sich auch in anderen Gesetzen vereinzelt „Forschungsklauseln", die der Forschung Auskunft oder Zugriff gewähren, etwa § 5a NetzDG oder § 303e SGB V. Allgemeine sektorübergreifende Regelungen für den Zugang zu Daten seitens der Wissenschaft gibt es indes bislang nicht, vgl. *Specht-Riemenschneider/Wehde* (Fn. 94), S. 4.

1. Pläne auf nationaler Ebene

Auf Bundesebene hat die Regierungskoalition in ihrem Koalitionsvertrag[96] für die laufende Legislaturperiode zwei Gesetzesvorhaben vereinbart, die den Forschungszugang zu (Gesundheits-)Daten verbessern sollen. So sieht er zum einen ein Gesundheitsdatennutzungsgesetz vor, das es der Forschung vereinfachen soll, Gesundheitsdaten „in Einklang mit der DSGVO" zu nutzen.[97] Im Zusammenhang mit dem Gesetz möchte die Bundesregierung auch eine dezentrale Forschungsdateninfrastruktur aufbauen. Ganz in diesem Sinne sieht das Bundesministerium für Gesundheit in seiner im März 2023 präsentierten Digitalisierungsstrategie vor, Dateninfrastrukturen „durch verbindliche Interoperabilitätsvorgaben unter Nutzung international anerkannter Standards"[98] zu vernetzen und zu harmonisieren. Im Hinblick auf den Datenschutz soll es nach dem Wunsch des BMG eine einheitliche federführende Datenschutzaufsicht für sämtliche länderübergreifende Forschung im Gesundheitsbereich geben.[99]

Als weiteren Baustein auf dem Weg zur besseren Verfügbarkeit gesundheitsbezogener Daten für die Wissenschaft sieht der Koalitionsvertrag den Entwurf eines Forschungsdatengesetzes vor, das den Zugang zu Daten für die öffentliche wie private Forschung „umfassend verbessern sowie vereinfachen" soll.[100] Bislang ist der Datenzugang in Deutschland auf die Forschungsdatenzentren und im medizinischen Bereich auf den Zugang zu Daten des Forschungsdatenzentrum beim BfArM nach § 303e SGB V beschränkt.[101] Möchte der Gesetzgeber ein allgemeines Forschungsdatenzugangsgesetz schaffen, muss er die unterschiedlichsten und häufig konfligierenden Interessen berücksichtigen und miteinander versöhnen. Denn dem Zugangsinteresse der Forschung stehen nicht nur die Datenschutzrechte der Patient:innen, sondern auch Urheberrechte, etwa von Studienautoren, bzw. Geschäftsgeheimnisse von Hersteller:innen und datenverarbeitenden Unternehmen gegenüber.

Konkrete Vorschläge für die mögliche regulatorische Ausgestaltung des Forschungsdatenzugangs unterbreiten *Specht-Riemenschneider/Wehde*. Sie plädieren für ein gestuftes Regulierungssystem, das sich aus einem grundrechtsunmittelbaren

[96] SPD, Bündnis 90/Grüne, FDP, Koalitionsvertrag 2021 – 2025, 7. 12. 2021.

[97] Ebd., S. 67.

[98] *Bundesministerium der Gesundheit*, Gemeinsam digital – Digitalisierungsstrategie für das Gesundheitswesen und die Pflege, 2023, S. 25.

[99] *Bundesministerium der Gesundheit*, Pressemitteilung: Bundesgesundheitsminister legt Digitalisierungsstrategie vor, https://www.bundesgesundheitsministerium.de/presse/pressemitteilungen/digitalisierungsstrategie-vorgelegt-09-03-2023.html [Abruf: 30. 3. 2023]. Siehe dazu nun den Vorschlag der Bundesregierung in § 5 des Entwurfs für ein Gesundheitsdatennutzungsgesetz (GDNG-E), BT-Drs. 20/9046, S. 16.

[100] SPD, Bündnis 90/Grüne, FDP (Fn. 96), S. 18.

[101] Vgl. *Specht-Riemenschneider/Wehde* (Fn. 94), S. 4. Der GDNG-E sieht neben der Umstellung auf ein Opt-Out-Verfahren bei der Weitergabe von Gesundheitsdaten aus der ePA an das Forschungsdatenzentrum auch eine Erweiterung der Zugriffsberechtigten auf alle natürlichen und juristischen Personen vor.

Datenzugangsanspruch, „echten" Forschungsklauseln, Regeln für Open Data, Transparenz- und Berichtspflichten sowie aus Datenzugangsgewährungserlaubnissen zusammensetzt.[102] Für den Gesundheitssektor schlagen sie ein „gemischtes System originärer Forschungsklauseln mit zentralen Datenspeichern, dezentral-zentralen Datenspeichern (…) und gänzlich dezentralen Datenspeichern"[103] vor. Wann und mit welchem Inhalt das Forschungsdatengesetz in der laufenden Legislaturperiode als Referentenentwurf in die öffentliche sowie parlamentarische Debatte Einzug finden wird, ist derzeit noch offen. Das insoweit federführende Bundesministerium für Bildung und Forschung hat ein öffentliches Konsultationsverfahren zum Forschungsdatengesetz gestartet, um sich ein möglichst umfassendes Bild von den konkreten Bedarfen der Praxis einzuholen.[104] Um Datenzugänge für die Forschung zu ermöglichen, hatte die Bundesregierung im EU-Rat auch vorgeschlagen, ein eigenes Kapitel im Data Act (Datengesetz-E, dazu sogleich II. 1.) vorzusehen, konnte dafür aber keine Mehrheit erzielen; immerhin stieß sie damit einen Prozess an, der in der allgemeinen Ausrichtung des Rates eine Öffnungsklausel für nationale Forschungsdatenzugänge auf die Daten aus vernetzten Produkten vorsieht.

2. Entwürfe der Europäischen Kommission

Auch die EU-Kommission schickt sich an, die datengetriebene Forschung durch verbesserte regulatorische Rahmenbedingungen zu unterstützen. Zu diesem Zweck hat sie sowohl den Verordnungsentwurf eines Datengesetzes (a)) als auch den Entwurf einer Verordnung über einen europäischen Gesundheitsdatenraum (*European Health Data Space*, im Folgenden: EHDS-E)[105] (b)) initiativ in den Gesetzgebungsprozess eingespeist. Während das legislative Schicksal des EHDS-E noch offen ist, haben sich Kommission, Parlament und Rat in den Trilog-Verhandlungen zum Datengesetz bereits auf einen Kompromisstext (Datengesetz-E)[106] geeinigt. Eine baldige Verabschiedung des Verordnungstexts sowie dessen Veröffentlichung im Amtsblatt steht damit zu erwarten.

[102] *Specht-Riemenschneider/Wehde* (Fn. 94), S. 8.

[103] Ebd., S. 10.

[104] https://www.bmbf.de/bmbf/shareddocs/kurzmeldungen/de/2023/03/230306-forschungsdatengesetz.html [Abruf: 30. 3. 2023].

[105] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über den europäischen Raum für Gesundheitsdaten, COM(2022) 197 final.

[106] Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair assess to and use of data (Data Act) – Analysis of the final compromise text in view to agreement, EU-Dok. Nr. 11284/23.

a) Datengesetz (*Data Act*)

Mit dem *Data Act* bezweckt die Union, Hindernisse für den Binnenmarkt für Daten abzubauen, indem sie festlegt, wer unter welchen Bedingungen und auf welcher Grundlage berechtigt ist, auf Daten zuzugreifen.[107]

Konkret sieht der Entwurf etwa in Art. 4 Abs. 1 Datengesetz-E ein Recht der Nutzenden – sie können etwa Besitzer, Mieter oder Leasingnehmer sein (Art. 2 Nr. 5 Datengesetz-E) – auf Zugang zu Daten vor, die sie bei der Nutzung eines vernetzten Produkts oder verbundenen Diensts erzeugt haben. „Vernetztes Produkt" meint jeden Gegenstand, der Daten über seine Umgebung erfassen und über einen öffentlichen elektronischen Kommunikationsdienst übermitteln kann (Art. 2 Nr. 2 Datengesetz-E), während der „verbundene Dienst" ein digitaler Dienst wie etwa Software ist, der mit dem Produkt unmittelbar verknüpft ist und den das Produkt für seine Tätigkeiten benötigt (Art. 2 Nr. 3 Datengesetz-E). Ein solches Produkt können etwa Fitnessgeräte ohne medizinische Zweckbestimmung (sog. Enhancement-Wearables), aber ausdrücklich auch Medizin- und Gesundheitsprodukte sein (ErwGrd. 14 S. 3 Datengesetz-E). Ausnahmen vom Zugangsrecht bestehen etwa bei Geschäftsgeheimnissen (Art. 4 Abs. 3 Datengesetz-E) oder mangelnder datenschutzrechtlicher Grundlage (Art. 4 Abs. 5 Datengesetz-E), weil etwa personenbezogene Daten Dritter betroffen sind.

Der Datengesetz-E geht indes auch über persönlichkeitsrelevante Aspekte des Datenteilens hinaus. Entstehen bei der Nutzung eines Produkts nicht-personenbezogene Daten, soll der Dateninhaber diese künftig nur noch auf Basis eines Vertrags mit dem Nutzer verwenden (Art. 4 Abs. 6 Datengesetz-E). Generiert oder speichert ein physisches Produkt Nutzerdaten, muss der Dateninhaber daher, wenn er diese Daten etwa zur Marktanalyse oder Produktentwicklung nutzen möchte, nach Inkrafttreten des Datengesetzes auch bei anonymen Daten eine Vereinbarung mit den einzelnen Nutzer:innen abschließen.

Für die Forschung wird das Zugangsrecht der Nutzenden insoweit interessant, als diese nach Art. 5 Datengesetz-E auch die Weitergabe an einen Dritten verlangen können. Dritter kann neben einem Unternehmen explizit auch eine Forschungseinrichtung oder gemeinnützige Organisation sein (ErwGrd. 29 S. 1 Datengesetz-E), sodass Nutzende die Wissenschaft auf dieser Basis explizit mit einer „Datenspende" bedenken können. Als Empfänger kommen aber auch Datenvermittlungsdienste oder datenaltruistische Organisationen i. S. d. DGA in Betracht.[108]

Eine besondere Pflicht, private Daten an Behörden „wegen außergewöhnlicher Notwendigkeit" weiterzugeben, regelt Kapitel V Datengesetz-E. Eine solche Notsituation sieht die Kommission dann gegeben, wenn die Daten zur Bewältigung eines öffentlichen Notstands notwendig sind (Art. 15 Abs. 1 lit. a Datengesetz-E). Ein öffentlicher Notstand liegt wiederum in einer Ausnahmesituation vor, die sich negativ

[107] ErwGrd. 4 Datengesetz-E.

[108] Dazu oben III. 2.

auf die Union oder einen Mitgliedstaat auswirken kann und die u. a. das Risiko schwerwiegender Folgen für die Lebensbedingungen oder die wirtschaftliche Stabilität birgt (Art. 2 Nr. 10 Datengesetz-E). Unter diese Definition des öffentlichen Notstands ließe sich – was kein Zufall sein dürfte – der Ausbruch der Corona-Pandemie in Europa Anfang 2020 subsumieren: Die Kommission wollte mit dem Verordnungsvorschlag explizit „Lehren aus der COVID-19-Pandemie und den Vorteilen von im Bedarfsfall leichter zugänglicher Daten“[109] ziehen. Im Ergebnis entsteht erstmals ein originärer adhoc-Zugangsanspruch öffentlicher Stellen gegenüber der Privatwirtschaft.[110]

Außerhalb des öffentlichen Notstands kann eine außergewöhnliche Notwendigkeit gegeben sein, wenn eine öffentliche Stelle aufgrund fehlender nicht personenbezogener Daten gehindert ist, ihre gesetzlich vorgesehene Aufgabe zu erfüllen und sie die Daten auch nicht anderweitig, etwa auf dem Markt zu Marktpreisen, einholen kann (Art. 15 Abs. 1 lit. b Datengesetz-E). Im Rahmen der außergewöhnlichen Notwendigkeit kann die befasste Behörde die Daten auch an im öffentlichen Interesse handelnde Forschungsinstitutionen weiterleiten, damit diese mit ihrer Expertise bei der Bewältigung der Situation unterstützen können (Art. 21 Datengesetz-E). Eine weitere Nutzung für andere (Forschungs-)Zwecke ist untersagt (Art. 21 Abs. 3 i. V. m. Art. 19 Datengesetz-E).

Im Vergleich zur Kommissionfassung sieht die finale Trilog-Fassung weitere Einschränkungen bei der Pflicht zur Datenweitergabe im Ausnahmefall vor: KMU sind nunmehr von der Auskunftspflicht ausgenommen, soweit kein öffentlicher Notstand vorliegt (Art. 15 Abs. 2 Datengesetz-E). Ebenfalls in Abweichung zur Kommissionsfassung müssen öffentliche Stellen auch im Fall eines öffentlichen Notstands nachweisen, dass sie die notwendigen Daten nicht auf andere Weise rechtzeitig und unter gleichwertigen Bedingungen beschaffen konnten (Art. 15 Abs. 1 lit. a Datengesetz-E).

Mit Regeln zur Interoperabilität europäischer Datenräume (Art. 28 Datengesetz-E) möchte der Unionsgesetzgeber darüber hinaus sicherstellen, dass der EU-weite Fluss von Daten nicht an unterschiedlichen Systemen, inkompatiblen Formaten und Schnittstellen scheitert. Hier kommt erneut die Sphäre der technischen Standardisierung ins Spiel: Erfüllen Datenraumbetreiber harmonisierte Normen, greift die Rechtsvermutung, dass sie mit den Interoperabilitätsanforderungen in Einklang stehen (Art. 28 Abs. 3 Datengesetz-E). Die Kommission soll gleichermaßen wiederum

[109] COM(2022) 68 final, Begründung S. 8.

[110] Kritik daran kommt u. a. von der DIHK, vgl. *Deutscher Industrie- und Handelskammertag*, Stellungnahme zum Vorschlag für eine Verordnung über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Datengesetz), 13. 5. 2022, S. 11 ff.: So sei das Teilen von Daten auf freiwilliger Basis, etwa auf Grundlage steuerlicher Anreize, gegenüber den in Art. 15 ff. vorgesehenen Regelungen grundsätzlich vorzugswürdig. Ferner seien die Rechtsbegriffe „außergewöhnliche Notwendigkeit“, „öffentliche Notlage“ und „andere Ausnahmesituation“ allesamt wenig konkret. Es bedürfe daher einer gesetzgeberischen Konkretisierung, in welchem zeitlichen und inhaltlichen Umfang Daten weiterzugeben seien.

gemeinsame Spezifikationen erlassen können, sofern keine einschlägigen harmonisierten Normen zur Verfügung stehen (Art. 28 Abs. 5 Datengesetz-E).

b) Europäischer Gesundheitsdatenraum

Mit dem Vorschlag zum europäischen Gesundheitsdatenraum wagt die Kommission einen ersten Aufschlag für einen bereichsspezifischen Datenraum im europäischen Binnenmarkt. Diese Idee der Datenräume („data spaces“) stammt aus der europäischen Datenstrategie[111] und soll später auf andere Bereiche (etwa Umwelt- oder Energiedaten) skaliert werden. Der Datenraum soll einerseits Einzelpersonen den Zugriff auf bzw. die Kontrolle über personenbezogenen Gesundheitsdaten erleichtern (Primärnutzung), aber auch den grenzüberschreitenden Datenaustausch sowie die Weiterverwendung für Forschungs- und gemeinnützige Zwecke (Sekundärnutzung) verbessern.[112] Der EHDS-E sieht zu diesem Zweck sektorspezifische Regelungen vor, welche die EU-Kommission als Erweiterung der horizontalen Regelungen des DGA und des Datengesetz-E versteht.[113] Harmonisierte Regeln und Datenumgebungen im Gesundheitsbereich sollen zudem auch dazu beitragen, die Entwicklung und Nutzung datengetriebener Gesundheitsdienste im Binnenmarkt zu verbessern. Regelungssystematisch untergliedert sich der Entwurf grob in die folgenden Bereiche: Vorschriften zur Primärnutzung von Daten, die insbesondere Patient:innen die Kontrolle über ihre Gesundheitsdaten ermöglichen sollen; Vorschriften zur Sekundärnutzung von Daten, welche die Bereitstellung von Daten für „andere Zwecke mit gesellschaftlichem Nutzen“ wie etwa der Forschung regeln; Vorschriften zur Verbesserung des Binnenmarkts durch einen einheitlichen Rechtsrahmen für die ePA (ErwGrd. 1 EHDS-E). Weitere Kapitel regeln etwa die Einrichtung eines Ausschusses für den Gesundheitsdatenraum (sog. EHDS-Ausschuss) sowie die Ermächtigung der Kommission, delegierte Rechtsakte zu erlassen.

Die für die Forschung relevanten Regelungen über die Sekundärnutzung verpflichten einerseits Dateninhaber, gesammelte Gesundheitsdaten bereitzustellen – dazu zählen etwa die ePA (Art. 33 EHDS-E). Dateninhaber im Sinn der EHDS-E ist jede natürliche oder juristische Person, die im Gesundheits- und Pflegesektor bzw. der Gesundheitsforschung tätig und berechtigt – etwa nach der DSGVO – oder verpflichtet ist, Gesundheitsdaten zur Verfügung zu stellen (Art. 2 Abs. 2 lit. y EHDS-E). Die „Zugangsstellen für Gesundheitsdaten“ gewähren Antragsstellern als vermittelnde Instanz Zugang zu Daten für näher spezifizierte Zwecke – wie etwa der öffentlichen Gesundheit, wissenschaftlichen Forschung, aber auch zum Training, der Erprobung oder Bewertung von KI-Systemen und Medizinprodukten (Art. 34 EHDS-E). Explizit ausgeschlossen ist die Sekundärnutzung der Daten etwa zum Schaden einer natürlichen Person, für Werbezwecke, zur Entwicklung

[111] COM(2022) 197 final, Begründung S. 1.

[112] Vgl. ebd.

[113] Ebd., S. 5.

schädlicher Produkte oder zur Änderung von Versicherungsprämien (Art. 35 EHDS-E). Die Regelungen des DGA zu Datenaltruismus ergänzt Art. 40 EHDS-E sektorspezifisch für den Gesundheitsbereich.

Der EHDS-E soll systematisch neben die Vorschriften der DSGVO treten, die insoweit unberührt bleiben und ebenso anzuwenden sind. Für den Bereich der Primärnutzung möchte die Kommission den Patient:innen gleichwohl mit Art. 3 EHDS-E ein zusätzliches sektorales Auskunftsrecht an die Hand geben, das über den datenschutzrechtlichen Auskunftsanspruch des Art. 15 DSGVO hinausgeht. Für den Bereich der Sekundärnutzung stellt ErwGrd. 37 S. 2 EHDS-E klar, dass der EHDS-E insoweit als Rechtsgrundlage für die Verarbeitung auf Grundlage der Öffnungsklauseln des Art. 9 Abs. 2 lit. g, h, i, j DSGVO gelten soll. Der Datenantragsteller soll ferner eine Rechtsgrundlage im Sinne des Art. 6 DSGVO nachweisen müssen (ErwGrd. 37 S. 3 EHDS-E). Die Privatsphäre der betroffenen Patient:innen soll nach dem Willen der Kommission regelmäßig dadurch geschützt sein, dass eine Anonymisierung der Daten[114] stattfindet (ErwGrd. 49 S. 2 EHDS-E). Wenn der Datennutzer personenbezogene Gesundheitsdaten benötigt, weil diese für die geplante Verarbeitung erforderlich sind, soll die Zugangsstelle die Daten pseudonymisieren (ErwGrd. 49 S. 4 EHDS-E). Der Bayerische Landesbeauftragte für den Datenschutz *Petri* sieht gleichwohl datenschutzrechtliche Defizite: So sehe der Verordnungsentwurf etwa nicht einmal in Ausnahmefällen ein Widerspruchsrecht vor, sodass selbst nach dem Gendiagnostikgesetz (GenDG) besonders geschützte genetische Daten weiterzuleiten seien.[115] Dass die DSGVO Anwendung finde, helfe dabei wenig, da Art. 6 Abs. 1 UAbs. 1 lit. c DSGVO für den Fall der Übermittlung zur Erfüllung einer rechtlichen Pflicht kein Widerspruchsrecht vorsehe.[116]

Um die Übertragbarkeit personenbezogener Gesundheitsdaten zu erleichtern, sieht der Entwurf zusätzliche Regelungen zur Harmonisierung und Interoperabilität von elektronischen Patientenakten und den dazugehörigen Diensten, sog. EHR-Systemen, vor. Unter elektronischer Patientenakte bzw. EHR (*Electronic Health Record*) versteht der Entwurf nicht nur die in Deutschland von den Krankenkassen angebotenen zentralen ePAs, sondern jede Sammlung elektronischer Gesundheitsdaten einer natürlichen Person, sofern diese im Gesundheitssystem für Gesundheitszwecke Verwendung findet (Art. 2 Abs. 2 lit. m EHDS-E). EHR-Systeme sind demnach jegliche Software oder Geräte, die nach dem Willen des Herstellers elektronische Patientenakten anzeigen, bearbeiten, speichern, im- und exportieren oder konvertieren (Art. 2 Abs. 2 lit. n EHDS-E). Demgegenüber sind sog. Wellness-Anwendungen (Art. 2 Abs. 2 lit. o EHDS-E), die nicht zur Verwendung im Gesundheitssystem be-

[114] Zu dem Problem, dass eine wirksame Anonymisierung bei Gesundheitsdaten kaum möglich ist, siehe oben IV. 2.

[115] *Petri*, Die primäre und sekundäre Nutzung elektronischer Gesundheitsdaten, DuD 2022, S. 413 (418).

[116] Ebd.

stimmt sind und die Nutzer etwa lediglich zum Messen ihres sportlichen Erfolgs nutzen, keine EHR-Systeme.

Für EHR-Systeme legt Anhang II EHDS-E grundlegende Anforderungen an Interoperabilität und Sicherheit fest, deren Erfüllung Hersteller mit einer Konformitätserklärung erklären müssen (Art. 17 Abs. 1 lit. d i. V. m. Art. 26 EHDS-E). Erklären Hersteller von Medizinprodukten und Hochrisiko-KI-Systemen, dass ihre Produkte mit EHR-Systemen operabel sind, müssen sie ebenfalls die Anforderungen an die Interoperabilität aus Anhang II Abschnitt 2 EHDS-E nachweisen (Art. 14 Abs. 2 und 3 EHDS-E). Der deutsche Gesetzgeber will bei der nationalen Umsetzung offenbar besonders schnell sein und hat – parallel zur Beratung des EHDS-E im EU-Rat – mit den Entwürfen für DigiG und GDNG bereits synchronisierte nationale Reformgesetze für die Primär- und Sekundärnutzung von Gesundheitsdaten vorgelegt.

VI. Personalisierung

Am Ende des „Datenkreislaufs" der datengetriebenen Medizin steht die Personalisierung, also die an den konkreten Patienten angepasste Maßnahme (bspw. Therapie). Auf Basis persönlicher Faktoren von Patienten, wie etwa Geschlecht, Alter und Vorerkrankungen, lässt sich häufig eine wirksame, maßgeschneiderte Behandlungslösung finden, die einem „one size fits all"-Ansatz überlegen ist. Es gehört seit jeher zur Aufgabe von Ärzt:innen, jede:r Patient:in die passende und individuelle beste Therapie zu empfehlen.

Der EHDS-E sieht daher in Art. 34 Abs. 1 lit. h EHDS-E auch die Datenweitergabe für Zwecke der „Bereitstellung einer personalisierten Gesundheitsversorgung" als geeigneten Zweck an. Anhand der bereitgestellten Daten anderer Patient:innen können Ärzt:innen etwa vergleichend bewerten, welche Therapien bei ähnlichen Parametern am erfolgreichsten waren und die Therapie der von ihnen zu behandelnden Person daran orientieren.

Eine Personalisierung außerhalb des regulierten Gesundheitswesens – etwa durch Apps, die keine DiGA sind, oder unzertifizierte Wearables – ist jedoch datenschutz- wie auch verbraucherschutzrechtlich mit Vorsicht zu genießen.[117]

VII. Systematisierung „von unten"

Der Überblick über die Vielzahl an gesetzlichen Neuerungen und regulatorischen Initiativen, die sich um die Frage drehen, unter welchen Voraussetzungen einzelne Akteure gesundheitsbezogene Daten generieren, auswerten, akkumulieren, speichern und weitergeben dürfen, lässt bereits erahnen: Wer sensible Gesundheitsdaten verarbeitet, sieht sich einem komplexen Regelungsgefüge ausgesetzt. Neben der blo-

[117] Vgl. etwa *Victoria Seeliger*, Qualitätskriterien für Gesundheits-Apps – Eine Analyse der bisherigen Rechtslage, GuP 2022, S. 91 (97 f.).

ßen Fülle der Rechtsakte, ihrer Detailtiefe und terminologischen Unbestimmtheit zum jetzigen Zeitpunkt, erweist sich ein Befund als besonders problematisch: Die Normgefüge der einzelnen Rechtsakte sind sowohl in materieller als auch formeller Hinsicht allenfalls teilweise aufeinander abgestimmt und bleiben in Bezug auf spezifische Verarbeitungssituationen häufig unkonkret.

Dadurch droht in der Praxis eine Entwicklung, die im schlimmsten Fall verhindert, dass Forschung, Ärzt:innen und Industrie das volle Potenzial datengetriebener Medizin heben können. Dadurch setzen sich innovative Ansätze, die womöglich das Leben von Patient:innen retten oder deren Gesundheitszustand verbessern könnten, im europäischen Binnenmarkt nicht durch – und schwappen später aus anderen Rechtsräumen mit geringen Schutzniveaus zu uns herüber. Der EU steht es deshalb besser zu Gesicht, durch eine Kombination aus horizontalen und sektorspezifischen Rechtsakten die Grundlage für eine nachhaltige und faire Datenökonomie zu legen, die dem individuellen Bedürfnis nach Privatsphäre angemessen Rechnung trägt. Dann wird im besten Fall „eHealth made in Europe" zum Markenkern für Lösungen, die Schutzinteressen der beteiligten Akteure – von Ärzt:innen über Pharmakonzerne bis hin zu Universitätskliniken und eben den einzelnen Patient:innen – durch technisch ausgefeilte Lösungen in Balance bringt. Dass weder der Staat noch private Unternehmen in der Lage sein sollten, den Einzelnen in seiner Persönlichkeit und im Hinblick auf seine gesundheitliche Verfassung vollständig zu katalogisieren, ihm aufgrund des überlegenen Wissens paternalistische Vorstellungen über ein „gutes Leben" aufzudrängen oder ihn heimlich zu vermessen und durch verhaltenspsychologisch wirksame Mittel zu lenken, ist Ausdruck der Menschenwürde.[118]

Um der bestehenden Rechtsunsicherheit zu begegnen, kann aber auch eine umfangreiche und ebenenübergreifende Deregulierung für den Bereich der Gesundheitsanwendungen keine sinnvolle Lösung sein. Denn die Sicherheit der Patient:innen ist sowohl in gesundheitlicher, als auch in persönlichkeitsrechtlicher Hinsicht grundrechtlich geschützt. Der Staat ist aufgerufen, den Einzelnen vor illegitimen Übergriffen aus dem Gesundheitswesen oder der Privatwirtschaft effektiv abzuschirmen. Vielmehr sollten die beteiligten Akteure ihre Anstrengungen darauf lenken, die abstrakten Vorgaben mit geeigneten Instrumenten bis zur Anwendungsebene herunterzubrechen – wie es in Europa etwa auch im Bereich der Zulassung zum Straßenverkehr oder im Arzneimittelrecht durch eine jahrzehntelange Rechtsentwicklung im Zusammenspiel aller gesellschaftlicher Stakeholder gelungen ist.[119] So ist im Jahre 2023 hinreichend geklärt, welche Vorgaben zu erfüllen sind, um einen Neuwagen, einen Impfstoff oder bestimmte Lebensmittel auf den Markt zu bringen – durch kluge Regulierung kann dies bei Anwendungen einer datengetriebenen Medizin in einigen Jahr(zehnt)en ähnlich sein.

[118] Dazu aus grundrechtsdogmatischer Sicht im Einzelnen *Quirin Weinzierl*, Dissertation Speyer, 2023 (i.E.).

[119] Dazu *Kolain* (Fn. 49).

Ein sinnvoller und niedrigschwelliger Weg, um die rechtlichen Vorgaben für eine datengetriebene Medizin zu systematisieren und einander inhaltlich anzugleichen, stellt eine Ausweitung bzw. verstärkte Nutzung des Konzepts der harmonisierten Normen dar. Die spätere Entwicklung und staatliche Anerkennung von Standards sollten die an der Gesetzgebung beteiligten Institutionen – ähnlich wie bei der Verankerung von Verordnungsermächtigungen oder der Befugnis delegierter Rechtsakte – als regulatorische Instrumente stets *en détail* mitdenken.

Das heißt konkret, erstens, dass die Standardisierungsorganisationen einerseits in der Lage sein müssen, jedenfalls ein Mindestmaß an Repräsentativität, Diversität und Interessenausgleich abzubilden.[120] Zivilgesellschaftliche und wissenschaftliche Akteure spielen in der Standardisierungswelt bislang noch keine tragende Rolle; oftmals fehlt ihnen der (auch finanzielle) Anreiz, sich intensiv an der Arbeit in DIN, CEN und ISO zu beteiligen. Neben den Standardisierer:innen mit engem Fokus, die etwa im Bereich KI, Blockchain oder Medizinprodukte eine detaillierte Expertise aufweisen, wird es zunehmend auch Standardisierungs-Generalist:innen geben müssen. Deren Kenntnisse lägen dann eher auf der Systematisierung zwischen verschiedenen Standardisierungsdömanen und dem generellen Zusammenspiel zwischen rechtlichen und technischen Normen. Ihnen wäre es aufgrund ihrer Kompetenzen dann auch möglich, Inkohärenzen in den materiell-rechtlichen Vorgaben zu identifizieren und ggf. nach technischen Ansatzpunkten Ausschau zu halten, um diese auf der Designebene zu überbrücken. Auf diese Weise ließen sich Unklarheiten im Zusammenspiel der Gesetze überwinden, indem auf Ebene der Standards einheitliche Lösungen entstehen, die den abstrakten Vorgaben konkret Rechnung tragen. Langfristig entsteht ein lebendiger Dialog zwischen Informatik, Recht, Philosophie und Ingenieurswissenschaften über die konkrete Umsetzung von „Ethical Design" oder „Security and Privacy by Design". Zweitens bedarf es eines klaren Verfahrens, nach dem die EU-Kommission entscheidet, ob beauftragte oder aus Eigeninitiative ergangene technische Standards den notwendigen Mindestanforderungen genügen, um im Amtsblatt veröffentlicht zu werden. Es bedarf also klarer Vorgaben dafür, unter welchen Voraussetzungen eine technische Norm in den Rang der „harmonisierten Standards" erhoben werden darf und wann es wegen geringen Schutzniveaus oder fehlender Grundrechtskonformität durch das Raster fällt. Nichts anderes gilt für „gemeinsame Spezifikationen", welche die EU-Kommission auf eigene Rechnung erstellen und verabschieden kann. Neben einer normativen Analyse, nach welchem Maßstab die EU-Kommission darüber entscheidet, ob Industriestandards den europarechtlichen Vorgaben hinreichend entsprechen, bedarf es auch klarer Verfahren und Ausschreibungsmodalitäten, um ggf. „gemeinsame Spezifikationen" schnell und mit hoher Qualität auf den Weg zu bringen.

Drittens muss bereits im legistischen Prozess ein klares Verständnis darüber herrschen, wie weit die technische Standardisierung in einzelnen Bereichen schon fort-

[120] Dafür ist entscheidend, dass „alle Interessen am ‚runden Tisch der Standardisierung' vertreten sind und Gehör finden", s. *Kolain/Baeva/Buchsbaum* (Fn. 56), S. 10.

geschritten ist und inwiefern sie sich dazu eignet, über eine Referenz in einem Rechtsakt zur Konkretisierung rechtlicher Vorgaben herangezogen zu werden.[121] Dafür bedarf es interdisziplinärer Arbeitsgruppen, die über Ebenen und Sektoren hinweg an den rechtlichen Grundlagen für eine rechtskonforme Datenökonomie arbeiten, und in konkrete Regulierungsvorschläge und -ansätze überführen. Wenn die aktuelle Bundesregierung ein „Zentrum für Legistik" plant, um die Aus- und Weiterbildung von Legist:innen (auch vor dem Hintergrund der Digitalisierung von Recht und Gesellschaft) weiter zu professionalisieren und systematisieren, ist das ein erster Schritt in die richtige Richtung.[122] Auch das angekündigte „Dateninstitut" könnte einen wichtigen Beitrag dazu leisten, die Sphären der Rechtssetzung, Gesetzesinterpretation und technischen Standardisierung besser zusammenzuführen.[123]

So erstrebenswert es auch ist, möglichst gute und klare Gesetze zu verabschieden: Die Aufteilung exekutiver Aufgaben auf verschiedene Ressorts und die Notwendigkeit politischer Kompromisse im Gesetzgebungsprozess werden auch auf absehbare Zeit dazu führen, dass Gesetze eher schnell verfasst und reformiert als gründlich systematisiert werden. Die hier vorgeschlagene Systematisierung „von unten" hat einen besonderen Reiz. Denn für unterschiedlichste Anwendungsszenarien könnten maßgeschneiderte Leitfäden entstehen, die Forschung und Industrie klare Parameter für eine rechtssichere Datenverarbeitung im Medizinbereich bieten. Zwar vermag Standardisierung bestehende materiell-rechtliche Widersprüche nicht gänzlich aufzuheben: Wesentliche Entscheidungen, etwa über Ver- und Gebote, kann nur der Gesetzgeber treffen. Sofern die Rechtsordnung bestimmte Handlungsweisen aber grundsätzlich erlaubt, kann Standardisierung indes dabei helfen, die Vorgaben der unterschiedlichen Rechtsakte so auszulegen und miteinander in Einklang zu bringen, dass sie Rechtsanwender:innen eine Art Checkliste für rechtskonforme Technikgestaltung bietet. Die Standards bieten dann eine Orientierung in der Umsetzung, die sich allein aus der Gesetzesinterpretation nicht ergäben. Im besten Fall sind sie die Klammer, die verschiedene Zulassungsregimes und Rechtsgebiete substanziell miteinander verknüpft. Eine besondere Rolle werden dabei nicht nur die zuständigen Aufsichtsbehörden spielen, sondern auch Standardisierungsorganisationen, Branchenverbände und zivilgesellschaftliche sowie wissenschaftliche Expertise.

Der Staat ist gut beraten, seine Rechtssetzung in diese Richtung noch stärker zu planen und weiterzudenken. Es greift zu kurz, ein Gesetz durch politische Kompromisse auf den Weg zu bringen – und die Implementierung weitgehend unzureichend

[121] Für den Bereich Robustheit (Art. 15 KI-VO-E) ist es etwa für KI-Systeme mehr als fragwürdig, ob die Erkenntnisse aus der Grundlagenforschung derzeit geeignet sind, auf konkrete Anwendungsfälle heruntergebrochen zu werden. Vgl. dazu EU Joint Research Center, Analysis of the preliminary AI standardisation work plan in support of the AI Act, Publications Office of the European Union, Luxembourg, 2023, S. 13 ff.

[122] Vgl. https://www.bmj.de/DE/Themen/RechtssetzungBuerokratieabbau/Legistik/Zentrum_ fuer_Legistik.html [Abruf: 17. 6. 2023].

[123] Vgl. https://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/it-des-bundes/dateninstitut/dateninstitut-artikel.html [Abruf: 17. 6. 2023].

ausgestatteten Aufsichtsbehörden, einzelnen Standardisierungsbestrebungen oder für betroffene Unternehmen sehr kostspieligen Beratungsunternehmen zu überlassen. Vielmehr sollten der Unionsgesetzgeber sowie die nationalen Gesetzgeber eine „Übersetzung von Recht in Technik" noch stärker unterstützen. Der Prozess der Legistik muss interdisziplinär gedacht werden und sich allmählich mit Leben füllen – im Bereich des Technikrechts darf die Formulierung von Gesetzentwürfen dann nicht mehr allein in Hand von Jurist:innen liegen.

Einerseits bedarf es einer möglichst weitgehenden horizontalen – also spezifisch für den einzelnen Rechtsakt –, aber auch vertikalen – also rechtsaktübergreifenden – Standardisierung, die eine staatliche Anerkennung einzelner Standards in den maßgeblichen Rechtsakten ermöglicht. Harmonisierte Standards ließen sich im Gesundheitskontext etwa für (kontextspezifische) rechtskonforme Datenverarbeitung nach der DSGVO, rechtskonforme Medizinprodukte, rechtskonforme Hochrisiko-KI, aber auch allgemein für rechtskonforme Apps, Clouds, Personalisierung, (Mindest-)Vorgaben für IT-Sicherheit, Interoperabilität und Datenübermittlung nutzen. Das geplante Dateninstitut und die zur Gesundheitsagentur umzubauende Gematik können einen wichtigen Beitrag leisten, den letzten Meter zwischen rechtlicher Norm und technischem Standard zu schließen.

Andererseits sollte der Staat zivilgesellschaftliche, wirtschaftliche und von Standardisierungsorganisationen getriebene Initiativen stärker fördern und den Nachwuchs von technikaffinen Jurist:innen sowie rechtsaffinen Techniker:innen noch besser ausbilden. Sie müssen nicht nur in Richtung IT-Unternehmen, sondern auch der medizinischen Forschung übersetzungsfähig sein. Denn es wird nur dann gelingen, eine menschenzentrierte und grundrechtskonforme digitale Transformation des Gesundheitswesens zu begünstigen, wenn Recht, Technik und Medizin eine gemeinsame Sprache finden und an einem Strang ziehen. Die Zukunftsvision sollte es sein, dass die Zulassung einer KI-gesteuerten Gesundheitsapp so klar strukturiert vonstattengeht, wie eine Zulassung eines Impfstoffs im EU-Binnenmarkt.

Die Gesetzgebung in Berlin und Brüssel läuft auf Hochtouren, um das Gesundheitswesen zu digitalisieren und den Erkenntniswert gesundheitsbezogener Datenanalysen noch stärker in die medizinische Forschung und Praxis einfließen zu lassen. Es ist zu erwarten, dass sich der „Datenkreislauf" allmählich mit rechtlichen und standardisierten Vorgaben für jeden der Abschnitte füllen wird, während sich bestehende Lücken der Rechtssicherheit allmählich schließen. So wie heutzutage kaum Zweifel daran bestehen, wie ein Kraftfahrzeug gebaut und instandgehalten werden muss, um rechtmäßig am Straßenverkehr teilnehmen zu können, sollte auch die „datengetriebene Medizin" eines Tages so klar durchdekliniert sein, dass sich Produkte und Leistungen gleichsam nach Schema F ausformen lassen. Den neuen Regelwerken Leben einzuhauchen, wird bis dahin der noch größere Kraftakt als die Verständigung auf neue Rechtsakte. Doch die Mühen hätten sich gelohnt, wenn dadurch ein digitales Gesundheitswesen entsteht, das die divergierenden Interessen ausgleicht

und neue Technologiestandards etabliert. Es wäre letztlich ein Dienst an der Freiheit – denn „wer gesund ist, hat Hoffnung und wer Hoffnung hat, hat alles".

Literatur

Gierschmann, Sibylle/*Schlender*, Katharina/*Stentzel*, Rainer/*Veil*, Winfried (Hrsg.): Kommentar Datenschutz-Grundverordnung, Köln, 2018.

Hennemann, Moritz/*Ditfurth*, Lukas von: Datenintermediäre und Data Governance Act, NJW 2022, S. 1905.

Jorzig, Alexandra/*Kellermeier*, Lukas: Besondere datenschutzrechtliche Anforderungen an Gesundheitsapps auf Rezept (DiGA), MedR 2021, S. 976.

Kolain, Michael/*Baeva*, Gergana/*Buchsbaum*, Katharina: Wie können Regulierung und Standards zu vertrauenswürdiger KI beitragen?, ZVKI-Fachinformation vom 28.7.2022, https://www.zvki.de/storage/publications/Essay_Regulierung+Standards_ZVKI.pdf (2.1.2023).

Kolain, Michael/*Grafenauer*, Christian/*Ebers*, Martin: Anonymity Assessment – A Universal Tool for Measuring Anonymity of Data Sets Under the GDPR with a Special Focus on Smart Robotics, 2021.

Kolain, Michael/*Molavi*, Ramak: Zukunft Gesundheitsdaten, Wegweiser zu einer forschungskompatiblen elektronischen Patientenakte, Berlin, Nov 2019.

Kühling, Jürgen/*Buchner*, Benedikt (Hrsg.): Datenschutz-Grundverordnung / BDSG, Kommentar, 3. Aufl., München, 2020.

Kühling, Jürgen/*Schildbach*, Roman: Die Reform der Datentransparenzvorschriften im SGB V, NZS 2020, S. 41.

Martini, Mario/*Hohmann*, Matthias: Der gläserne Patient: Dystopie oder Zukunftsrealität?, Perspektiven datengetriebener Gesundheitsforschung unter der DS-GVO und dem Digitale-Versorgung-Gesetz, NJW 2020, S. 3573.

Martini, Mario/*Hohmann*, Matthias/*Kolain*, Michael: Digitale-Versorgung-Gesetz – Widerspruch nicht ganz ausgeschlossen, netzpolitik.org vom 3.12.2019, https://netzpolitik.org/2019/ein-bisschen-widerspruch-digitale-versorgung-gesundheitsdaten/ (2.1.2023).

Paal, Boris P./*Pauly*, Daniel A. (Hrsg.): Datenschutz-Grundverordnung, 3. Aufl., München, 2021.

Petri, Thomas: Die primäre und sekundäre Nutzung elektronischer Gesundheitsdaten, DuD 2022, S. 413.

Schreiber, Kristina/*Gottwald*, Bernadette: Gesundheits-Apps auf Rezept, Die neue Datenschutzprüfung im Digitale-Versorgung-Gesetz, ZD 2020, S. 385.

Specht-Riemenschneider, Louisa/*Wehde*, Alexander: Forschungsdatenzugang, Rahmenbedingungen, Prinzipien und Leitlinien für einen privilegierten Zugang zu Daten für Forschung und Wissenschaft, ZGI 2022, S. 3.

Tolks, Daniel: Die finale Fassung des Data Governance Acts, Erste Schritte in Richtung einer europäischen Datenwirtschaft, MMR 2022, S. 444.

Weichert, Thilo: „Datentransparenz“ und Datenschutz, MedR 2020, S. 539.