Die Infrastruktur, mein digitaler Zwilling und ich: Das Individuum und die digitale Identität im Mittelpunkt des Datenkapitalismus

Oliver Vettermann

Zusammenfassung

Politisch-strategisch und konzeptionell fokussieren sich Projekte zum Aufbau von Forschungsdateninfrastrukturen auf die Gewinnung und den Erhalt von Daten. Dies lenkt jedoch ab von den darin in Form digitaler Identitäten abgebildeten Individuen. Ein Beleg dafür ist die stetige Referenz auf den nicht greifbaren Begriff der „Datensouveränität". Dieses begriffliche Vakuum füllen die Gesetzesvorhaben auf EU-Ebene nicht in einem datenschutzaffinen Sinne aus, sondern verstehen darunter das ökonomische Ziel der gleichberechtigten Teilnahme an einem Datenbinnenmarkt. Dieses Ergebnis stützt auch die Analyse der nationalen und europäischen Digital- und Datenstrategien. Der status quo honoriert das extraktive Verhalten von Forscher:innen zu Lasten der datengenerierenden Personen in einem kapitalistischen System. Zusätzlich fehlt es den Infrastruktur-Vorhaben in der Konzeption und Umsetzung an ethischem Bewusstsein, um Interessen des Gemeinwohls in den Strukturen zu verankern.

1. Einleitung

2023 war das Jahr der Dateninfrastrukturen: Die Nationale Forschungsdateninfrastruktur (NFDI) weitet mit insgesamt 26 Konsortien ihre Fühler in die verschiedenen Forschungsdisziplinen aus, verknüpft Expertise und bereitet die Verknüpfung bestehender Infrastrukturen mit der European Open Science Cloud (EOSC) vor. In einem ähnlichen Fahrwasser bereitet der European Health Data Space (EHDS) den Boden für Gesundheitsdaten in der Forschung und lässt die fortwährende Diskussion um den Broad Consent in der DSGVO neu aufleben. GAIA-X ergänzt die wissenschaftliche EOSC und will eine europäische Dateninfrastruktur schaffen, die ähnlich wie die NFDI die Datensouveränität durch ein dezentrales Netz aus Datenspeichern in ganz Europa für Unternehmen herstellen will. Neben

dem Plan in NFDI und GAIA-X, anstatt eigener auf bestehende Infrastrukturen zurückzugreifen, fällt ein weiterer gemeinsamer Aspekt auf: Der Nukleus, das datengenerierende Individuum und seine digitale Identität, wird kaum diskutiert.

Basierend auf der im Rahmen der eigenen Doktorarbeit[1] ausgearbeiteten Sicht sämtlicher, von einer Person verursachter Datenbündel als Teil ihrer digitalen Identität sollen in diesem Beitrag nationale und europäische Bestrebungen digitaler Infrastrukturen näher untersucht werden. Damit versucht sich der Beitrag an einer Meta-Analyse, wie die tatsächliche (datenschutzrechtliche) Kontrolle und in der Politik verwendete ethische Konzepte wie Vertrauen, Transparenz und Souveränität umgesetzt werden. In den Blick zu nehmen sind dabei neben der Einwilligung eines „Datensouveräns" auch die Nachvollziehbarkeit eigenen rechtlich relevanten Handelns, technische und organisatorische Maßnahmen und Sanktionsapparate. Resultierend soll dann untersucht werden, ob es einer anderen, ethischen Lesart europäischer Regelungen bedarf, um digitale Identitäten zu schützen und die subjektive bzw. individuumzentrierte Datensouveränität zu stärken. Es ergeben sich folgende, im Beitrag aufzuarbeitende Schlüsselfragen: Auf welche legislativen Grundlagen stützen sich die politischen Bestrebungen nach Transparenz, Souveränität und Vertrauen? Wie lassen sich die verschiedenen Ebenen einer Datensouveränität – nämlich subjektbezogen, geopolitisch und ökonomisch – hier einordnen? Und gelingt es kommenden und jüngeren Regelwerken der EU, den Ausgleich zwischen Infrastruktur und Individuum angemessen umzusetzen?

Mit diesem Thema soll dieser Beitrag ein Gegengewicht zum Überthema der Konferenz – „Data Sharing – Datenkapitalismus by Default?" – bilden, um das datengebende Individuum nicht aus den Augen zu verlieren.

2. Zum Begriff der digitalen Identität

Bevor sich der Untersuchung in der Sache gewidmet wird, ist eine Definition des Begriffs der digitalen Identität[2] für das weitere Verständnis nötig:

Als digitale Identitäten sind in diesem Beitrag miteinander verknüpfte Daten (dann: Teilidentität) oder Datensätze (dann: Gesamtidentität) zu

1 *Vettermann*, Der grundrechtliche Schutz der digitalen Identität, 2022.

2 Hierzu sowie im Folgenden ausführlich *Vettermann*, Der grundrechtliche Schutz der digitalen Identität, 2022 (7ff).

verstehen, die sich durch ihren hohen Aussagegehalt und Identifizierungsgrad in ihrer aggregierten Form auszeichnen. Sie bilden die analoge Identität und damit verschiedenste Wesenszüge, Emotionen und Gedanken des Menschen ab – etwa als „digitaler Zwilling"[3] zum realen Ich. Meistens sind sie mit einem Pseudonym bzw. Identifier versehen, können aber auch selbst als solches fungieren (dann: Quasi-Identifier). Die dadurch mögliche Zusammenführung von Datensätzen bildet Teile und Wesenszüge der analogen Identität ab, bezieht den Begriff des Personenprofils daher ein. Jedoch reicht der Begriff der digitalen Identität weiter, da er nicht das einzelne Profil in den Mittelpunkt stellt, sondern das Bündel aller Datenemissionen des Individuums (z.B. Accounts) selbst. Insofern sind auch anonyme bzw. anonymisierte Datensätze Teil der digitalen Identität, da sie unter gewissen Umständen ein Abbild komplettieren könnten. Ergänzt wird die inhaltliche durch eine zeitliche Abbildungsebene, da mit zunehmender Digitalisierung alltäglicher Vorgänge auch der gesamte menschliche Lebenszyklus mitzudenken ist. Mit zunehmendem Aufhalten in der digitalen Welt bilden Online-Shops, Netzwerke, usw. das analoge Selbst ab. Die Fähigkeit, hierüber aktiv verfügen zu können, wird als digitale Selbstbestimmung bezeichnet.[4] Eine dahingehende (subjektive) Datensouveränität meint also den Gehalt des Grundrechts auf informationelle Selbstbestimmung im Sinne einer eigenverantwortlichen Verfügung über Verbleib und Nutzung der „eigenen" Daten.

3. Thesen

Die einleitenden Fragen werden durch drei Thesen und ihre Analyse beantwortet: Aus dem Blickwinkel des datengebenden bzw. datenden[5] Individuums wird im Folgenden der Begriff der Datensouveränität (These 1), dessen rechtliche Umsetzung in Forschungsdatenräumen (These 2) und ihr rechtlich-ethischer Unterbau (These 3) analysiert.

3 Daher nicht gleichzusetzen mit dem Begriff in der Industrie 4.0, siehe *Müller*, ZD-Aktuell 2021, 05096.

4 Exemplarisch *Digital Autonomy Hub*, Policy Brief #4, S. 5; *Denga*, GRUR 2022, 1113 (1113) mwN.

5 Meint „daten" als Verb, stehend für „Daten produzieren/generieren". In Anlehnung an *Lisker*, Masterarbeit: Von der (Un-)Möglichkeit, digital mündig zu sein, 2023.

These 1: Die Datensouveränität ist eine Leerformel für die wirtschaftliche und forschungspolitische Anschlussfähigkeit Deutschlands.

Der Ursprung des Begriffs „Datensouveränität" lässt sich unter anderem[6] im Jahr 2017 auf die Erwähnung von Alexander Dobrindt im Bezug auf ein geplantes Datengesetz zurückführen. Das Gesetz selbst ist Gegenstand des „Strategiepapier Digitale Souveränität", mit dem das Ziel des Gesetzes und das Begriffsverständnis vorwiegend ökonomisch eingeordnet werden. Darin der Satz: „Der Schlüssel dazu ist die Datensouveränität des Einzelnen."[7] Mit „des Einzelnen" referenziert dieser Satz wie auch der Großteil der juristischen Literatur[8] die *subjektive* Lesart im Volkszählungsurteil des BVerfG, in dem die Verfügungsherrschaft über die eigenen Informationen im Mittelpunkt steht: „Im Mittelpunkt [...] stehen Wert und Würde der Person, die in freier Selbstbestimmung als Glied einer freien Gesellschaft wirkt."[9] Die Definition der Datensouveränität erscheint also zunächst als eine subjektivrechtliche, die für das schützende Grundrechtsbündel der digitalen Identität steht. Bündel, weil wegen der zunehmenden Digitalisierung des Alltags der digitale Aspekt des Persönlichkeitsrechts aus Art. 7, 8 GrCh und Art. 2 Abs. 1 iVm 1 Abs. 1 GG in die übrigen, geeigneten Grundrechte hineinstrahlt, sich in diesen verzweigt und sie verselbstständigt. Das subjektive Verständnis erscheint deshalb auch synonym zu den Begriffen „Digitale Souveränität" und „digitale Selbstbestimmung". Eine trennscharfe Definition gibt es insoweit nicht.[10]

Der subjektive Begriff hat in den letzten Jahren eine wiederholte Wandlung und Erweiterung erfahren. Wie die Facetten eines Diamanten hat die Politik die Datensouveränität auch ökonomisch, geopolitisch und nunmehr forschungsbezogen bzw. forschungspolitisch geschliffen:

Ökonomisch steht die Wertschöpfung an und aus Daten im Fokus. Distanziert vom Individuum wird sich allein dem Objekt gewidmet, dessen inhaltlichen Werte möglichst fair und transparent erschlossen werden sol-

6 Vertiefend zur Genese *Pohle/Thüer/Dammann/Winkler*, in: Kersting/Radtke/Baringhorst (Hrsg.), Handbuch Digitalisierung und politische Beteiligung.

7 Siehe https://web.archive.org/web/20171101193849/https://www.bmvi.de/SharedDocs/DE/Artikel/DG/datengesetz.html.

8 *Denga*, GRUR 2022, 1113 (1118f); *Roßnagel*, MMR 2023, 64 (64f); *Krüger*, ZRP 2016, 190 (190f).

9 BVerfGE 65, 1 (41).

10 So auch *Umweltbundesamt*, Digitale Kommune/Digitale Region, Texte 62/2023 (57); *Pohle/Thüer/Dammann/Winkler*, in: Kersting/Radtke/Baringhorst (Hrsg.), Handbuch Digitalisierung und politische Beteiligung.

len. Es handelt sich also in einem kapitalistischen System[11] um „strategische Vermögenswerte"[12], die u. a. als Tauschmittel für die Nutzung von Diensten (also Konsum) genutzt werden – daher auch: Datenkapitalismus. Profiteure sind Staat und Wirtschaft.[13] Regelmäßig werden Nutzer:innen ebenso als Profitierende gesehen, da sie sich durch das Einspeisen von Daten in den Kreislauf einbringen und ihnen je nach Perspektive unmittelbar oder zumindest mittelbar Profit zufließt.[14] Schließlich können Nutzer:innen freiwillig einwilligen („dezentrale Entscheidungsprärogative der Datensubjekte"[15]), zwischen verschiedenen Anreizen – finanziell, moralisch, technisch – wählen und so informiert entscheiden, ob sie mit den Vorzügen übereinstimmen oder nicht – ganz nach dem Vorbild der DSGVO, vgl. Art. 1 Abs. 1. Eine derartige Perspektive gewichtet das Binnenmarkt-Ziel der DSGVO allerdings höher als den grundrechtlichen (Daten-)Schutz der Personen. Schon das Setzen von Anreizen zur Motivation der Wertschöpfung beeinflusst die Freiwilligkeit, weil sie die Wahlmöglichkeit vorgibt und damit begrenzt. Sie ist stets von der Rolle des Subjekts in diesem System abhängig.[16] Die Einwilligung entpuppt sich so als responsibilisierte Form[17] der Souveränität, die systemisch keine echte Souveränität im Sinne einer Entscheidungshoheit aufweist, sondern einem Daten-Extraktivismus im digitalen Raum dient.

Geopolitisch zeigt sich die Datensouveränität dagegen als politische und staatliche Handhabe, und hat dabei die Abhängigkeiten zwischen verschiedenen Staaten und die Sicherheit Europas[18] im Blick. Diese bestehen u. a. in Lieferketten oder durch technische Bedrohungen wie Cyberangriffe. Aufgabe ist es dabei, den Schutz von Daten bzw. Informationen institutionell abzusichern[19] (auch hier: „strategische Vermögenswerte") und per Gesetz für sicherere Systeme zu sorgen – beispielsweise durch den Cyber Resilien-

11 Hierzu exemplarisch die Beispiele von *Bisges*, MMR 2017, 301 (304ff).
12 So Europäische Kommission, Digitalstrategie, 2022 (5).
13 *Denga*, GRUR 2022, 1113 (1114). Vgl. die Ziele von GAIA-X in *Schütrumpf/Person*, RDi 2022, 281 (283).
14 Zu Datennutzungsverträgen *Rosenkranz/Scheufen*, ZfDR 2022, 159 (170ff). Zum Berufsbild des Dategenerierens unter Art. 12 Abs. 1 GG siehe *Vettermann*, Der grundrechtliche Schutz der digitalen Identität, 2022 (210ff).
15 EuGH C-252/21, Rn. 143, 148f; *Denga*, GRUR 2022, 1113 (1120, 1114).
16 Hierzu *Engeler*, NJW 2022, 3398 (3403).
17 *Lisker*, Masterarbeit: Von der (Un-)Möglichkeit, digital mündig zu sein, 2023 (17ff mwN).
18 Vgl. Europäische Kommission, Digitalstrategie (5).
19 Vgl. *Kelber/Bortnikov*, NJW 2023, 2000 (2001f).

ce Act und die NIS2-Richtlinie. Diese Sicht reiht sich in das allgemeine Monitoring von staatlichen Abhängigkeiten[20] ein, in denen auch das Wissensmanagement als Datenschatz[21] erwähnt wird.

Forschungsbezogen kann die Datensouveränität dagegen als spezielle Form der subjektbezogenen Version verstanden werden. Forscher:innen finden sich in Gesprächen regelmäßig in der Position wieder, eigene Forschungsdaten teilen zu müssen und zugleich nicht aus der Hand geben zu wollen. Dabei kommt der Wunsch auf, dass „ihre" Daten lizenz- und datenschutzrechtlich geschützt werden sollen, auch wenn die gesetzlichen Anwendungsbereiche nicht greifen. Wichtig ist, die Inhalte und Schlussfolgerungen zu beanspruchen und die Lorbeeren – wissenschaftliche Credits – zu ernten. Der damit einhergehende Druck auf Forscher:innen ergibt sich ebenso aus dem Datenkapitalismus und einem stetigen Streben nach Innovation. Hierbei stehen neben Open-Data-Aspekten auch fehlende Anonymisierungsverfahren oder „der böse Datenschutz"[22] im Weg.

Forschungspolitisch dominiert die institutionelle Sicht auf Forschungsdaten, die ebenso das Teilen und Nachnutzen im Fokus hat. Die Begriffe „forschungsbezogen" und „forschungspolitisch" fallen auseinander, weil ersteres die Praxis und Forscher:innen im Fokus hat und zweiteres die übergeordnete Zielrichtung der institutionellen Forschung meint. Im Fokus stehen einzelne Forscher:innen dann nur mittelbar, z. B. wenn ihnen der Zugang zu den Forschungsdatenschätzen ermöglicht und gewährt werden soll. Das setzt jedoch auch voraus, dass sie sich von besagter eigener, subjektiver Souveränität lösen. Abseits davon zeigt sich die forschungspolitische Perspektive in der Datenverarbeitung „um des Antrags Willen", wenn sich Forschungsfragen an gesellschaftlichen Themen und entsprechenden Ausschreibungen orientieren, anstatt sich aus der Sachebene und der wissenschaftlichen Arbeitsweise selbst zu ergeben. Dieser Aspekt ist also ökonomisch, institutions- und strukturbezogen geprägt, um Deutschland international an die Spitze der Forschung „made in Germany" zu führen.

So facettenreich der Begriff damit wirkt, so leer ist er zugleich: Die gezeigten Perspektiven setzen die Erhebung und Verarbeitung von Daten und

20 *BMWi*, Schwerpunktstudie Digitale Souveränität, 2021.

21 Ähnlich *Kelber/Bortnikov*, NJW 2023, 2000 (2001).

22 Exemplarisch die Unsicherheit von Forscher:innen bei Interessenabwägungen skizzierend *Buchner*, DuD 2022, 555 (556f). Ob gemeinwohlorientierte Forschungsinteresse in der datenschutzrechtlichen Interessenabwägung pauschal „unstreitig als hoch" einzuordnen sind, ist vor dem Hintergrund einer einzelfallbezogenen Risikoabwägung streitbar.

damit eine bestehende Rechtsgrundlage voraus. Bei genauem Hinsehen fällt der Wandel von einer subjektivrechtlichen Prägung zu einer struktur- und wirtschaftsbezogenen Neigung der Begriffsverwendung hin auf, die die Interessen der Nutzer:innen als Datensubjekte und -produzent:innen vernachlässigt. Es werden Möglichkeiten zur Teilhabe am Datenmarkt gewährt und positiv herausgestellt, ohne in aktuellen Strategien brauchbare Ansätze und Vorhaben für eine ethische wie grundrechts- bzw. datenschutzkonforme Umsetzung anzureißen[23] – wie noch zu zeigen sein wird. Der Grund dafür liegt auf der Hand: Datenschutz und Datensouveränität sind unter der Einwilligung systemisch nicht vereinbar. Wie *Engeler*[24] und *Samardzic/Becker*[25] herausgearbeitet haben, führt die Einwilligung durch ihre mittlerweile stark ökonomische Prägung zwar zu Anreizen, die aber wiederum nicht zur gesetzlich angelegten Freiwilligkeit führen.[26] Die Einwilligung fungiert damit als Symbol ökonomischer Datensouveränität. Im Forschungskontext spielen forschungspolitische und ökonomische Lesart der Souveränität zusammen: Das Übermaß an Information gegenüber Betroffenen zur Erfüllung der auferlegten Transparenz führt dazu, dass die Einwilligung zunehmend schwieriger für die Forschung umzusetzen ist. Die forschungspolitische Datensouveränität übt hier entsprechend Druck auf Forscher:innen aus, mehr Daten zu verarbeiten und länger nachzunutzen. Die inhärente Dynamik eines Broad Consent, der nur vorübergehend die nicht-detaillierte Information zum Forschungskontext überwinden soll, wird daher selten zutreffend adressiert. Eher wird er glorifiziert, weil sonst keine Möglichkeit besteht, an wertvolle (Gesundheits-)Daten zu kommen.[27] Mit generativen LLM-Modellen und der öffentlichen Diskussion nachgeordneter, sekundärer Verarbeitungsformen liegt das Problem des Kontrollverlustes jedoch offen, da durch eine Einwilligung nur die primäre Verarbeitung betroffen, aber selten die Zwecke der sekundären Verarbeitung vorhergesagt werden könnte. Eine Freiwilligkeit kann sich also nur auf die primäre Verarbeitung beziehen.

Die Einwilligung als Instrument der Datensouveränität ist damit ein leeres Versprechen, im Forschungskontext Handhabe über einen Sachverhalt

23 Beispielsweise *Bundesregierung*, Datenstrategie 2023, S. 32 ohne Einbettung.
24 *Engeler*, NJW 2022, 3398ff.
25 *Becker/Samardzic*, EuZW 2020, 646.
26 Vgl. EuGH C-252/21, Rn. 143, 148f.
27 Vgl. *Spitz/Cornelius*, MedR 2022, 191 (192ff); *Medizininformatik-Initiative AG Consent*, Stellungnahme Dynamic Consent.

zu geben, von dem weder Forscher:innen noch Nutzer:innen vorher wissen können. Werkzeuge wie der Datenmanagementplan oder das Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO) können hier helfen. Bislang werden sie von Forscher:innen aber nicht als Selbstkontrolle verstanden, sondern häufig als zusätzliche Last der Dokumentation. Vertrauen und Transparenz laufen damit ins Leere. Die Datensouveränität verkommt so zur Worthülse, die den eigentlichen Kern der Privatheit und dem Schutz vor informationellen Kontextverletzungen – zeitlich, kulturell oder publikumsbezogen –[28] nicht gerecht wird. Stattdessen wird sie in wirtschaftlichen und forschungspolitischen Kontexten dazu genutzt, ökonomische Ziele zu verkörpern und Nutzer:innen eine gefühlte Selbstbestimmung zu vermitteln.

These 2: Forschungsdatenräume sind „menschenleer" und datenfreundlich konzipiert.

Die Grundlage eines Zusammenwirkens von Nutzer:innen und der Forschung besteht vor allem darin, dass ein regelmäßiger Datenfluss besteht und die Ergebnisse dieser Preisgabe sich positiv auf die Gesellschaft auswirken. Dies ist mit Blick auf Art. 179 AEUV die Grundvoraussetzung für einen Daten-Binnenmarkt im Sinne eines „free flow of data", vgl. Art. 1 Abs. 1 DSGVO. Forschung, vor allem Gesundheitsforschung, ist damit ein Katalysator für Lösungen, die in Daten-Heuhaufen verborgen sind. Das Gemeinwohl ist diesem Begriffsverständnis schon qua Forschungsfreiheit gem. Art. 13 S. 2 GrCh, Art. 5 Abs. 3 GG in die Wiege gelegt.[29] Dies setzt aber voraus, dass die Datenpreisgabe als Ausnahme und nicht Regel verstanden wird; Privatheit muss respektiert und stets an den Grenzen zu anderen Freiheiten verteidigt werden. Privatheit ist dabei die „Schaffung eines geschützten Raumes als Voraussetzung zur Persönlichkeitsentfaltung, geschützt von den invasiven Kräften einer in die Lebenswelt eindringenden Wirtschaft"[30] in Form des Datenkapitalismus. Dies gesagt, müssen auch Grundlagen wie Governance-Strukturen und Infrastrukturen abbilden, dass die Datenaufnahme und -nutzung stets ein Eindringen ist. Grundsätz-

28 *Heesen/Ammicht Quinn* et al., in: Roßnagel/Friedewald (Hrsg.), Die Zukunft von Privatheit und Selbstbestimmung, 161 (175).

29 Vgl. BVerfGE 35, 79 (114); 111, 333 (354); *Ruffert*, in: Calliess/Ruffert, EUV/AEUV, Art. 13 GrCh Rn. 7.

30 *Heesen/Ammicht Quinn* et al., in: Roßnagel/Friedewald (Hrsg.), Die Zukunft von Privatheit und Selbstbestimmung, 161 (167 mwN). Ausführlich hierzu *Sandfuchs*, Privatheit wider Willen?, 2015 (7ff).

lich kann so ein Eindringen durch das hohe Gut der Volksgesundheit und ähnliche altruistische Ziele gerechtfertigt sein – es kommt für diese Ausnahme aber stets auf den Einzelfall an.

Einen Rahmen für das Verhältnis von Datengebenden und der Forschung als Datenempfängerin sollten die aktuellen[31] europäischen und nationalen Regulierungsvorhaben bieten: Data Act, Data Governance Act, Forschungsdatengesetz sowie Gesundheitsdatennutzungsgesetz, jeweils im Einklang mit der DSGVO. Der Data Act und der Data Governance Act bilden dabei die allgemeine Regulierung von Daten ab; der Data Act bezieht sich auf die aus der Nutzung eines Produkts generierten Daten, der Data Governance Act dagegen auf die Daten in der öffentlichen Hand. Beide EU-Regelungen setzen sich also mit dem Datenzugang auseinander. Für einen ausreichenden Bezug müsste sich der EU-Rahmen aber auch mit den Betroffenenrechten auseinandersetzen. Infrastruktur und Governance-Strukturen müssen die Interessen und Rechte Betroffener sichtbar mitdenken, sei es durch Beteiligungsmöglichkeiten als Kontrolle oder menschliche Werte (z. B. Ethik, siehe hierzu These 3).

Der *Data Act*[32] adressiert vor allem Hersteller von Produkten und Bereitstellung von verbundenen Diensten (also Hard- und Software von smarten Datenanwendungen wie IoT), ihre Nutzer:innen, Dateninhaber:innen und Datenempfänger:innen. Der Begriff der Dateninhaber:in meint gem. Art. 2 Nr. 13 DA im Hinblick auf nicht-personenbezogene Daten eine damit einhergehende Handhabe über die Daten durch die produktherstellenden Unternehmen selbst. Die datengenerierende Person wird in den Erwägungsgründen (zB ErwGr 5 und 18 DA) und via Einschub in Art. 2 Nr. 5 DA als Nutzer:in beschrieben. Wenngleich es sich nicht um personenbezogene Daten handelt, stehen der Person Zugangs-, Weitergabe- und Nutzungsrechte des Kapitel II zu. Nutzer:innen werden so maßgebliche Rechte eingeräumt, allerdings zur Effektuierung des Daten-Binnenmarktes.[33] Sobald es sich um personenbezogene Daten handelt, kommen gem. ErwGr 34 DA die Rechtsgrundlagen der DSGVO hinzu, sodass es für das Datengenerieren bei Personenbezug der Daten einer Einwilligung nach Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO bedarf. Während mit Geltung der DSGVO das Risiko für personenbezogene Daten beim Verantwortlichen liegt, liegt es

31 Der Beitrag bezieht sich auf den letzten Stand im April 2024.

32 Siehe https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202302854

33 Vgl. *Funk*, CR 2023, 421 (425f).

nach dem Data Act bei den Nutzer:innen selbst: „Der Nutzer trägt die Risiken und genießt die Vorteile der Nutzung des vernetzten Produkts und sollte auch Zugang zu den von ihm generierten Daten haben. Er sollte daher berechtigt sein, aus den von diesem vernetzten Produkt und allen verbundenen Diensten generierten Daten Nutzen zu ziehen."[34] Über den Umfang an Daten und Risiken werden Nutzer:innen gem. Art. 3 Abs. 2 DA informiert. Eine Gegenleistung für eine Datenweitergabe enthält nicht die Nutzer:in, sondern die Dateninhaber:in (also das Unternehmen) als Kompensation für die technische Infrastruktur und Dienstleistung (Art. 9 DA).[35] Im Gegenzug erhält die Nutzer:in Zugriff auf die selbst generierten Daten (Art. 4 Abs. 1 DA). Nutzer:innen erhalten damit zumindest auch die Nutzung des Geräts und damit verbundener Dienste im Tausch gegen ihre Daten, was dem jüngeren Bild einer datenökonomischen Position der Verbraucher:in entspricht.[36] Dezent lässt sich der Charakter von Leistung (Daten) und Gegenleistung auch in der „Gegenseitigkeit geschlossener Verträge" über nicht-personenbezogene Daten erkennen (vgl. Art. 4 Abs. 13, Art. 1 Abs. 10 DA). Insofern widersprechen sich die Erwägungsgründe leicht im Abschnitt zur Prüfung relevanter Grundrechte, worin wegen der marktorientierten Ausrichtung der Datennutzung für Nutzer:innen durchaus ökonomische Interessen (Art. 15, 16 GrCh als Spiegelbild der Art. 12, 14 GG) benannt werden könnten.[37] Insgesamt lässt der Data Act aber neben erwähnten Möglichkeiten für Information und Teilhabe an dem generierten, nicht-personenbezogenen Datenschatz wenig Spielraum für Widerspruch/Widerruf und Abwägungen von rechtsethischen Interessen. Höchstens über den offenen Begriff der Fairness über die Nutzung wegen außergewöhnlicher Notwendigkeit (Art. 14 ff DA) lassen sich Mechanismen erkennen. Die Schwäche auf der Betroffenenseite könnte darin begründet liegen, dass mit Aktivierung des Personenbezuges dynamisch das Datenschutzrecht zur Anwendung kommt und für nicht-personenbezogene Daten primär keine grundrechtlichen Interessen aufkommen.[38]

Der *Data Governance Act* widmet sich der Weiterverwendung von Daten bestimmter Datenkategorien, die sich im Besitz der öffentlichen Hand in-

34 ErwGr 18 DA.
35 Jeden Ausgleich aufseiten der Nutzer:innen ablehnend *Funk*, CR 2023, 421 (424ff).
36 Vgl. EuGH C-252/21, Rn. 102, 143, 148ff. Auch *Gesmann-Nuissl/Meyer*, Die neue Ära des Datenhandels – in diesem Band.
37 Vgl. *Vettermann*, Der grundrechtliche Schutz der digitalen Identität, 2022 (210ff).
38 Ähnlich *Funk*, CR 2023, 421 (426).

nerhalb der Union befinden (Art. 1 Abs. 1 DGA) und installiert mit dem Datenaltrusimus und Diensten zur Datenvermittlung bei Preisgabe der Daten durch Betroffene Konzepte zur Daten-Governance. Alle Konzepte enthalten Ansätze, die Individuen in die Prozesse einzubeziehen. Einige Beispiele: Für die personenbezogenen Daten im Besitz öffentlicher Stellen sind Schutzmaßnahmen vorgesehen wie die vorherige Anonymisierung und entweder digitale oder physische Zugangsschranken (Art. 5 Abs. 3 DGA). Da die Einwilligungsmöglichkeit hier entfällt, wenn die personenbezogenen Daten per Anonymisierung aus dem Geltungsbereich des Datenschutzrechts entfernt werden, wird sie durch das Erlaubnisverfahren (Art. 5 Abs. 2, 4 und Art. 9 DGA) ersetzt. Datenvermittlungsdienste referenzieren in Art. 12 DGA auf die traditionellen Mechanismen des Datenschutzes und der informationellen Selbstbestimmung, also technische und organisatorische Maßnahmen für Daten- und IT-Sicherheit (lit. c und j), Zweckbegrenzung (lit. a), das Angebot spezifischer technischer Werkzeuge zur Erhöhung der subjektiven Datensouveränität (lit. e) sowie einen fairen, transparenten und nicht-diskriminierenden Zugriff (lit. f). Der Datenaltruismus basiert auf der freiwilligen Datenweitergabe für Zwecke, die eine datenaltruistische Organisation anbietet. Sie fußt damit auf Einwilligung und subjektiver Datensouveränität, wenngleich die nationalen Regeln zur Einrichtung einer Aufsichtsbehörde und der Verfahren (siehe Art. 16 DGA) sowie Empfehlungen zur Einwilligung (Art. 25 DGA) bis dato fehlen. Insoweit dürfte sich nicht nur hierin an der DSGVO orientiert werden, sondern auch bei der Erfüllung der Transparenzanforderungen nach Art. 20 DGA und den Vorgaben zum Schutz subjektiver Interessen der Dateninhaber:innen nach Art. 21 DGA. Informiertheit und Transparenz gepaart mit Freiwilligkeit sollen jedoch ebenso das stark ökonomisch geprägte Ziel des DGA stützen: „Daten stehen im Mittelpunkt dieses Wandels: Die von Daten vorangetriebene Innovation wird sowohl den Bürgerinnen und Bürgern der Union als auch der Wirtschaft enorme Vorteile bringen."[39] Die Governance der Bürger:innen dient damit in erster Linie der „Gestaltung, Schaffung und Aufrechterhaltung gleicher Wettbewerbsbedingungen in der Datenwirtschaft", also dem gleichberechtigten Zugang zu einem Daten-Binnenmarkt. Wie bei These 1 zeigt sich hier erneut, dass subjektive und

39 ErwGr 2 DGA.

ökonomische Datensouveränität eng miteinander verzahnt sind. Ein Indiz dafür ist das Ziel der Innovation.[40]

Der *European Health Data Space* (kurz EHDS) soll laut Entwurf einen Forschungsdatenraum speziell für Gesundheitsdaten schaffen, bestehend aus Vorschriften auf EU-Ebene, Standards und Verfahren sowie Infrastrukturen und einem Governance-Rahmen.[41] Relevante Akteure sind hier Dateninhaber:innen, Zugangsstellen für Gesundheitsdaten und Datennutzer:innen. Nach Art. 2 Abs. 2 lit. y EHDS-VO[42] lässt sich die Dateninhaber:in als natürliche oder juristische Person verstehen, die im Gesundheits- oder Pflegesektor aktiv ist oder die Forschungstätigkeiten hinsichtlich dieser Sektoren durchführt. Dennoch zielt die VO auf den Schutz natürlicher Personen, indem Rechte über Verfügbarkeit und Kontrolle gestärkt werden sollen. Konkret soll diese Stärkung durch Zugriffsrechte (zB Art. 8a EHDS-VO) oder vorgegebene Zwecke der Nutzung (Art. 33, 34 EHDS-VO) als neue Rechtsgrundlagen im Zusammenspiel mit der DSGVO gelingen. Soweit es für den EHDS nicht weiter vorgegeben ist, sind bei personenbezogenen Daten aber die Informationspflichten der Art. 13, 14 DSGVO zu erfüllen – auch bei der Sekundärnutzung. Dadurch wird das Verständnis der Forscher:innen für die eigene Verantwortung verkompliziert. Weitere Unsicherheiten produzieren die fehlende Legaldefinition der Anonymisierung und ihrer relativen bzw. volatilen Wirkung, fehlende interoperable Formate und ein Abgleich der Weiterverarbeitung nach DSGVO mit dem Konzept der Sekundärnutzung nach EHDS-VO.[43] Hevorgehoben sei zuletzt der Ausschluss des Patientenwillens: Soweit in der Trilog-Fassung ersichtlich ist gem. Art. 8h (Primärzweck) und Art. 35f EHDS-VO (Sekundärzweck) keine Einwilligung vorgesehen; alle Patient:innen werden ohne Ausweichmöglichkeit in die elektronischen Register aufgenommen. Der Gesetzgeber nimmt damit eine Abwägung vorweg, die im Einzelfall trotz Anonymisierung und Pseudonymisierung weiterhin eine Identifizierbarkeit ermöglicht.[44]

Doch wie wirkt sich all dies auf die Infrastrukturvorhaben wie GAIA-X oder NFDI aus? Konzeptionell sollten die erwähnten Infrastrukturen unter

40 Kritisch *Buccafusco/Weinstein*, Antisocial Innovation, 2023 (630ff, 623f).

41 Art. 1 Abs. 1 EHDS-VO; *Roos/Maddaloni*, RDi 2023, 225 (226).

42 Der Beitrag bezieht sich auf die vorläufige Fassung aus dem Kompromiss des Trilog, siehe https://www.consilium.europa.eu/media/70909/st07553-en24.pdf.

43 *DSK*, Stellungnahme vom 27.3.2023 – auch DuD 2023, 325; im Einzelnen *Denga*, EuZW 2023, 25 (30 f, 32 ff).

44 So *Denga*, EuZW 2023, 25 (30).

dem fragmentierten Verständnis von Privatheit, Datenschutz und Security (nach NIS2-RL und CRA) by Design bzw. Default entsprechende technische Mechanismen zum Schutz der Betroffenen vorsehen. Das wäre je nach Ansatz der Datenweitergabe vor allem mit Blick auf die European Open Science Cloud (EOSC) eine am Einzelfall ausgerichtete Silo-Lösung, in der Datensätze modular und zweckspezifisch freigegeben würden. Wegen der unterschiedlichen Ausrichtung sollten EOSC und GAIA-X unterschiedlich erreichbar sein, also z. B. nicht auf gleichen Servern liegen. Dies betrifft auch anonymisierte Identitäten aufgrund einer möglichen Auflösbarkeit. In der Realität ist GAIA-X vorwiegend als dezentrale Infrastruktur bestehender Partner konzipiert.[45] Der Fokus liegt dabei auf einer Kooperation von Privatwirtschaft, industrienaher Forschung und öffentlicher Hand.[46] Das Konzept des Datenraums von Datenraum Kultur[47] und des Datenraum Mobilität[48] setzt mit einem ähnlichen B2B-Fokus auf die Triebfedern Wertschöpfung, Innovation, Transparenz, Effizienz und Souveränität – und ist damit auf die ökonomische Datensouveränität ausgerichtet. Ergänzend wirkt insoweit die NFDI als Konstrukt, das community-driven aus der Forschung für die Forschung wächst. Im Fokus steht dabei, dass sich die Anforderungen an die Infrastruktur im Sinne einer forschungsbezogenen Datensouveränität aus der Forschung selbst ergeben. Die Umsetzung der aufgezeigten Ansätze geschieht daher stets in einem Spannungsverhältnis zwischen Recht und Bedarf.

Im Hinblick auf die Konzeption von Regulierung und Forschungsdatenräumen lässt sich also die Tendenz erkennen, dass die Infrastrukturen auf die Datenerhebung und -sammlung ausgerichtet sind und von ihr abhängen. Sowohl Forschung als auch der datenbasierte Binnenmarkt können – glaubt man den Rechtsakten – nur erfolgreich sein, wenn Individuen ihre Daten freiwillig und vertrauensvoll teilen oder ihre Daten anonymisiert

45 Im Beitrag von *Lang/Kneuper*, DuD 2022, 778 ist die dezentrale Architektur nur indirekt als „föderaler Dienst […] der Cloud-Dienste kommerzieller Anbieter auf Basis eines einheitlichen Frameworks zu einem komplexen Ökosystem zusammenschließt" beschrieben. In der Konzeption als Datenraum wird die dezentrale Struktur dagegen als Merkmal für Souveränität benannt, siehe *Reiberg/Niebel/Kraemer*, GAIA-X Hub Whitepaper 1/2022: Definition Datenraum, 5.

46 Vgl. *Reiberg/Niebel/Kraemer*, GAIA-X Hub Whitepaper 1/2022: Definition Datenraum, 5f; *Kraemer/Niebel/Reiberg*, GAIA-X Hub Whitepaper 1/2023: Geschäftsmodelle, 9ff.

47 So *Datenraum Kultur*, Projektsteckbrief; Kurzinformation; Factsheet.

48 *Pretzsch* et al., Mobility Data Space – Whitepaper, 2021 (3).

geteilt werden. Damit bewegen sich die Rechtsakte hin zu einer ökonomischen Datensouveränität, ohne die subjektive Datensouveränität merklich zu stärken. Stattdessen wird der Daten-Extraktivismus in Gesetzen und Vorgaben verstetigt. Vor dem aufgezeigten Hintergrund ist ein Recht auf Vergessenwerden und die Rückzugsmöglichkeit als negative Schutzrichtung von informationeller Selbstbestimmung[49] und europäischem Datenschutzgrundrecht (Art. 7, 8 GrCh) nicht mehr zu erkennen, obwohl sie Teil „europäischer Werte" sind. Forschungsdatenräume und Infrastrukturvorhaben müssen sich an den gezeigten Regelungen orientieren, haben aber auf Ebene der Ethik bzw. Forschungsethik noch Spielraum. Die traditionellen Vorgaben sind gewohnt offen formuliert, sodass die Forschung hier eigenhändig das Individuum in den Fokus rücken könnte. Die Forschung bzw. Forscher:innen selbst benötigen hierbei allerdings Unterstützung, um rechtliche Vorgaben zum Schutz der Interessen der Datengebenden auch umsetzen und wahrnehmen zu können. Hieran fehlt es aufgrund der rechtlich wie forschungspolitisch stark ökonomischen Prägung. Infrastrukturen und Forschungsdatenräume sind also bislang datenfreundlich und forschungsorientiert ausgerichtet, aber nicht menschenzentriert bzw. „menschenleer" angelegt.

These 3: Deutsche und europäische Gesetzesvorhaben fangen die Menschenleere nicht auf. Es fehlt an ethischem Bewusstsein.

Wenn die Infrastruktur Nutzer:innen und ihre digitalen Identitäten nicht ausreichend menschengerecht auffängt, liegt der Grund möglicherweise nicht nur in mäßig guten Governance-Strukturen mit geringen Einwirkungsmöglichkeiten. Es ist zu überprüfen, ob die jeweiligen subjektiven Interessen der Datensubjekte durch das Berücksichtigen (forschungs-)ethischer Grundsätze einbezogen werden. Menschenleere Infrastrukturen könnten so doch noch mit menschlichen Werten angefüllt werden.

Die Ansätze dafür sind zahlreich: National benennen diverse Hochschulgesetze die Verantwortung der Forscher:innen, im Rahmen einer Folgenabschätzung „die Anwendung wissenschaftlicher Erkenntnisse in der Praxis" zu berücksichtigen, „die sich aus der Anwendung wissenschaftlicher Erkenntnisse ergeben können."[50] In einigen Bundesländern wie in Berlin und Schleswig-Holstein wird dieses Vorgehen durch das Einbinden einer Ethik-

49 *Vettermann*, Der grundrechtliche Schutz der digitalen Identität, S. 109 mwN.
50 Exempl. § 40 LHG BW.

kommission gestützt.[51] Ethische Prinzipien-Bündel wie CARE[52], OCAP[53] oder FACT[54] sind darin aber nicht explizit erwähnt, sondern dienen höchstens als Leitlinie für die eigene wissenschaftliche Arbeit.[55] Ergänzt wird die Auseinandersetzung mit den Interessen der Beforschten durch die Einbeziehung der DFG-Praxisregeln in das Arbeitsverhältnis per schriftlicher Vereinbarung, um zukünftige Fördergelder aus DFG-Ausschreibungen zu erhalten.[56] Das verfassungsrechtliche Selbstverständnis der Forschung des Art. 5 Abs. 3 GG, der Gesellschaft per Publikation stets zur Erkenntniserweiterung zu verhelfen[57], wird so mittelbar gesetzlich abgesichert.

Politisch wird die Notwendigkeit, sich mit den Folgen der Forschung auseinanderzusetzen, recht lose eingebunden. In der aktuellen *Datenstrategie der Bundesregierung* sollen für die Nutzung pseudonymisierter Daten „angemessene Haftungsregeln und […] faire Ausgleichsregeln" gefunden werden.[58] Zu ethischen Fragen im Rahmen des kommenden Forschungsdatengesetzes äußert sich die Strategie nicht ausdrücklich. Höchstens lässt sich die Abwägung ethischer Interessen in die „verfassungsrechtlichen und unionsrechtlichen Spielräume"[59] hineinlesen. Ethische Aspekte berücksichtigt die Strategie explizit nur für Künstliche Intelligenz.[60] Die Datenstrategie aus dem Jahr 2021 gibt sich da nur minimal genauer, indem sie unter einer verantwortungsvollen Datennutzung „auch die Orientierung an zentralen ethischen Grundsätzen und Prinzipien" versteht. „Bei der Nutzung von Daten ist nicht alles, was technisch möglich ist, auch ethisch vertretbar und politisch wünschenswert. […] Datenrecht und ethische Grundsätze sind keine Bremse, sondern wichtig für den Schutz der Grundrechte und eine verantwortungsvolle Datennutzung."[61] Damit referenziert der Wortlaut das im Jahr 2019 veröffentlichte Gutachten der Datenethikkommission und die

51 *Vettermann/Petri*, RuZ 2023, 5 (19 ff; zur Übersicht aller Länderklauseln S. 21 – Stand April 2023).
52 Für ethische Aspekte indigener Gruppen, siehe https://www.gida-global.org/care.
53 Die Interessen von First Nations adressierende Interessen, siehe https://fnigc.ca/ocap-training/.
54 Für die Data Science, siehe https://redasci.org/.
55 *Vettermann/Petri*, RuZ 2023, 5 (22, 26).
56 *Vettermann/Petri*, RuZ 2023, 5 (12 mwN): faktisch bindende Wirkung.
57 Zum drittnützigen Grundrecht siehe *Vettermann/Petri*, RuZ 2023, 5 (11).
58 *Bundesregierung*, Datenstrategie, 2023 (17).
59 Ebd.
60 *Bundesregierung*, Datenstrategie, 2023 (32).
61 *Bundesregierung*, Datenstrategie, 2021 (7).

darin erläuterten rechtlich-ethisch geprägten Grundsätze.[62] In der jüngsten Datenstrategie fehlen sie allerdings gänzlich.

Die im Frühjahr 2024 veröffentlichte *Strategie für die Internationale Digitalpolitik* der Bundesregierung setzt diesen Zwiespalt aus Fokus auf Individuen und fehlender Konkretheit fort: Unter anderem widmet sich die Strategie der Förderung „menschenzentrierter und innovationsfreundlicher Regeln für den digitalen Raum". Dies soll auch durch „internationale Regeln […] zu ethischen Herausforderungen der Technologienutzung"[63] gelingen, worunter wohl der Fokus auf eine „menschenzentrierte […] Künstliche Intelligenz"[64] zu verstehen ist. Wie bereits im Zusammenhang mit These 1 erwähnt wurde, schließen sich ökonomische Datensouveränität in Form des Datenkapitalismus und eine ethische, menschenzentrierte Perspektive aus. Anders ausgedrückt: In einem innovationgetriebenen Modell findet nur das Individuum Halt, das in einem Datenmarkt über Daten als kapitalisierte Anteile verfügt und diese einbringen kann. Ein Bewusstsein, weitreichende ethische Fragen als Aushandlungs- und Gesprächsraum beispielsweise auch auf den globalen Süden auszurichten, fehlt.[65]

Eine mögliche Erklärung für dieses Ethik-Defizit wäre die Überformung durch europäische Vorgaben, sofern sie Angaben zur Datenethik enthalten und dadurch Lücken auffüllen. Ein erster Anlaufpunkt sind die Strategievorhaben der EU: Die *EU-Datenstrategie (2020)* beabsichtigt, „den Austausch und die breite Nutzung von Daten kanalisieren und gleichzeitig hohe Datenschutz-, Sicherheits-, und Ethik-Standards [zu] wahren."[66] Gemeint sind damit aber die in der Strategie stets genannten „europäischen Werte"[67], gegebenenfalls auch die Stärkung der Selbstbestimmtheit im Umgang mit Daten.[68] Eine konkrete ethische Einbettung fehlt. Die *Digitalstrategie der Europäischen Kommission (2022)* plant grundlegend einen menschenzentrierten Ansatz zur Konzeption des digitalen Europas. Abgesehen von einer „ethischen Nutzung innovativer Technik"[69] gibt es auch hier keine Anzeichen, wie sich die Ethik in der Strategie niederschlägt – weder

62 Gutachten der Datenethikkommission, 2019 (43 ff).
63 *Bundesregierung*, Internationale Digitalpolitik, 2024 (9).
64 Ebd.
65 Vgl. hierzu die Zusammenarbeit mit westlich orientierten Ländern, *Bundesregierung*, Internationale Digitalpolitik, 2024 (8).
66 EU-Datenstrategie, 2020 (4).
67 EU-Datenstrategie, 2020 (1, 5).
68 EU-Datenstrategie, 2022 (11f).
69 Europäische Kommission, Digitalstrategie, 2022 (2).

unter dem Punkt „Digitale Führung" noch in der „Kommissionsweiten Architektur" von Infrastruktur und Governance.[70] Im Gegenteil lässt die *Pressemitteilung zur Errichtung virtueller Welten*[71] erkennen, dass weniger der Mensch in der virtuellen Welt im Mittelpunkt steht als das damit verknüpfte ökonomische Potenzial der Daten. Oder wie die Kommission selbst in der Mitteilung „Virtuelle Welten, die für Menschen geeignet sind"[72] hervorhebt: „Mit einem geschätzten weltweiten Wachstum von 800 Mrd. Euro bis 2030 und potenziellen 860,000 neuen Arbeitsplätzen bis 2025 werden virtuelle Welten den Wirtschafts- und Beschäftigungssektor in der EU verändern."[73] Die in der damit verbundenen Studie herausgearbeiteten Risiken für digitale Identitäten erwähnt die Kommission nicht.[74]

Die EU-Regelungen DGA, DA und der EHDS-VO sind konkrete Umsetzungen dieser Strategien, in denen sich dann Indizien für erwähnte ethische Aspekte und europäische Grundwerte finden müssten. Der DGA enthält hierzu aber kaum Anhaltspunkte. Einzig im Hinblick auf die „Datenspende" bzw. den Datenaltruismus auf Basis einer Einwilligung werden ethische Aspekte angesprochen. Gemäß ErwGr 46 Abs. 2 DGA kann im Kontext von Aufsichtsmechanismen wie einem Ethikrat eine entsprechende Prüfung erfolgen, ob ein datenaltruistisches Modell also „hohe wissenschaftliche Ethikstandards und den Schutz der Grundrechte einhält". Ähnlich enthält der DA keine eigenständigen Hinweise zu ethischen Vorgaben. Wiederholt weist er formelhaft auf die Absicherung „fairer, angemessener und nichtdiskriminierender Bedingungen für die Bereitstellung von Daten"[75] hin. Gemeint ist damit allerdings nicht der Hinweis, Grundrechte natürlicher Personen und Diskriminierungen marginalisierter Gruppen aus ethischen Gründen abzubauen. Verortet ist die Formulierung vielmehr in der Ungleichbehandlung von Marktteilnehmer:innen im B2B-Kontext, hat damit also einen starken wettbewerbsrechtlichen bzw. ökonomischen Bezug.[76] Die EHDS-VO baut auf beiden EU-Gesetzesvorhaben auf und formuliert im Vergleich dazu konkret ethische Maßstäbe. Beispielsweise

70 Europäische Kommission, Digitalstrategie, 2022 (16).
71 EU-Kommission, Pressemitteilung vom 11.6.2023.
72 Siehe https://digital-strategy.ec.europa.eu/de/policies/virtual-worlds.
73 Ebd.
74 EU-Kommission, Extended Reality: Opportunities, success stories and challenges (Health, Education) – Final Report, S. 58f.
75 Beispielsweise Art. 8 Abs. 1, Art. 10 Abs. 1 DA.
76 Vgl. hierzu *Bornkamm/Feddersen*, in: Köhler/Bornkamm/Feddersen, UWG, § 5 Rn. 3.95-97 sowie ErwGr 42 DA.

legen Art. 45 Abs. 2 lit. ha EHDS-VO sowie ErwGr 50 EHDS-VO nahe, im Genehmigungsverfahren zur Sekundärnutzung von Gesundheitsdaten auch Informationen über die Bewertung ethischer Aspekte der Verarbeitung gemäß nationalem Recht einzuholen. Sie referenziert damit das Gesundheitsdatennutzungsgesetz (GDNG). Letztlich ergeben sich hieraus aber auch nur geringe und disziplinspezifische Leitlinien für Forscher:innen selbst, die eigentlich als Bürger:innen von den Gesetzen und Verordnungen betroffen sind.

Die in These 2 aufgezeigte Menschenleere wird folglich auch nicht dadurch gefüllt, dass in politischen Strategien oder nunmehr umgesetzten Gesetzgebungsvorhaben ethische Maßstäbe klarer eingebunden wären. Stattdessen wird sich üblicher legislativer Instrumente zur Stärkung der informationellen Selbstbestimmung und des Datenschutzes bedient: Transparenz durch Information und Berichte, Verantwortlichkeitsketten und Zuständigkeiten oder die Rechtsgrundlage der Einwilligung als bewusstes Entscheidungsinstrument. Die damit verbundenen „europäischen Werte" regeln damit am Menschen vorbei, sowohl an Bürger:innen als Verwalter:innen ihrer digitalen Identitäten als auch an verunsicherten Forscher:innen.

Damit einher geht eine zunehmende Unsicherheit der Forscher:innen im Umgang mit gesellschaftlichen Anforderungen an ihre Arbeit, die aus ethischen Vorgaben erwachsen: Zum einen benennt die Digitalstrategie der Kommission die „digitale Inklusion"[77], die in der Strategie neben der Barrierefreiheit auch die Data Literacy und Zugänglichkeit meinen kann. Inklusion kann insoweit auch bedeuten, entsprechend niedrigschwellig verschiedene Nationalitäten und marginalisierte Gruppen einzubeziehen. Für die CARE-Prinzipien ist die Verständlichkeit und Zugänglichkeit grundlegend, da indigenen Gruppen der Zugang zu westlich-europäischen Datensätzen in öffentlichen Forschungsrepositorien fremd ist. Insofern kann die Darstellung ihrer digitalen Souveränität schaden, wenn ihre Geschichte durch westlich geprägte Metadatenfelder dargestellt und ggf. verkürzt oder entstellt wird. Inklusion und Souveränität gehen also ineinander auf, wenn durch die Zugänglichkeit auch eine Handhabe über die Darstellung der eigenen (kulturellen) Informationen (vgl. Art. 5 lit. d DSGVO – Richtigkeit) geschaffen wird. Durch die bislang geringe Einordnung – strategisch, (forschungs-)politisch und gesetzlich – sind Forscher:innen regelmäßig überfordert und auf niedrigschwellige Gesprächsformate wie den Legal Helpdesk im DFG-geförderten Forschungsprojekt NFDI4Culture angewie-

77 Europäische Kommission, Digitalstrategie, 2022 (2).

sen. Das Benennen und Einbinden ethischer Grundsätze erfordert jedoch das Gegenteil, also die langfristige und nachhaltige Sensibilisierung für ihre Perspektive. Zum anderen werden sensible Themen wie das Loslösen von Sexualität und Gender als ethische und identitätsstiftende Frage kaum adressiert, obwohl dies für Metadaten und Infrastrukturen in bestimmten Bereichen relevant sein kann. Schon die Aufarbeitung von Frauenrollen in den letzten 50 bis 100 Jahren zeigt, dass in bestehenden Datensätzen – auch in öffentlich auffindbaren – ein gender bias vorliegen kann. Verweise auf „hohe Ethik-Standards" greifen da zu kurz, wo das Bewusstsein schon für bestehende ethische Regelungen fehlt. Forscher:innen und Forschungsprojekten ist bislang selten bekannt, wie angemessen und richtig bei Einwilligungen zu informieren ist oder wie Fotografien von Personen persönlichkeitsrechtlich und datenschutzrechtlich zu behandeln sind – trotz zahlreicher öffentlich verfügbarer Handreichungen, Assistenzsysteme und Entscheidungsbäume. Wenn der Mensch im Mittelpunkt der Daten- und Digitalstrategien stehen soll, braucht es auch eine Orientierung und Unterstützung der Forschung bei der Umsetzung ihrer ethischen Verantwortung. In diesem Punkt fehlt es den Umsetzungen politisch und infrastrukturell in der Breite an einem ethischen Bewusstsein.

4. Conclusio

Insgesamt gelingt es den Regelwerken der EU also nicht, die Perspektive von Individuen aktiv und gestärkt einzubinden. Der Beitrag konnte lediglich folgende strukturellen Defizite offenlegen:

Zunächst konnte gezeigt werden, dass das Politikum der Datensouveränität sich nicht als greifbarer Begriff eignet, den grundrechtlichen Datenschutz zu reflektieren. Er dient vielmehr als flexibler Terminus, der eine von Beginn durch ökonomisch-kapitalistische Werte geprägt war. Der Terminus an sich ist damit kein Ansatzpunkt, der die Betroffenenperspektive und grundrechtlichen Datenschutz in Infrastruktur-Vorhaben hineinbringt.

Diese Perspektive schlägt sich in der untersuchten EU-Regulierung nieder: Data Act, Data Governance Act und EHDS-Verordnung enthalten zwar traditionelle Instrumente des Datenschutzes wie Informationspflichten, Meldeprozesse und Zugangsansprüche. Sie sind jedoch eher symbolischer Natur, da sich sowohl die übergeordneten EU-Strategien als auch die Präambeln der Regelungen für eine Wertschöpfung an Daten in der Breite aussprechen. Infrastruktur-Vorhaben wie der EHDS animieren daher

zum Datenteilen und zur Nachnutzung durch die Forschung in jeder Form. Das Individuum bleibt dabei mangels Opt-In – da ein Opt-Out lt. EHDS-Verordnung vorgesehen ist – und einer unbeeinflussten Entscheidung mit eigenen Interessen außen vor.

Die Interessen der betroffenen Personen in Bezug auf ihre digitale Identität werden auch nicht durch ethische Vorgaben aufgefangen. Weder die Strategien noch EU-Regelungen enthalten konkrete Vorgaben für Forscher:innen sowie für Infrastrukturen an sich. An Konzepten zur (langfristigen) Unterstützung von Forscher:innen bei einer ethischen und rechtskonformen Forschung fehlt es ebenso.

Danksagung

Der Verfasser dankt Malte Engeler, Mareike Lisker und Aline Blankertz für den umfänglichen Austausch anlässlich des Redebeitrags auf dem Forum Privatheit 2023.

Literatur

Bisges, Marcel (2017): Personendaten, Wertzuordnung und Ökonomie. *Multimedia und Recht (MMR)*, S. 301-306.

Buccafusco, Christopher J.; Weinstein, Samuel N. (2023): Antisocial Innovation. Georgia Law Review, Duke Law School Public Law & Legal Theory Series No. 2023-42, Cardozo Legal Studies Research Paper No. 723, S. 573-661. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4520979 (besucht am 8.2.2024).

Buchner, Benedikt (2022): Forschungsdaten effektiver nutzen. *Datenschutz und Datensicherheit (DuD)*, 46(9), S. 555-560.

Bundesregierung (2021): Datenstrategie. Berlin: Deutscher Bundestag. URL: https://www.bundesregierung.de/resource/blob/992814/1845634/f073096a398e59573c7526feaadd43c4/datenstrategie-der-bundesregierung-download-bpa-data.pdf?download=1 (besucht am 8.2.2024).

Bundesregierung (2023): Fortschritt durch Datennutzung. Strategie für mehr und bessere Daten für neue, effektive und zukunftsweisende Datennutzung. Berlin: Bundesministerium für Digitales und Verkehr u.a. URL: https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2023/datenstrategie.pdf;jsessionid=DC18FD49F90D19C686236DA5A65B0B3C.1_cid505?__blob=publicationFile&v=3 (besucht am 8.2.2024).

Bundesregierung (2024): Strategie für die Internationale Digitalpolitik. Berlin: Bundesministerium für Digitales und Verkehr. URL: https://bmdv.bund.de/SharedDocs/DE/Artikel/K/strategie-internationale-digitalpolitik.html (besucht am 8.2.2024).

Calliess, Christian; Ruffert, Matthias (Hrsg.) (2022): *EUV/AEUV Kommentar*, 6. Auflage. München: C.H. Beck.

Datenethikkommission der Bundesregierung (Oktober 2019): Gutachten der Datenethikkommission. Berlin: Bundesministerium des Innern, für Bau und Heimat. URL: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf?__blob=publicationFile&v=6 (besucht am 8.2.2024).

Datenraum Kultur (Jan. 2023): Factsheet. URL: https://www.acatech.de/wp-content/uploads/2023/01/Factsheet_Datenraeume_de.pdf (besucht am 8.2.2024).

Datenraum Kultur (Jan. 2023): Kurzinformation. URL: https://www.acatech.de/wp-content/uploads/2023/01/Kurzinformation_Datenraum-Kultur.pdf (besucht am 8.2.2024).

Datenraum Kultur (Jan. 2023): Projektsteckbrief. URL: https://www.acatech.de/wp-content/uploads/2023/01/Projektsteckbrief_Datenraum-Kultur.pdf (besucht am 8.2.2024).

Datenschutzkonferenz des Bundes und der Länder (2023): Stellungnahme vom 27.3.2023 = DuD 2023, 325. URL: https://www.datenschutzkonferenz-online.de/media/st/2023-03-27_DSK-Stellungnahme_EHDS.pdf (besucht am 8.2.2024).

Denga, Michael (2022): Digitale Souveränität durch Datenprivatrecht? *Gewerblicher Rechtsschutz und Urheberrecht (GRUR)*, 124, S. 1113-1120.

Denga, Michael (2023): Die Nutzungsgovernance im European Health Data Space als Problem eines Immaterialgütermarkts. *Europäische Zeitschrift für Wirtschaftsrecht (EuZW)*, S. 25-33.

Digital Autonomy Hub (2021): Policy Brief #4: Digitale Selbstbestimmung. URL: https://digitalautonomy.net/fileadmin/PR/Digitalautonomy/PDF/DAH_Policy_Brief__4_Digitale_Selbstbestimmung.pdf.

Engeler, Malte (2022): Der Konflikt zwischen Datenmarkt und Datenschutz. *Neue Juristische Wochenschrift (NJW)*, 47/2022, S. 3398-3405.

Europäische Kommission (12. Feb. 2020): Datenstrategie. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066 (besucht am 8.2.2024).

Europäische Kommission (30. Juni 2022): Digitalstrategie. URL: https://commission.europa.eu/publications/european-commission-digital-strategy_de (besucht am 8.2.2024).

Europäische Kommission (2023): Extended Reality: Opportunities, success stories and challenges (Health, Education). Final Report. URL: https://op.europa.eu/en/publication-detail/-/publication/f242f605-a82e-11ed-b508-01aa75ed71a1 (besucht am 8.2.2024).

Europäische Kommission (11. Juni 2023): Web 4.0 und virtuelle Welten: Kommission stellt EU-Strategie vor. Pressemitteilung. URL: https://germany.representation.ec.europa.eu/news/web-40-und-virtuelle-welten-kommission-stellt-eu-strategie-vor-2023-07-11_de (besucht am 8.2.2024).

Funk, Axel (2023): Das Prinzip der Nutzerzentriertheit des Data Act – ein gravierender Strukturfehler. *Computer und Recht (CR)*, 7/2023, S. 421-427.

Heesen, Jessica; Ammicht Quinn, Regina; Baur, Andreas; Hagendorff, Thilo; Stapf, Ingrid (2022): Privatheit, Ethik und demokratische Selbstregulierung in einer digitalen Gesellschaft. In: Roßnagel/Friedewald (Hrsg.), *Die Zukunft von Privatheit und Selbstbestimmung*, Wiesbaden: Springer Vieweg, S. 161-188.

Kelber, Ulrich; Bortnikov, Vyacheslav (2023): Digitale Souveränität von Sicherheitsbehörden und Nachrichtendiensten. *Neue Juristische Wochenschrift (NJW)*, 28/2023, S. 2000-2006.

Kraemer, Peter; Niebel, Crispin; Reiberg, Abel (2023): GAIA-X Hub Whitepaper 1/2023: Geschäftsmodelle. URL: https://gaia-x-hub.de/wp-content/uploads/2023/02/Whitepaper-Gaia-X-Geschaeftsmodelle.pdf (besucht am 8.2.2024).

Krüger, Philipp-L. (2016): Datensouveränität und Digitalisierung. *Zeitschrift für Rechtspolitik (ZRP)*, 7/2016, S. 190-192.

Lang, Simon; Kneuper, Ralf (2022): Datenschutz und Informationssicherheit in Gaia-X. *Datenschutz und Datensicherheit (DuD)*, 46(12) S. 778-781.

Lisker, Mareike (2023): Von der (Un-)Möglichkeit, digital mündig zu sein. Masterarbeit, TU Berlin. URL: https://depositonce.tu-berlin.de/items/ab50df77-b748-4ea3-8dbc-b5afc1ef9574 (besucht am 8.2.2024).

Medizininformatik-Initiative AG Consent (2019): Stellungnahme zu patientenindividueller Datennutzungstransparenz und Dynamic Consent. URL: https://www.medizininformatik-initiative.de/sites/default/files/2019-09/MII_AG-Consent_Stellungnahme-Consent-Modelle_v05.pdf.

Müller, Johannes (2021): Der „digitale Zwilling". *ZD-Aktuell*, Nr. 05096.

Pretzsch, Sebastian; Drees, Holger; Rittershaus, Lutz; Schlueter Langdon, Christoph; Lange, Christoph, Weiers, Christian (2021): Mobility Data Space – Whitepaper. URL: https://www.mobility-data-space.de/content/dam/ivi/mobility-data-space/documents/Mobility_Data_Space_DE_20220603_web.pdf besucht am 8.2.2024).

Pohle, Julia; Thüer, Leo; Dammann, Finn; Winkler, Jan (2020): Das Subjekt im politischen Diskurs zu „digitaler Souveränität". In: Kersting, Norbert; Radtke, Jörg; Baringhorst, Sigrid (Hrsg.): *Handbuch Digitalisierung und politische Beteiligung*. Wiesbaden: Springer VS, S. 1-23.

Reiberg, Abel; Niebel, Crispin; Kraemer, Peter (2022): GAIA-X Hub Whitepaper 1/2022: Definition Datenraum. URL: https://gaia-x-hub.de/wp-content/uploads/2022/10/20220914_White_Paper_22.1_Definition_Datenraum_final.pdf (besucht am 8.2.2024).

Roos, Philipp; Maddaloni, John-Markus (2023): Regulierter Datenaustausch zur Gesundheitsforschung. *Recht Digital (RDi)*, S. 225-232.

Rosenkranz, Frank; Scheufen, Marc (2022): Die Lizenzierung von nicht-personenbezogenen Daten: Eine rechtliche und rechtsökonomische Analyse. *Zeitschrift für Digitalisierung und Recht (ZfDR)*, 2(2), S. 159-198.

Roßnagel, Alexander (2023): Digitale Souveränität im Datenschutzrecht. *Multimedia und Recht (MMR)*, 26(1), S. 64-68.

Samardzic, Darko; Becker, Thomas (2020): Die Grenzen des Datenschutzes – Der beschränkte Schutz durch Freiwilligkeit und Einwilligung bei Corona-Apps. *Europäische Zeitschrift für Wirtschaftsrecht (EuZW)*, 15/2020, S. 646-654.

Schütrumpf, Moritz; Person, Christian (2022): Gaia-X: Vernetzte Infrastrukturen für eine europäisch geprägte Datenwirtschaft. *Recht Digital (RDi)*, S. 281-288.

Spitz, Markus; Cornelius, Kai (2022) Einwilligung und gesetzliche Forschungsklausel als Rechtsgrundlagen für die Sekundärnutzung klinischer Daten zu Forschungszwecken. *Medizinrecht (MedR)*, 40(3), S. 191–198. URL: https://doi.org/10.1007/s00350-022-6136-7.

Umweltbundesamt (2023): Digitale Kommune/Digitale Region, Texte 62/2023. URL: https://www.umweltbundesamt.de/publikationen/digitale-kommunedigitale-region (besucht am 8.2.2024).

Vettermann, Oliver (2022): Der grundrechtliche Schutz der digitalen Identität. Dissertation, Universität Leipzig. URL: 10.5445/KSP/1000148103 (besucht am 8.2.2024).

Vettermann, Oliver; Petri, Grischka (2023): Should I CARE about FAIR? – Ein rechtlicher Blick auf die Prinzipien des Forschungsdatenmanagements, *Recht und Zugang (RuZ)*, 4(1), S. 5–29. DOI: 10.5771/2699-1284-2023-1-5 (besucht am 8.2.2024).