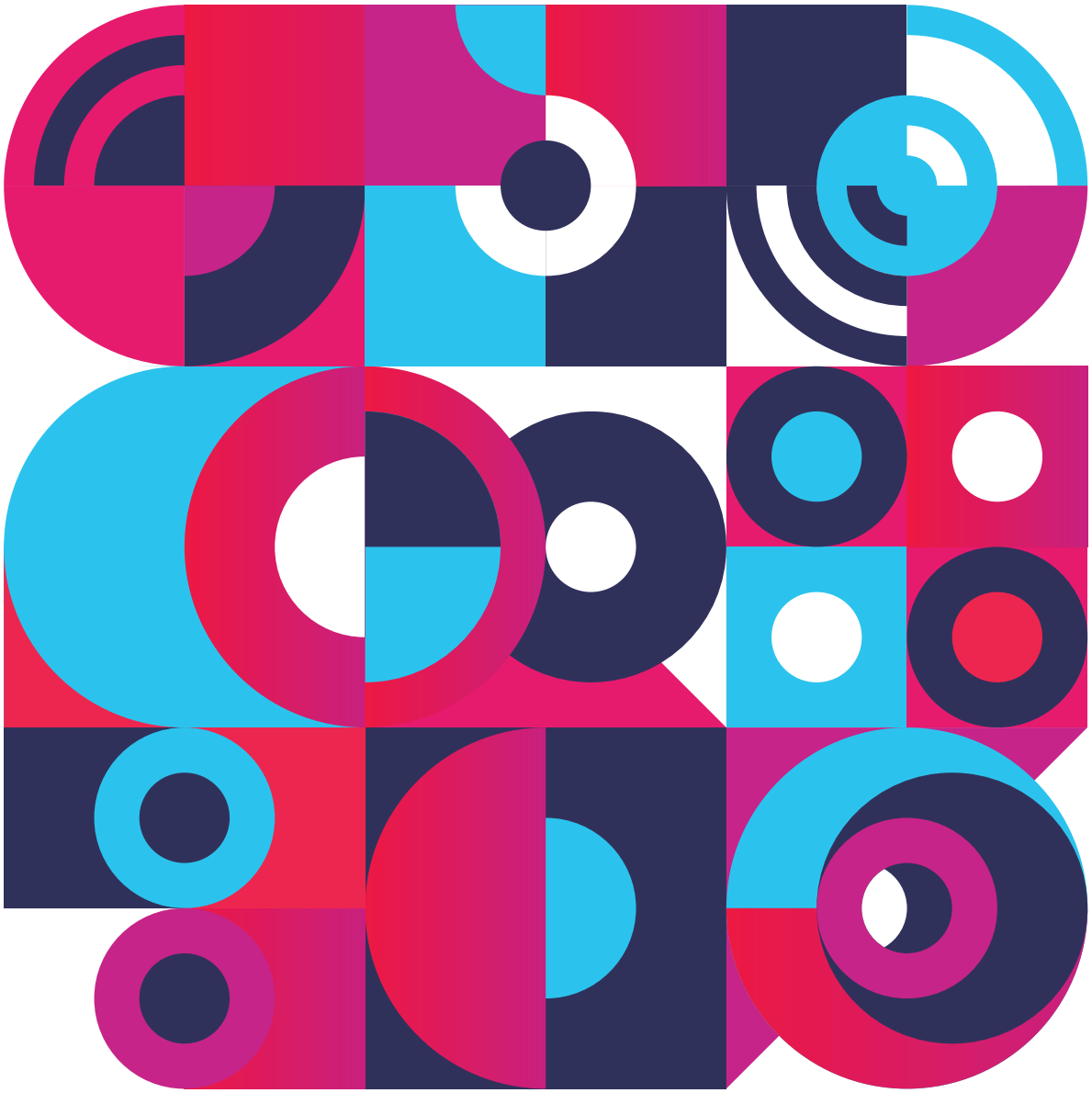
universität wien

DIGITAL TRANSFORMATIONS FOR HEALTH LAB

GOVERNING HEALTH FUTURES 2030



Data Solidarity Glossary 2024

German translation

universität wien

DIGITAL TRANSFORMATIONS FOR HEALTH LAB
GOVERNING HEALTH FUTURES 2030

Glossar zur Datensolidarität 2024

Deutsche Übersetzung

Barbara Prainsack
Institut für Politikwissenschaft, Universität Wien, Österreich.

Ilona Kickbusch
Direktor, Digital Transformations for Health Lab, Universität Genf, Schweiz.

German translation: **Birgit Bauer**, european digital health academy gGmbH / Data Saves Lives Deutschland

This report has been made possible by financial contributions from Fondation Botnar, Switzerland, to Project IMG-22-005 at Digital Transformations for Health Lab (DTH-Lab). Fondation Botnar's commitment to advancing global health is deeply appreciated, and this project would not have been possible without their contribution. DTH-Lab is hosted by Université de Genève (UNIGE), Switzerland.

This publication is the German translation of the Data Solidarity Glossary by Barbara Prainsack & Ilona Kickbusch, published on 19 September 2024 by Digital Transformations for Health Lab (DTH-Lab) and University of Vienna and available in open access at https://dthlab.org/wp-content/uploads/2024/09/DTH-Data-Solidarity-Glossary-2024.pdf. The English version is the original. DTH-Lab takes no responsibility for any errors, omissions or ambiguities in the German translation.

Suggested citation: Prainsack, B,. & Kickbusch, I. (2024). Glossar zur Datensolidarität. Übersetzt von B. Bauer. Geneva: Digital Transformations for Health Lab.

Design by Inís Communication

Layout by Janhavi Nikharge

Inhalt

Inhalt

Danksagung

Wir danken allen Mitgliedern des Forschungsprogramms Datensolidarität sowie Seliem El-Sayed, Torsten Möller, Péter Ferenc Gyarmati, Bernhard Jordan und Laura Koesten für die gemeinsame Arbeit an der Entwicklung des *PLUTO-Tools*. Wir danken Seliem El-Sayed, Nikolaus Forgó, Łukasz Szoszkiewicz, Philipp Baumer, Theresa Henne, Katja Mayer und Gertrude Saxinger für ihre Beiträge zum Weißbuch zur Datensolidarität, von denen Teile in dieses Glossar eingeflossen sind. Der Eintrag über *Public Value* basiert auf Forschungsarbeiten von Connor Hogan. Wir danken Caitlin Harjes, Louise Holly und Ananya Choyal für ihre Hilfe bei der Formatierung und Bearbeitung des Manuskripts. Wir danken Antonia Modelhart, Anurag Agrawal, Connor Hogan, Deborah Drgac, Deborah Mascalzoni, Elias Weiss, Gertrude Saxinger, Katharina Kieslich, Kazuto Kato, Njide Ndili und Rohinton P. Medhora für hilfreiche Kommentare zur englischen Version dieses Glossars. Besonderer Dank gilt Eric Sutherland für seine – wie immer scharfsinnigen und durchdachten – Kommentare, Bearbeitungen und Änderungen.

Ganz besonderer Dank geht an Birgit Bauer für die Übersetzung des Glossars vom Englischen ins Deutsche, sowie Marlene Auer für die sorgfältige Redaktion.

Über das Glossar

Dieses Glossar wurde im Rahmen des Data Solidarity Work Programme entwickelt, einer multidisziplinären Zusammenarbeit von Forscherinnen und Forschern und politischen Entscheidungsträgerinnen und Entscheidungsträgern unter der Leitung von Professorin Barbara Prainsack an der Universität Wien. Seit 2024 ist das Arbeitsprogramm Datensolidarität auch mit dem Digital Transformations for Health Lab (DTH-Lab) unter der Leitung von Professorin Ilona Kickbusch verbunden. Diese Kooperation unterstreicht die hohe Relevanz der Datensolidarität für die Gesundheit im Kontext der digitalen Transformationen.

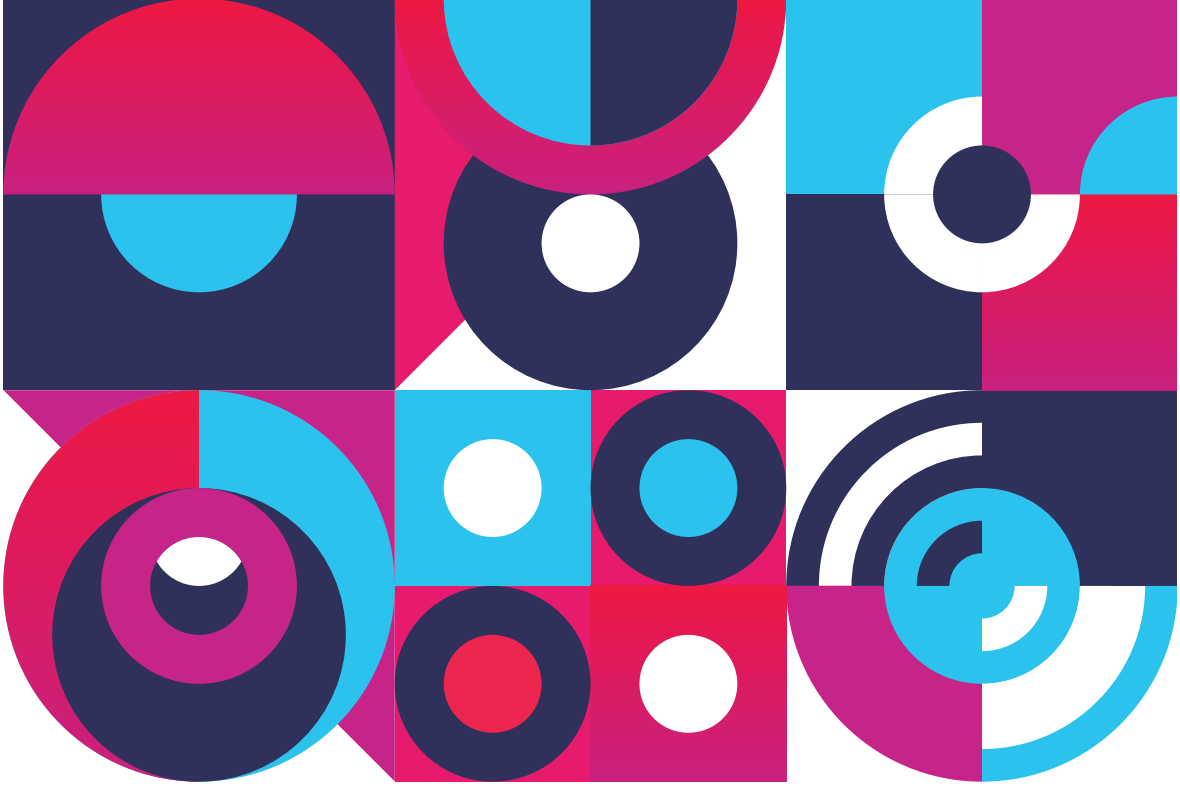
Dieses Glossar soll die Schlüsselbegriffe der Datensolidarität klären und die Beziehung der Datensolidarität zu anderen Schlüsselbegriffen und Instrumenten im Bereich der Datenverwaltung und Datenethik erläutern. Es ergänzt frühere Veröffentlichungen zu diesem Thema und insbesondere das Weißbuch zur Datensolidarität (*White Paper Data Solidarity, 2022*).

Der erste Abschnitt des Glossars beginnt mit einer Klärung von Schlüsselbegriffen, die für den Ansatz der Datensolidarität von zentraler Bedeutung sind. Im zweiten Abschnitt werden dann die wichtigsten Ansätze zur Regulierung von Daten (*Data Governance*) erörtert.

In Abschnitt drei werden Konzepte vorgestellt, die mit der Datensolidarität in enger Verbindung stehen, wobei jeweils Ähnlichkeiten und Unterschiede zur Datensolidarität herausgearbeitet werden. Abschnitt vier greift ethische Herausforderungen auf und verweist auf wichtige Ansätze, die die neuen Dimensionen von Macht und Ungleichheit analysieren, die mit der digitalen Transformation entstanden sind. Abschnitt fünf setzt sich mit wichtigen Fragen auseinander, die dabei helfen, den Ansatz der Datensolidarität weiterzuentwickeln, und endet mit einem eindringlichen Plädoyer für ein neues Konzept der digitalen Gesundheitsbürgerschaft (*Digital Health Citizenship*).

Dieses Glossar ist ein Ausgangspunkt, dem weitere Materialien folgen werden, die sich auf die Anwendung der Datensolidarität im Gesundheitswesen konzentrieren.

Wir hoffen, dass dieses Glossar dazu beiträgt, die Bedeutung eines Konzepts der Datensolidarität im Gesundheitswesen zu verdeutlichen – und viele engagierte Diskussionen über seine praktische Anwendung anzustoßen.



Abschnitt 1: Solidarität

1.1 Solidarität

Solidarität ist ein entscheidendes Element für den Aufbau gerechterer Gesellschaften, in denen alle Menschen die gleichen Möglichkeiten haben, Gesundheit, Wohlbefinden und andere Güter zu erreichen.

Solidarität hat viele Bedeutungen. Um Solidarität besser zu verstehen, nimmt dieses Glossar die Definition von Barbara Prainsack und Alena Buyx als Ausgangspunkt. Diese Autorinnen definieren Solidarität *als eine Praxis, die die Bereitschaft von Menschen widerspiegelt, andere zu unterstützen, mit denen sie Ähnlichkeiten in einem relevanten Bereich erkennen*. Die Gemeinsamkeiten zwischen den Mitgliedern dieser „Interessengemeinschaften“ sind nicht unbedingt objektiv messbare Merkmale. Sie können ein gemeinsames Ziel sein, ein gemeinsamer Kampf gegen Unterdrückung oder ein Teil der sozialen oder politischen Identität. Im Prinzip ist keine dieser Eigenschaften oder Gemeinsamkeiten wichtiger als andere: Was Menschen mit anderen verbindet, hängt von der jeweiligen Situation oder Praxis ab – und davon, was Personen jeweils als relevante Ähnlichkeiten mit anderen sehen.

Solidarität wird oft als sozialer Wert beschrieben, wobei sich ändernde Normen zur Entstehung neuer Formen von Solidarität führen. Zum Beispiel die Solidarität zwischen den Generationen in Bezug auf den Klimaschutz oder Solidarität

Tabelle 1: Die verschiedenen Ebenen der Solidarität

Ebene 1	**Zwischenmenschliche Solidarität**	Praktiken der Solidarität zwischen Individuen
Ebene 2	**Gruppenbezogene Solidarität**	Praktiken der Solidarität innerhalb von Gruppen – z. B. Patientenorganisationen
Ebene 3	**Institutionalisierte Solidarität**	Rechtliche, administrative und bürokratische Normen, die Mechanismen der Solidarität definieren und umsetzen Formelle Institutionen – z. B. solidarische Gesundheitssysteme

mit Menschen desselben Geschlechts. Aber Solidarität in einem Bereich ist nicht notwendigerweise auf andere Bereiche übertragbar: Während eine Person desselben Geschlechts vielleicht eine andere unterstützt, wenn diese zur Zielscheibe geschlechtsspezifischer Belästigung wird, wird dieselbe Person in einem Kontext, in dem ihre politischen Werte oder Handlungen sie voneinander trennen, nicht solidarisch mit der anderen handeln. Mit anderen Worten: Solidarität findet statt, wenn Gemeinsamkeiten zwischen Menschen handlungsleitend werden, und nicht die Unterschieden, die es zwischen ihnen gibt.

Solidarität ist zwar kein Ersatz für Gerechtigkeit, aber sie kann dazu beitragen, Ungerechtigkeiten entgegenzuwirken und Menschen hinter gemeinsamen Zielen zu vereinen. In diesem Sinne kann Solidarität ein Mechanismus zur Förderung des Gemeinwohls nicht nur innerhalb, sondern auch zwischen Gesellschaften sein.

Prainsack und Buyx unterscheiden außerdem drei Ebenen der Solidarität (siehe **Tabelle 1**):

Ebene 1 ist die Ebene der zwischenmenschlichen Solidarität: Sie findet tatt, wenn einzelne Menschen Solidarität mit anderen ausüben, mit denen sie sich in irgendeiner relevanten Weise verbunden fühlen.

Ebene 2 ist die Ebene der Gruppensolidarität: Sie findet statt, wenn solidarisches Verhalten zum „normalen" Verhalten in einer Gruppe wird.

Ebene 3 ist die Ebene der institutionalisierten Solidarität: Sie findet statt, wenn gesetzliche, bürokratische, administrative oder soziale Normen Solidarität umsetzen. Sie umfasst auch formale solidarische Institutionen. Solidaritätseinrichtungen sind solche, zu denen die Menschen entsprechend ihren Fähigkeiten beitragen und von denen sie Unterstützung auf der Grundlage ihrer Bedürfnisse erhalten.

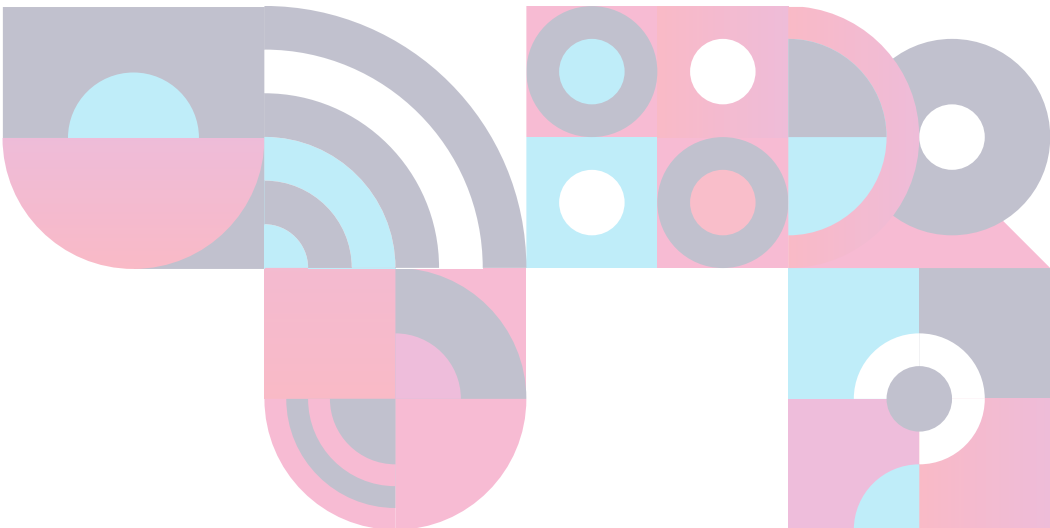
Der paradigmatische Fall einer solidarischen Einrichtung sind solidarische Gesundheitssysteme. Das sind Gesundheitssysteme wie die in Deutschland oder Österreich, die allen Menschen mit gesetzlicher Krankenversicherung Zugang zu hochwertiger Gesundheitsversorgung

bieten, wenn sie diese brauchen, unabhängig davon, wieviel sie eingezahlt haben. Für jene Menschen, die kein Geld haben, um sich selbst zu versichern, tritt der Staat ein.

In Bezug auf Gesundheit gibt es weitere Formen der Solidarität: Verhaltenssolidarität (Organspende, Verzicht auf nicht dringende Eingriffe, wenn andere sie dringender benötigen), Solidarität beim Austausch von Daten, oder Solidarität im verantwortungsvollen Umgang mit der eigenen Gesundheit.

In diesem Sinne kann die Solidarität die Politikgestaltung und den Aufbau von Institutionen in verschiedenen Politik- und Praxisfeldern anleiten. Sie wurde unter anderem auch zur Entwicklung eines neuen Konzepts für die Daten-*Governance* genutzt (siehe **Datensolidarität**). Solidarität wird auch als ein Schlüsselprinzip der internationalen Gesundheitszusammenarbeit angesehen, wie es in der politischen Entschließung des hochrangigen Treffens zu *Universal Health Coverage (UHC)* bei den Vereinten Nationen im Jahr 2023 zum Ausdruck kommt.

Referenzen: Dawson & Verweij, 2012; Prainsack, 2022; Prainsack & Buyx, 2011; Samochowiec & Müller, 2021; Sangiovanni & Viehoff, 2023; UHC 2030, ohne Datum; van Till et al., 2023.



1.2 Datensolidarität

Datensolidarität ist ein Ansatz, der darauf abzielt, eine gerechtere Aufteilung der Vorteile und Risiken zu erreichen, die sich aus digitalen Praktiken ergeben. Darüber hinaus, müssen nicht nur einzelne Menschen, sondern auch Gruppen und Gesellschaften in der Lage sein, sinnvoll Kontrolle darüber ausüben zu können, wie Daten verwendet werden, von wem und zu wessen Nutzen.

Der derzeitige Rahmen für die Verwaltung von Gesundheitsdaten ist auf den Schutz der primären Datensubjekte – d. h. der Personen, von denen die Daten stammen – und besonders sensibler Informationen, wie ihrer medizinischen Daten, ausgelegt. In digitalen Gesellschaften können die Risiken und Vorteile der Datennutzung jedoch einen viel größeren Personenkreis betreffen und viel mehr Datenpunkte aus dem täglichen Leben und Verhalten umfassen. Dies gilt sowohl für die Primärnutzung der Daten – also der Nutzung zu dem Zweck, zu dem sie erhoben wurden – und zur sekundären Nutzung, wie etwa für die Forschung oder Qualitätssicherung.

Zudem können auch Daten einer Gruppe zum Vorteil oder zur Diskriminierung einer anderen Gruppe verwendet werden. Aus diesem Grund reicht es nicht aus, die Personen zu schützen, von denen die Daten stammen. Man muss auch jene schützen, auf die die Daten anderer Menschen angewandt werden. Darüber hinaus sind die digitalen Praktiken auch in teils starke Machtasymmetrien eingebettet, sowohl innerhalb eines Landes als auch länderübergreifend. Die Bewältigung dieser Herausforderungen und Ungleichheiten erfordert einen Ansatz, der über die bloße Möglichkeit hinausgeht, den Menschen mehr Kontrolle über ihre eigenen Daten

Tabelle 2: Die drei Säulen der Datensolidarität

Säule I	Säule II	Säule III
Erleichterung der Datennutzung, die einen erheblichen öffentlichen Wert schafft	Schadensverhütung und Schadenslinderung	Teilen kommerzieller Profite mit den Menschen und Gesellschaften (z. B. Gemeinden, Krankenhäusern, Ländern) von denen die Daten stammen
z. B. durch geringere rechtliche Vorgaben, oder öffentliche Förderung für die Datennutzung	z. B. durch das Verbot von Datenverwendungen, die bekanntermaßen Menschen schaden, und durch die Einführung effektiver Instrumente zur Schadenslinderung (siehe **Schadenslinderung**)	z. B. durch Steuern oder *Benefit Sharing Agreements*

zu geben. Das entspricht den Ansätzen im Bereich der öffentlichen Gesundheit, welche die individuellen Gesundheitsrechte durch Maßnahmen der öffentlichen Gesundheit ergänzen.

Die Datensolidarität umfasst drei Säulen (siehe **Tabelle 2**):

Säule I konzentriert sich auf die Erleichterung der Datennutzung durch verschiedene Akteure wie gemeinnützige Forschungsinstitutionen, aber auch die Industrie, sofern die Datennutzung einen großen Nutzen für Menschen verspricht ohne Menschen erheblichen Risiken auszusetzen (wie z.B. Diskriminierung oder Stigmatisierung). Dies kann über die Reduktion regulatorischer Hürden für Datennutzung mit hohem gesellschaftlichen Wert erfolgen, oder über finanzielle Unterstützung.

Säule II zielt darauf ab, Schaden zu verhindern und zu lindern. Ein Beispiel ist ein wirksames Verbot von Datenverwendungen, die ein hohes Risiko bergen. Da nicht alle Schäden wirksam verhindert werden können, müssen diese gelindert werden (siehe **Schadenslinderung**). Es ist wichtig, dass alle Personen, die durch die Datennutzung einen Schaden erlitten haben, Zugang zu der Unterstützung haben, die sie brauchen. Derzeit ist dies oft nicht der Fall, wenn beispielsweise Menschen keinen Zugang zu Rechtsmitteln haben, weil kein Gesetz gebrochen wurde oder weil sie nicht feststellen können, wer für den Schaden verantwortlich ist. Letzteres ist immer schwieriger zu erkennen, wenn Daten mehrfach in verschiedenen Umgebungen geteilt werden.

Säule III versucht zu erreichen, dass kommerzielle Gewinne aus der Datennutzung mit den Menschen und Gemeinschaften geteilt werden, die die Datennutzung überhaupt erst ermöglicht haben – z. B. kommerzielle Unternehmen, die durch ihr Handeln die Daten von Patientinnen und Patienten, Bürgerinnen und Bürgern oder über öffentliche Infrastrukturen nutzen. Kommerzielle Gewinne können über Steuern oder verschiedene andere Formen eines gerechten Vorteilsausgleichs (z. B. *Benefit Sharing Agreements* mit lokalen Gemeinschaften) geteilt werden. (So können etwa große Unternehmen, die anonymisierte Patientendaten von einem Krankenhaus bekommen, um damit eine neue medizinische Software oder Medikamente zu entwickeln, einen Teil der Gewinne an das Krankenhaus zurückzahlen.)

Datensolidarität erfordert Veränderungen in der Art, wie wir über Daten denken und sie verwalten, in mindestens zweierlei Hinsicht.

Erstens wird in den bestehenden *Data-Governance*-Rahmenwerken (*Data Governance* = Verfahren, die sicherstellen, dass Daten korrekt verwaltet und genutzt werden) häufig davon ausgegangen, dass die Re-Identifizierung von Personen das Hauptrisiko bei der Datennutzung darstelle und dass einige Datentypen möglicherweise „riskanter“ sein könnten als andere. Die Datensolidarität hingegen geht davon aus, dass die Risiken auch in der *Datennutzung* liegen und nicht nur darin, welche *Arten* von Daten verwendet werden.

Ein Beispiel: Wenn unterschiedliche Datentypen miteinander verknüpft werden, kann jeder Datensatz zu Erkenntnissen führen, die Menschen theoretisch schaden können, wenn sie mit anderen Datensätzen verknüpft werden. Datensolidarität gebietet, dass Arten der Datennutzung, die nur wenige Risiken für Einzelpersonen und Gemeinschaften mit sich bringen und wahrscheinlich erhebliche Vorteile bringen, anders behandelt werden sollten als Datennutzungen, die sehr riskant

sind, und sehr wahrscheinlich nur große Unternehmen reicher machen (siehe auch **Öffentlicher Wert *[Public Value]*** und **Kasten: PLUTO-Tool**).

Zweitens: Zusätzlich zu den Rechten und Pflichten jeder einzelnen Person in Bezug auf ihre persönliche Gesundheit macht die Datensolidarität von kollektiven Kontroll- und Überwachungsinstrumenten Gebrauch. Dies passiert unter anderem durch die Nutzung von Daten-*Commons* (siehe **Digitale und Datengemeinschaften [Daten-*Commons*]**), die stärkere Anwendung verbindlicher Rechtsvorschriften zur Unterstützung der Datennutzung mit hohem öffentlichem Wert und das Verbot schädlicher Datennutzung und vieles mehr.

In ihrem Bericht, der durch ein Weißbuch über Datensolidarität ergänzt wird, hat die *Lancet* und *Financial Times* Kommission zum Thema *„Governing health futures 2030: Growing up in a digital world“* dargelegt, warum Solidarität eines der Grundprinzipien sein muss, auf denen jeder Ansatz zur Verwaltung von Gesundheitsdaten beruht. Ein solidarischer Ansatz für Gesundheitsdaten muss als entscheidendes Merkmal des öffentlichen Gesundheitswesens des 21. Jahrhunderts auf nationaler und globaler Ebene betrachtet werden, das mit der Gleichheit als einem Schlüsselwert des öffentlichen Gesundheitswesens in Einklang steht.

Referenzen: Braun & Hummel, 2022; El-Sayed et al., 2023; Kickbusch et al., 2021; McMahon et al., 2020; Prainsack et al., 2022a; b.

1.3 Digitale Solidarität

Digitale Solidarität bezieht sich auf die Nutzung oder Fähigkeit digitaler Technologien und Online-Plattformen zur Erleichterung der Zusammenarbeit, insbesondere in Krisenzeiten.

Digitale Solidarität wird häufig zur Beschreibung einer Strategie verwendet, die die Zusammenarbeit zwischen Staaten bei der Verfolgung gemeinsamer Ziele im Zusammenhang mit der Nutzung digitaler Technologien verbessert. Dies ist insbesondere in Krisenzeiten der Fall. In jüngster Zeit wurde die digitale Solidarität, die zum Teil auf den Erfahrungen während der COVID-19-Pandemie beruht, als Alternative zum Konzept der digitalen Souveränität vorgeschlagen (siehe **Digitale Souveränität**). Außerdem wächst bei vielen Menschen die politische Besorgnis in Bezug auf Bemühungen, die zur Aushöhlung eines gemeinsamen digitalen Ökosystems beitragen und somit zu einem Internetmodell führen könnten, das weniger offen, weniger sicher und weniger wirtschaftlich vorteilhaft für alle ist.

Anstatt sich auf geschlossene technologische Ökosysteme zu verlagern, wird vorgeschlagen, dass politische Entscheidungsträgerinnen und Entscheidungsträger zu einer grenzüberschreitenden digitalen Solidarität als Rahmen für die Förderung des wirtschaftlichen Fortschritts, der nationalen Sicherheit und anderer gesellschaftlicher Interessen in offenen, demokratischen und regelbestimmten Gesellschaften übergehen. So forderte die Europäische Union beispielsweise die „Digitale Solidarität der EU: ein gesamteuropäischer Ansatz gegen die Pandemie“. In ähnlicher Weise zielt der vorgeschlagene *Global Digital Compact* der Vereinten Nationen darauf ab, gemeinsame Prinzipien für eine offene, freie und sichere digitale Zukunft für alle zu umreißen, um die digitale Zusammenarbeit als Schlüsselmerkmal der multilateralen Kooperation zu verbessern. Es wird zunehmend gefordert, die grenzüberschreitende Datennutzung weltweit zu regeln.

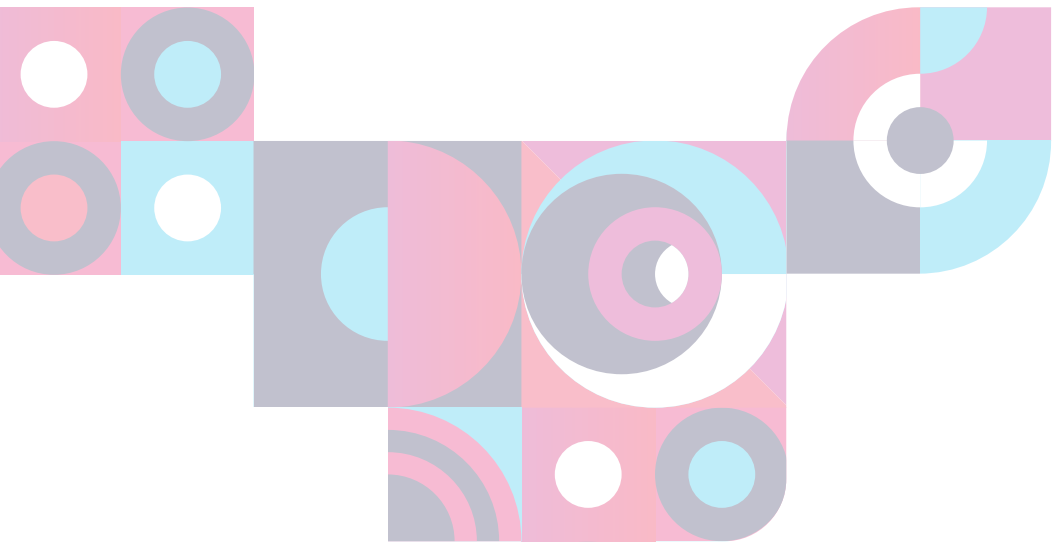
Als Ausdruck digitaler Solidarität wurden zum Beispiel auch Aktivitäten wie *Online-Fundraising*-Kampagnen, die Nutzung der *Social-Media*-Plattformen für Austausch, Diskussion und Zusammenarbeit oder der Einsatz von Technologie für die Lösung sozialer Probleme und zum Eintreten für Gerechtigkeit und Integration bezeichnet.

Diese Verwendung des Konzepts verdeutlicht die Fähigkeit von Technologie, ein Gemeinschaftsgefühl aufzubauen und Herausforderungen im digitalen Zeitalter gemeinsam anzugehen. Es geht um die Nutzung digitaler Werkzeuge und Ressourcen zur Überwindung wirtschaftlicher, sozialer und politischer Asymmetrien und um die Unterstützung derjenigen, die nur begrenzten Zugang zu Technologie haben oder mit verschiedenen Formen der digitalen Ausgrenzung konfrontiert sind.

Das Konzept der digitalen Solidarität wird manchmal auch verwendet, um an die Bereitschaft zu appellieren, Daten zu teilen oder Zugang zu den eigenen Daten zu gewähren – erleichtert durch digitale Technologien – um bestimmte wünschenswerte Ziele zu erreichen, wie z. B. die Unterstützung der Erforschung von Erkrankungen und die Verbesserung der

Pandemievorsorge. Die digitale Solidarität kann als eine Komponente der digitalen Bürgerschaft betrachtet werden, die sich von der individuellen Handlungsfähigkeit auf die kollektive Macht lose organisierter digitaler Netzwerke verlagert, die sich oft über physische Grenzen hinweg manifestieren.

Referenzen: Afina et al., 2024; Chavez, 2022; Peng et al., 2018; Roberts & Bosch, 2023; Stalder, 2013; United Nations, ohne Datum; U.S. Department of State, 2024; Walker, ohne Datum.



1.4 Digitale Gerechtigkeit *(Digital Justice)*

Die digitale Gerechtigkeit teilt viele Anliegen mit der Datengerechtigkeit, umfasst aber ein breiteres Spektrum. Sie umfasst nicht nur Daten, sondern auch den Zugang zu und die Nutzung von digitalen Technologien. Sie bezieht sich auf das Streben nach Gleichheit und Fairness im digitalen Zeitalter, wobei systembedingte Ungleichheiten im Zusammenhang mit dem Zugang zu digitalen Technologien, ungleichem Zugang zu digitalen Werkzeugen und digitalen Kompetenzen und den mit dem digitalen Umfeld verbundenen Rechten und Freiheiten behandelt werden. Digitale Gerechtigkeit soll sicherstellen, dass alle Menschen unabhängig von ihrem sozioökonomischen Status, ihrer ethnischen Zugehörigkeit, ihrem Geschlecht oder ihrem Wohnort die Möglichkeit haben, an der digitalen Gesellschaft teilzunehmen.

Ähnlich wie bei der Klimagerechtigkeit, bei der Gleichheit, Menschenrechte, kollektive Rechte und historische Verantwortung für den Klimawandel untersucht werden, geht es bei der digitalen Gerechtigkeit sowohl um verfahrens- als auch um verteilungsrelevante Aspekte. Sie unterstreicht, wie wichtig es ist, individuelle und kollektive Rechte und Interessen zu berücksichtigen und sicherzustellen, dass technologische Fortschritte bestehende Ungleichheiten nicht verschärfen oder neue Formen der Ungerechtigkeit schaffen.

Ein wesentlicher Aspekt der digitalen Gerechtigkeit ist die Wiedergutmachung von datenbedingtem Schaden, der Einzelpersonen oder Gruppen zugefügt wurde. Ungerechtigkeiten entstehen, wenn das Ausmaß des Schadens unterschätzt wird oder unbemerkt bleibt, wenn es keine Rechenschaftspflicht gibt oder wenn es keine wirksamen Wege zur Wiedergutmachung des Schadens gibt. Die digitale Gerechtigkeit versucht, diese Probleme anzugehen, indem sie sich auf die Prävention, die rückwirkende Identifizierung von Schäden, die Zuweisung von Verantwortung und die Ermittlung von gerechten Wegen zur Wiedergutmachung konzentriert. In dieser Hinsicht teilt sie wichtige Ziele mit der Datensolidarität (siehe **Schadenslinderung**).

Zum Konzept der digitalen Gerechtigkeit gehört es auch, dafür zu sorgen, dass alle Stimmen gehört werden und dass Randgruppen bei der digitalen Transformation nicht zurückbleiben. Dazu gehört auch das Eintreten für eine Politik, die die digitale Kompetenz und Zugänglichkeit fördert und so möglichst viele Menschen in die Lage versetzt, sich in den digitalen Technologien zurechtzufinden und von ihnen zu profitieren.

Zusammenfassend lässt sich sagen, dass es bei der digitalen Gerechtigkeit darum geht, faire und gerechte digitale Gesellschaften zu schaffen. Sie umfasst die proaktive Vorbeugung von digitalem Schaden, die Ermittlung und Beseitigung von Ungerechtigkeiten in der Vergangenheit und die Förderung integrativer digitaler Praktiken, die individuelle und kollektive Rechte respektieren und wahren.

Referenzen: Adecco Group, 2023; Benjamin, 2019; Brock, 2020; Couldry & Mejias, 2019; Eubanks, 2018; Noble, 2018.

1.5 Datengerechtigkeit *(Data Justice)*

Datengerechtigkeit bezieht sich auf die Idee, dass Praktiken der Datenerstellung und Datennutzung unsere Gesellschaft gerechter machen, und nicht bestehende Ungerechtigkeiten noch verstärken sollen. Genauer gesagt wurde Datengerechtigkeit als ein Konzept für nationale und supranationale (= auf EU-Ebene) Gesetzgebungsprozesse definiert, das Fairness in der Art und Weise sicherstellt, wie Menschen als Datenproduzentinnen und -produzenten sichtbar gemacht, vertreten und behandelt werden. Dazu gehört auch die Fairness in der Art und Weise, in der Menschen datenbasierten Entscheidungen unterworfen werden.

Ausgehend von dieser Überlegung muss ein Rechtsrahmen, der Datengerechtigkeit durchsetzt, drei zentrale Ziele erreichen:

Erstens muss er der oder dem Einzelnen die rechtliche Möglichkeit geben, über die Erhebung und Verwendung ihrer oder seiner personenbezogenen Daten Bescheid zu wissen.

Zweitens muss er es den Menschen ermöglichen, ihre persönlichen Daten vor der automatisierten kommerziellen Nutzung auf den globalen Datenmärkten zu schützen und gleichzeitig die Nutzung der Daten für das Gemeinwohl zu fördern.

Drittens muss er technischen Bedingungen entgegenwirken, die zu direkter oder indirekter Diskriminierung führen können. Ein Beispiel dafür ist die Anwendung von Algorithmen zur Unterstützung der Entscheidungsfindung durch Behörden oder private Unternehmen.

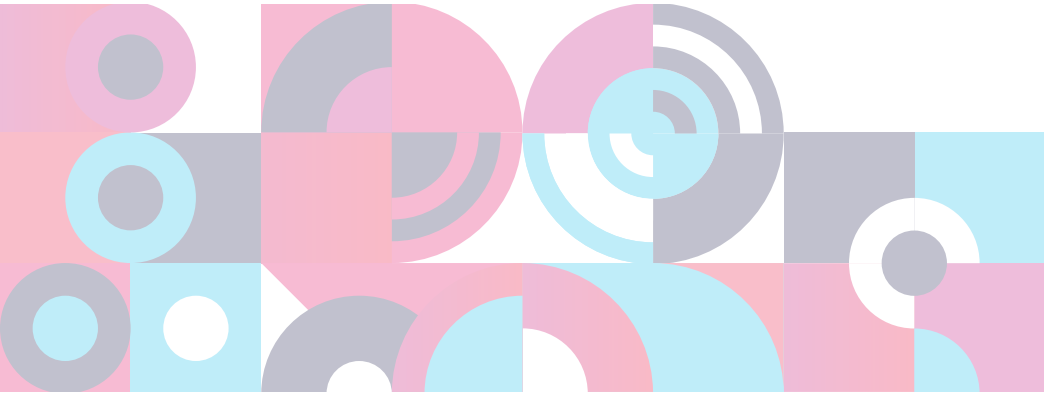
Manche Autorinnen und Autoren betonen auch *strukturelle* Faktoren in der Datengerechtigkeit. Strukturelle Gerechtigkeit stellt sicher, dass gesellschaftliche Systeme und Institutionen fair sind, gleiche Chancen bieten und Ungleichheiten reduzieren, um allen Menschen, insbesondere marginalisierten Gruppen, Möglichkeiten zur Verbesserung ihrer Gesundheit und ihrer Lebensumstände zu bieten. Strukturelle Gerechtigkeit befasst sich auch kritisch mit den Machtverhältnissen, in die die Produktion und die Nutzung von Daten in unserer Gesellschaft eingebettet sind. Ungerechtigkeiten wie Diskriminierung oder auch die ungerechte Verteilung von Profiten sehen diese Autorinnen und Autoren als das Ergebnis struktureller Bedingungen, die Machtpositionen und gesellschaftliche Beziehungen formen. Hier befasst sich Datengerechtigkeit insbesondere mit der Frage, wie der Zugang zu bestimmten Arten von Daten beispielsweise zwischen dem globalen Norden und Süden verteilt ist.

Datensolidarität und Datengerechtigkeit sind komplementär. Matthias Braun und Patrik Hummel etwa vertreten die Ansicht, dass Datensolidarität ein notwendiges, katalytisches Element für Datengerechtigkeit darstellt. Ihrer Meinung nach sind immer dann gemeinsame Solidaritätspraktiken erforderlich, wenn Ungerechtigkeiten im Bereich datengestützter Praktiken auftreten, die zu Diskriminierung oder Marginalisierung von Einzelpersonen oder Gruppen führen. Diese Praktiken müssen von Institutionen unterstützt und widergespiegelt werden. In diesem Sinne braucht Datengerechtigkeit gemeinsame Praktiken, die darauf abzielen, die Stimmen anderer zu hören (insbesondere die Stimmen marginalisierter Personen und Gruppen) und ihre Anliegen

als *gemeinsame* Probleme zu behandeln – und nicht nur als Probleme, die nur eben diese Gruppen etwas angehen. Dafür ist es notwendig, dass sich die Menschen auf gemeinsame Praktiken einlassen, die die Anliegen anderer berücksichtigen und darauf reagieren, um nachhaltige, reale Vereinbarungen über Datengerechtigkeit zu treffen.

Darüber hinaus kann die Datensolidarität dabei helfen, Ungerechtigkeiten als solche zu erkennen. Oft nehmen Menschen erst dann bewusst wahr, dass sie oder jemand anderes Unrecht erfahren haben, wenn sie ihre Erfahrungen mit den Erfahrungen anderer vergleichen. Ebenso können Solidaritätsbewegungen außenstehende Beobachterinnen und Beobachter auf mögliche Ungerechtigkeiten aufmerksam machen, die bestimmte Personen oder Gruppen erfahren. Solidarische Praxis ist daher nicht nur insofern relevant, als sie dabei helfen kann, Ungerechtigkeiten oder Unterdrückung zu reduzieren, sondern sie kann Entscheidungsträgerinnen und Entscheidungsträger dabei unterstützen, zu sehen, wo und wie sich Ungerechtigkeiten manifestieren.

Referenzen: Braun & Hummel, 2022; Heeks & Renken, 2018; Hummel & Braun, 2020; Prainsack et al., 2022b; Scholz, 2008; Shults, 2024; Taylor, 2017; Young, 1990.



1.6 Öffentlicher Wert *(Public Value)*

Der öffentliche Wert ist ein Schlüsselkonzept für die Datensolidarität. Er beschreibt den Wert, den eine Organisation oder Tätigkeit für die Gesellschaft hat.

Ursprünglich bezeichnete *Public Value* den Wert, der durch öffentliche Dienstleistungen und Verwaltung für die Gesellschaft geschaffen wird, und entsprach damit dem Konzept des *Shareholder Value*, das die Maximierung des Werts für Aktionäre als oberstes Ziel wirtschaftlichen Handelns versteht. Im weiteren Sinne kann *Public Value* als eine Methode zur Messung des Fortschritts bei der Verwirklichung breiter und weithin akzeptierter gesellschaftlicher Ziele verstanden werden. Beispiele sind der Übergang zu einer nachhaltigen globalen Ökologie, die Verringerung von Ungleichheit und die Förderung der Gesundheit. Ein solcher „auftragsorientierter" Ansatz für *Public Value* deckt sich mit der Forderung, dass die digitale Gesundheit nach den Grundsätzen der öffentlichen Gesundheit von öffentlichen Zwecken und nicht vom Streben nach kommerziellen Profiten angetrieben werden soll.

Im Rahmen der Datensolidarität hat eine Datennutzung dann hohen öffentlichen Wert *(Public Value)*, wenn plausibel davon ausgegangen werden kann, dass sie entweder für viele Menschen, für die Gesellschaft als Ganzes oder für künftige Generationen eindeutige Vorteile bringt und dass keine Person oder Gruppe durch die Datennutzung einen erheblichen und unangemessenen Schaden erleiden wird. Darüber hinaus ist der öffentliche Wert regelmäßig ausgeprägter, wenn der zu erwartende Nutzen für marginalisierte Gruppen höher ist.

Das bedeutet, dass im Rahmen der Datensolidarität nicht einfach Nutzen und Risiken abgewogen werden. Stattdessen kann eine Datennutzung nur dann hohen öffentlichen Wert haben, wenn sie Menschen keinen erheblichen Risiken aussetzt.

Zur Unterstützung einer strukturierten Bewertung des öffentlichen Wertes bestimmter Fälle von Datennutzung ist ein Online-Tool frei verfügbar (siehe **Kasten: PLUTO-Tool**). Dieses Tool kann als Entscheidungshilfe für Menschen dienen, die um Zugang zu ihren Daten gebeten werden oder auch die Entscheidungsfindung von Organisationen, öffentlichen Einrichtungen und Unternehmen, die Daten nutzen, unterstützen.

Referenzen: Bozeman, 2007; Bryson et al., 2014; El-Sayed et al., 2023; Fukumoto & Bozeman, 2019; Kattel & Mazzucato, 2018; Kickbusch et al., 2021; Mazzucato & Ryan-Collins, 2022; Meynhardt, 2009; Moore, 1995; Nabatchi, 2012; Nabatchi, 2018; Sorbie, 2021; Turkel & Turkel, 2016.

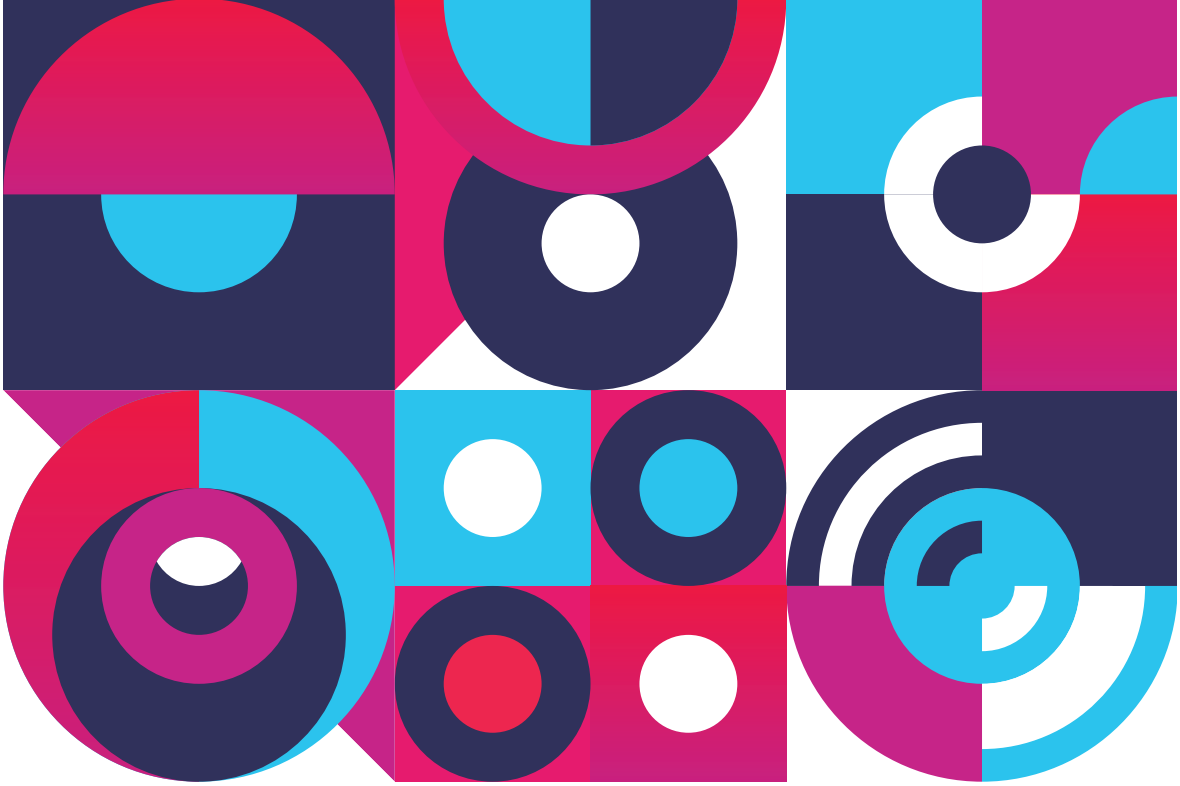
Kasten: Das Instrument zur Bewertung des öffentlichen Wertes (Public Value Assessment Tool, PLUTO)

Ein Team der Universität Wien hat ein Online-Tool entwickelt, das eine strukturierte Bewertung des öffentlichen Wertes (*Public Value*) der Datennutzung ermöglicht. Das Tool kann von allen genutzt werden, die wissen wollen, wieviel öffentlichen Wert eine bestimmte Datennutzung wahrscheinlich schafft: zum Beispiel von Unternehmen, Organisationen oder anderen Einrichtungen, die Daten nutzen, oder von Menschen, deren Daten genutzt werden.

Das Online-Tool besteht aus etwas mehr als 20 Fragen, die vier Bereiche abdecken: Informationen über die Organisation, die die Daten nutzt; die zu erwartenden Vorteile der Datennutzung; die Risiken der Datennutzung; und institutionelle Schutzmaßnahmen. Generell gilt: Je mehr eine bestimmte Datennutzung Menschen und Gemeinschaften nützt, ohne Einzelpersonen oder Gruppen zu gefährden, desto höher ist der öffentliche Wert. Nutzen und Schaden, die wahrscheinlich für unterversorgte oder anderweitig marginalisierte Gruppen eintreten, werden stärker gewichtet als Nutzen und Schaden für privilegierte Gruppen. Detaillierte Informationen zu den unterschiedlichen Gewichtungen der Antworten sind online auf der Website des Online-Tool verfügbar und für jeden mit Internetzugang offen einsehbar (https://pluto.univie.ac.at/).

Das PLUTO-Tool soll Menschen und Organisationen dabei helfen, auf strukturierte Weise über den öffentlichen Wert der Datennutzung nachzudenken. Es erhebt nicht den Anspruch, ein präzises und endgültiges Ergebnis zu liefern, und sollte nicht als alleinige Grundlage für eine Entscheidung verwendet werden. Der öffentliche Wert als Konzept ist nicht statisch, sondern entwickelt sich als Reaktion auf gesellschaftliche Veränderungen, technologische Fortschritte und sich wandelnde Werte. Infolgedessen muss PLUTO seine Kriterien und Definitionen im Laufe der Zeit möglicherweise anpassen, um relevant zu bleiben. Diese ständige Weiterentwicklung bedeutet auch, dass verschiedene Interessengruppen den öffentlichen Wert unterschiedlich interpretieren können, was zu fortlaufenden Debatten über die Wirksamkeit und Genauigkeit des Instruments führt.

Referenzen: El-Sayed & Prainsack, 2022; Prainsack & El-Sayed, 2023.



Abschnitt 2: Die Regulierung von Daten

2.1 Daten

Im allgemeinsten Sinne sind Daten Messwerte, die in ihrer Gesamtheit natürliche oder soziale Phänomene darstellen. Daten können auch als Messungen oder Werte beschrieben werden, die, wenn sie verarbeitet werden, Informationen ergeben. Der Begriff digitale Daten wiederum bezieht sich auf die Daten, die mit digitalen Mitteln gespeichert oder verarbeitet werden.

Wir sehen die Welt zunehmend durch Daten. Immer größere Teile unseres Körpers, unseres Verhaltens und unserer Umgebung, die früher nicht gemessen und nicht gezählt wurden, werden in Form von (digitalen) Daten erfasst. Gleichzeitig werden Daten zu einem Eckpfeiler unserer Gesellschaft, der Innovation, Effizienz und Entscheidungsfindung in verschiedenen Bereichen unterstützt oder sogar vorantreibt. Von der Gesundheitsversorgung über das Bildungswesen bis hin zum Finanzwesen und der Unterhaltungsbranche ermöglicht die Sammlung und Analyse von Daten personalisierte Dienste, vorausschauende Analysen und bessere Ergebnisse. Da die Menge der erzeugten Daten immer weiter zunimmt, wird ihre Bedeutung für die Gestaltung der Politik, die Verbesserung der Geschäftsabläufe und die Förderung des technologischen Fortschritts immer wichtiger. In diesem Zusammenhang steht der Begriff *„Big Data“* für Datensätze von noch nie dagewesenem Umfang, Vielfalt, Geschwindigkeit (d. h. Geschwindigkeit der Erfassung und Nutzung) und Wert.

Referenzen: Castells, 2002; Kitchin, 2014; Leonelli, 2020; Prainsack, 2019b; Rieder & Simon, 2017; van Dijck, 2014.

2.2 Datenverwaltung (Daten-*Governance*)

Daten-*Governance* bezieht sich auf das Gesamtmanagement der Verfügbarkeit, Nutzbarkeit, Integrität und Sicherheit der Daten, die gesammelt, verwendet und wiederverwendet werden. Dazu gehört das Erlassen von Richtlinien, Gesetzen, Verfahren und Standards, um sicherzustellen, dass Daten während ihres gesamten Lebenszyklus innerhalb von Organisationen sowie innerhalb und zwischen Ländern effektiv verwaltet werden.

Viele Länder sowie internationale und regionale Organisationen arbeiten daran, ihre Konzepte für die Datenverwaltung zu definieren. Ein prominentes Beispiel ist Indien, das der Datensouveränität, dem Schutz der Privatsphäre, der Förderung digitaler Innovationen, der Erleichterung der digitalen Integration und Entwicklung sowie der Gewährleistung größerer Sicherheit eine hohe Priorität einräumt. Ein weiteres Beispiel ist China, wo der Staat relativ leicht Zugang zu persönlichen Daten erhält und die Verwaltung digitaler Plattformen im Interesse des Wirtschaftswachstums und der nationalen Sicherheit liegt. Die Europäische Union hat Grundsätze für die Datenverwaltung aufgestellt, zu denen Rechtmäßigkeit, Fairness und Transparenz, Integrität und Vertraulichkeit sowie Verantwortlichkeit gehören.

Die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) hat mit ihren 38 Mitgliedsländern, die sich über die ganze Welt erstrecken – von Nord- und Südamerika bis hin zu Europa und dem asiatisch-pazifischen Raum –, im Jahr 2016 Empfehlungen für Daten-*Governance* erarbeitet. Zu den Empfehlungen gehören der individuelle Zugang zu Gesundheitsinformationen, die Einbeziehung von Interessengruppen in die Gestaltung von Strategien für Gesundheitsdaten, die Verwendung von Einwilligungen oder geeigneten Alternativen, die Bedeutung von Sicherheit und Datenschutz sowie die Optimierung von Daten und Technologien im öffentlichen Interesse.

Die Weltgesundheitsorganisation (WHO) hat die Notwendigkeit gemeinsamer Standards und koordinierter Ansätze erkannt, um das Potenzial des digitalen Wandels für die Gesundheit zu nutzen. In ihrer Globalen Strategie für digitale Gesundheit nennt die WHO die Interoperabilität und Governance von Gesundheitsdaten als zwei der dringendsten Bereiche für künftige internationale Vereinbarungen.

Hunderte von Organisationen forderten die WHO und ihre Mitgliedstaaten im Jahr 2021 auf, mit der Arbeit an einem globalen Rahmen für die Verwaltung von Gesundheitsdaten zu beginnen, der es ermöglicht, den Wert von Daten für das öffentliche Wohl zu nutzen und gleichzeitig die Rechte der und des Einzelnen sowie die Rechte von Gruppen, z. B. von Randgruppen, zu schützen. Die Verwaltung von Gesundheitsdaten sollte einen wichtigen Platz in allen gesundheitspolitischen Maßnahmen einnehmen, sei es auf globaler oder nationaler, regionaler oder lokaler Ebene .

Der Pandemievertrag, über den derzeit verhandelt wird, ist ein Beispiel auf globaler Ebene, die EU-Datenschutzgrundverordnung (DSGVO) und das Gesetz über künstliche Intelligenz (KI-Verordnung) sind Beispiele auf europäischer Ebene. Letzteres gilt für Anwendungen der künstlichen Intelligenz in allen EU-Ländern.

Die ASEAN-Länder (Verband Südostasiatischer Länder) setzen sich gemeinsam mit Japan für einen Ansatz des *„Data Free Flow with Trust“ (DFFT)* ein, der ein vertrauenswürdiges, interoperables

globales System zur Erleichterung des grenzüberschreitenden Datenverkehrs fördert *(„Cross Border Data Flows", [CBDF])*.

Die Afrikanische Union bemüht sich um die Entwicklung rechtlicher und regulatorischer Interoperabilität von Daten zwischen den rechtlich und kulturell unterschiedlichen 55 Mitgliedstaaten und um die Behebung des Mangels an Dateninfrastruktur.

Die *Lancet* und *Financial Times* Kommission schlug ein wertorientiertes *Governance*-Modell vor, das auf den Grundwerten Gleichheit, Datensolidarität, digitale Verwaltung und Vertrauen, Rechenschaftspflicht und öffentliche Beteiligung beruht. Während sich die oben genannten Initiativen und Strategien auf viele dieser Grundwerte beziehen, enthalten sie noch keinen ausdrücklichen Hinweis auf Datensolidarität. Datensolidarität ist ein spezifischer Ansatz für die Daten-*Governance*, der nicht nur die individuelle Kontrolle, sondern auch kollektive Formen der Aufsicht über und des Eigentums an digitalen Daten und Infrastrukturen in den Vordergrund stellt.

Referenzen: D4DHub, ohne Datum; Okinawa, 2024; He, 2023; Kickbusch et al., 2021; OECD, 2016; Struett et al., ohne Datum; Transform Health, 2022; World Health Organization, 2021.

2.3 Daten-*Stewardship*

Im Allgemeinen bezieht sich „Stewardship“ auf die verantwortungsvolle Verwaltung von Ressourcen oder Vermögenswerten, die einem anvertraut wurden. Sie betrifft auch Entscheidungen, die das langfristige Wohlergehen und die Interessen der Beteiligten oder Begünstigten in den Vordergrund stellen. Im Umweltbereich bedeutet *Stewardship*, die langfristige Erhaltung und Nachhaltigkeit von Ökosystemen zu fördern und gleichzeitig die Bedürfnisse der Bewohnerinnen und Bewohner dieser Ökosysteme zu erfüllen.

Im Gesundheitsbereich sind Daten-*Stewards* (Daten-Verwantwortliche) dafür verantwortlich, die gemeinsame Nutzung von und den Zugang zu Gesundheitsdaten zu fördern und gleichzeitig sicherzustellen, dass die Daten zweckdienlich und gemäß allen rechtlichen und ethischen Richtlinien genutzt werden. Sie sollten auch Strategien und Standards miterarbeiten, die datenbasierte Innovation fördern. Zu den wichtigsten Aufgaben der Daten-*Stewards* gehören:

- Sicherstellung der Einhaltung von Strategien, Standards und Verfahren für die Datenverwaltung und das Datenmanagement;
- Festlegung und Umsetzung von Maßnahmen und Prozessen zum Schutz von Daten vor unbefugtem Zugriff, Missbrauch oder Verstößen;
- Sicherstellung der Datenqualität durch Implementierung von Qualitätssicherungsprozessen;
- Sicherstellen, dass Daten ordnungsgemäß abgebildet, umgewandelt und vereinheitlicht werden, um ihre zweckmäßige Nutzung zu unterstützen;
- Beaufsichtigung der gesamten Datenwertschöpfungskette; und
- Gegebenenfalls Mitarbeit in Daten-*Governance*-Gremien.

Daten-*Stewards* überwachen die praktische Anwendung von Richtlinien und Standards für Daten, die von verschiedenen datenerzeugenden Stellen über die gesamte Datenwertkette hinweg stammen. Das reicht von der Erfassung, Speicherung und primären Nutzung bis hin zu verschiedenen Formen der Wiederverwendung von Datensätzen, die für andere Zwecke erhoben wurden. Auf diese Weise stellen Daten-*Stewards* sicher, dass zweckdienliche Daten für autorisierte Datennutzer nahtlos zur Verfügung stehen, um verwertbare Erkenntnisse zu gewinnen.

Dies unterscheidet Daten-*Stewards* von Daten-Treuhänderinnen und -Treuhändern, die für die Speicherung, die Verwaltung und den Schutz von Datenbeständen innerhalb ihrer eigenen Einrichtungen und Organisationen verantwortlich sind und gleichzeitig sicherstellen, dass die Daten gemäß den einschlägigen Vorschriften und Gesetzen weitergegeben werden. Beide Rollen sind wichtig, um sicherzustellen, dass Datenbestände effektiv verwaltet, geschützt und zum Wohle der Öffentlichkeit genutzt werden.

Referenzen: Plotkin, 2020; Public Health Agency of Canada, 2022.

2.4 Datensicherheit und Datenschutz

Datensicherheit und Datenschutz sind eng miteinander verknüpft. Sie konzentrieren sich auf den Schutz von Daten und Informationen im digitalen Bereich, behandeln jedoch unterschiedliche Aspekte des Umgangs mit und des Schutzes von Daten. Sie sind als ergänzende Praktiken zur Datensolidarität zu sehen.

Datensicherheit umfasst die Umsetzung von Maßnahmen und Protokollen zum Schutz digitaler Informationen vor unberechtigtem Zugriff, Offenlegung, Veränderung oder Zerstörung. Sie umfasst ein breites Spektrum von Praktiken und Technologien, die dazu dienen, Daten während ihres gesamten Lebenszyklus zu schützen. Dazu gehören Verschlüsselung, Zugangskontrollen, Firewalls, Antivirensoftware und andere Sicherheitsmaßnahmen, die darauf abzielen, Datenverletzungen zu verhindern und die Integrität und Vertraulichkeit von Informationen zu gewährleisten.

Datensicherheit ist ein entscheidender Aspekt für Unternehmen, Organisationen und Einzelpersonen, um sensible Daten zu schützen und das Vertrauen der Beteiligten zu erhalten.

Der Datenschutz konzentriert sich speziell auf die Kontrolle der Verwendung personenbezogener Daten – in der Regel werden darunter Daten verstanden, die sich auf eine bestimmte oder bestimmbare Person beziehen. Es geht um das Recht der Menschen, mitzubestimmen, wie und von wem Daten über sie verwendet werden und wie Organisationen personenbezogene Daten sammeln, verarbeiten und handhaben. Maßnahmen zum Schutz der Privatsphäre umfassen eine Reihe von Instrumenten wie z. B. die Einholung einer informierten Zustimmung vor der Datenerfassung und die Einhaltung von Datenschutzvorschriften und -richtlinien. Ziel des Datenschutzes ist es, den Menschen die Gewissheit zu geben, dass mit ihren persönlichen Daten verantwortungsvoll und ethisch korrekt umgegangen wird, und zu verhindern, dass Unbefugte auf sie zugreifen oder sie verwenden, was zu Datenschutzverletzungen oder zum Missbrauch sensibler Daten führen könnte. Sowohl die Datensicherheit als auch der Datenschutz sind integrale Bestandteile eines verantwortungsvollen Datenmanagements.

In der westlichen Welt ist Datenschutz sehr stark in einem individualistischen Weltbild verankert, was bedeutet, dass der Datenschutz vorwiegend als ein individuelles Recht definiert wird. Dieser individualistische Rahmen wird zunehmend durch empirische und normative Darstellungen in Frage gestellt, die zeigen, dass die Privatsphäre gleichzeitig nicht nur ein individuelles, sondern auch ein gesamtgesellschaftliches Interesse ist und sowohl durch individuelle als auch durch kollektive Rechte geschützt werden muss.

Datensolidarität erkennt an, dass Datensicherheit und Privatsphäre sowohl individuelle Bedürfnisse und Rechte als auch kollektive Güter sind, die dem Wohl ganzer Gesellschaften dienen. Die häufige oder sogar systematische Verletzung der Rechte einzelner Menschen verändert die Gesellschaft, und das Gleiche gilt auch andersherum: Die Menschen können ihre individuellen Rechte nur in einer Gesellschaft sinnvoll ausüben, in der gegenseitiger Respekt und Solidarität herrschen. Selbst wenn beispielsweise einzelne Menschen ein individuelles Recht auf freie Meinungsäußerung haben, kann dieses nicht ausgeübt werden, wenn es keine effektiven Sanktionen für Hass im Netz gibt.

Referenzen: Coventry & Branley, 2018; Ebeling, 2016; Harman et al., 2012; Koontz, 2017; Mittelstadt, 2017.

2.5 Digitale Souveränität

Digitale Souveränität bezieht sich auf die Regulierungs- und Kontrollmaßnahmen, die ein Staat oder eine supranationale Organisation (z. B. die EU) über digitale Daten und Infrastrukturen in seinem Zuständigkeitsbereich ausübt. Dazu gehört die Kontrolle darüber, wo Daten gespeichert werden, wie der Datenfluss organisiert ist und wer Zugang zu ihnen hat und sie kontrolliert. Wenn also eine chinesische oder amerikanische Plattform Daten von europäischen Nutzerinnen und Nutzern im EU-Raum exportiert und Nutzungen unterwirft, denen die Nutzerinnen und Nutzer nicht zugestimmt haben und die auch europäischen Datenschutzgesetzen widersprechen, dann verletzt dies die digitale Souveränität der EU.

Während sich der verwandte Begriff der Datensouveränität (siehe **Datensouveränität**) speziell auf die Politik und die Gesetze konzentriert, die die Datenspeicherung und -übertragung regeln, erstreckt sich die digitale Souveränität auf umfassendere technologische Aspekte, einschließlich der Infrastruktur, Plattformen und Dienste, die die Datennutzung und -speicherung unterstützen. Digitale Souveränität umfasst somit Kontrolle über Daten, aber auch Kontrolle über Hardware, Software und Netzwerkressourcen, die digitale Interaktionen ermöglichen.

Digitale Souveränität wird in der heutigen vernetzten Welt immer wichtiger. Staaten und Regionen versuchen, die Kontrolle über ihr digitales Umfeld (wieder) zu erlangen, um sich vor externen Abhängigkeiten und Schwachstellen zu schützen. Die EU beispielsweise setzt sich für größere digitale Souveränität ein, um die Abhängigkeit von Nicht-EU-Technologien zu verringern und die Einhaltung der EU-Datenschutzstandards zu gewährleisten.

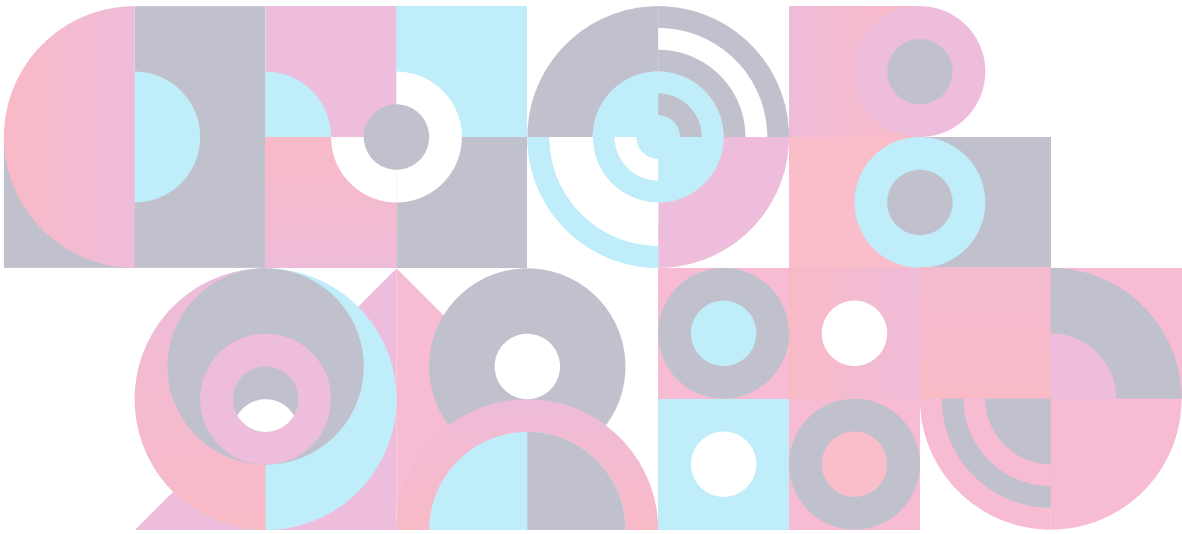
Unter dem Begriff der digitalen Souveränität wird ein breites Spektrum von Themen und Anliegen zusammengefasst. Dazu gehört die Frage, welche Kontrolle die Betroffenen über den Umgang mit ihren Daten haben sollen und wie diese Kontrolle umgesetzt werden kann. Diese Kontrolle kann auf der Ebene von Einzelpersonen oder Kollektiven (z. B. Familien, Patientenorganisationen, Gebietskörperschaften wie Gemeinden oder Ländern) erfolgen. Darüber hinaus stellt sich die Frage, wie Staaten oder internationale Organisationen sowohl die materiellen als auch die immateriellen Aspekte der digitalen Infrastrukturen verwalten und kontrollieren können.

Die Bedeutung der digitalen Souveränität wird durch die zunehmenden geopolitischen Spannungen im Zusammenhang mit Technologie noch unterstrichen. Viele Staaten sind misstrauisch gegenüber ausländischer Überwachung und Datenschutzverletzungen, die die nationale Sicherheit und wirtschaftliche Interessen gefährden können. Durch die Durchsetzung der digitalen Souveränität versucht die EU etwa, die Privatsphäre ihrer Bürgerinnen

und Bürger zu schützen und sicherzustellen, dass kritische digitale Infrastrukturen gegen externe Bedrohungen gewappnet sind.

Unter digitaler Souveränität werden häufig Gesetze und Regelwerke verstanden, die eine lokale Datenspeicherung und -verarbeitung vorschreiben, um sensible Informationen innerhalb der Landesgrenzen zu halten. Einige Länder haben beispielsweise Gesetze zur Datenlokalisierung erlassen, die Unternehmen dazu verpflichten, Daten auf Servern zu speichern und zu verarbeiten, die sich physisch im Land befinden. Dadurch wird nicht nur die Datensicherheit erhöht, sondern auch sichergestellt, dass die Daten den lokalen Gesetzen und Vorschriften unterliegen.

Referenzen: Broeders et al., 2023; Floridi, 2020; Sciences Po, ohne Datum; Tietoevry, 2023; Gordon, 2024.



2.6 Datensouveränität

Die Datensouveränität bezieht sich auf die Regeln, Technologien und Praktiken, die dazu beitragen können, einige der grundlegenden Prinzipien der digitalen Souveränität zu schützen. Ein Beispiel ist die Frage, wo die Daten gespeichert werden, wer die Kontrolle darüber hat, wie sie sicher gespeichert und verarbeitet und wie sie interoperabel und übertragbar gemacht werden können. Inhaberinnen und Inhaber von Datensouveränität können also Einzelpersonen, Organisationen, Unternehmen, Regierungen oder ganze Gesellschaften und Länder sein. Dies kann zu widersprüchlichen Ansprüchen an die Datenhoheit auf diesen Ebenen führen.

Wenn sie sich auf natürliche Personen bezieht, ist die Datensouveränität eng mit dem Begriff der digitalen Selbstbestimmung verbunden, der das individuelle Recht und die Fähigkeit einer Person bezeichnet, Autonomie über ihre digitale Präsenz, ihre Daten und ihre Online-Aktivitäten auszuüben. Soweit sich die Datensouveränität auf die kollektive Kontrolle über Daten bezieht, kann sie sich auf Ansprüche von Gemeinschaften (z. B. indigene Personen und Gemeinschaften) oder Nationen beziehen, die Kontrolle darüber auszuüben, welche Phänomene datenmäßig erfasst, wie Daten verwendet werden und wer davon profitiert (siehe **Indigene Datenhoheit**).

Aufgrund ihrer unterschiedlichen Herangehensweise an zentrale Fragen der Kontrolle über Daten können drei große Rechtssysteme der Welt – die USA, China und die EU – als drei verschiedene Systeme der Datensouveränität repräsentierend gesehen werden, nämlich die Unternehmenssouveränität (USA), die staatliche Souveränität (China) und die individuelle Souveränität (EU). Datensouveränität wird auch im Zusammenhang mit der Gestaltung der IT-Architektur und den Gesetzen, die die Datenverarbeitung regeln, heftig diskutiert.

In praktisch allen ihren unterschiedlichen Konzeptionen zielt digitale Souveränität darauf ab, die Kontrolle und Macht kollektiver Akteure über Daten zu stärken. Die Art der Macht, um die es geht, ist – anders als in einigen klassischen Konzepten der Souveränität – keine rohe Gewalt, sondern eine Machtausübung, die Werte wie Einbeziehung, Deliberation und die Grundrechte der betroffenen Personen respektiert.

In dem Maße, in dem Datensouveränität darauf abzielt, kollektive Kontrolle über Daten zu verbessern, teilt sie ein zentrales Anliegen mit Datensolidarität. Im Gegensatz zu Datensouveränität ist Datensolidarität jedoch nicht in erster Linie auf den Staat oder die Gemeinschaft ausgerichtet, sondern zielt darauf ab, durch politische Instrumente auf allen Ebenen – lokal, kommunal, national und global – eine gerechtere Verteilung von Vorteilen und Risiken zu unterstützen.

Referenzen: Gao, 2021; Hummel et al., 2021; Sciences Po, ohne Datum; Verhulst, 2023; Woods, 2018.

2.7 Indigene Datenhoheit

Indigene Datensouveränität ist ein Konzept, das das Recht indigener Menschen und Gemeinschaften betont, die von und über ihre Gemeinschaften gesammelten Daten zu kontrollieren.

Es besagt, dass Daten, die sich auf indigene Gruppen beziehen, gemäß den Normen, Werten und Interessen der Gemeinschaften, aus denen die Daten stammen, verwaltet und geregelt werden sollen.

Diese Idee stellt die vorherrschenden westlichen Daten-*Governance*-Modelle in Frage, die indigene Rechte und die einzigartigen kulturellen, kontextuellen und historischen Umstände indigener Gemeinschaften nicht berücksichtigen. Dies betrifft insbesondere die Schäden, die durch koloniale Herrschaft entstanden sind (sowie die Rechte und Interessen anderer marginalisierter Gruppen).

Von besonderer Bedeutung im Zusammenhang mit indigener Datensouveränität sind die so genannten CARE-Prinzipien. Sie stehen für Kollektiven Nutzen, Kontrollbefugnis, Verantwortung, und Ethik (auf Englisch: *Collective Benefit*, *Authority to Control*, *Responsibility and Ethics*), die als Ergänzung zu den FAIR-Prinzipien (*Findability, Accessibility, Interoperability and Reusability* – Auffindbarkeit, Zugänglichkeit, Interoperabilität und Wiederverwendbarkeit) eingeführt wurden. Während sich die FAIR-Grundsätze auf die technischen Aspekte von Daten konzentrieren, stellen die CARE-Grundsätze die Menschen und den Zweck hinter der Datenerhebung und -nutzung in den Mittelpunkt:

- Kollektiver Nutzen *(Collective Benefit)*: Die Gestaltung und Funktion von Datenökosystemen sollte es indigenen Gemeinschaften ermöglichen, Nutzen aus den von ihnen erhobenen Daten zu ziehen. Dazu gehört, dass die Daten in einer Weise genutzt werden, die indigene Werte und Selbstbestimmung unterstützt.

- Kontrollbefugnis *(Authority to Control)*: Indigene Gemeinschaften müssen die Befugnis haben, über die sie betreffenden Datenerhebungsprozesse zu bestimmen, einschließlich des Rechts zu kontrollieren, wie diese Daten erhoben, abgerufen und verwendet werden.

- Verantwortung *(Responsibility)*: Diejenigen, die mit den Daten umgehen, haben die Pflicht sicherzustellen, dass sie in einer Weise verwendet werden, die die Rechte und das Wohlergehen der indigenen Bevölkerung respektiert und dass angemessene Maßnahmen ergriffen werden, um den Schaden zu minimieren und den Nutzen für die indigenen Gemeinschaften zu maximieren.

- Ethik *(Ethics)*: Die Daten-*Governance*-Praktiken müssen sich an einem ethischen Rahmen orientieren, der von indigenen Weltanschauungen geprägt ist, zu denen oftmals Werte wie Gegenseitigkeit, Respekt und Sorge um die Gemeinschaft gehören.

Indigene Datensouveränität ist auch eng mit den Bemühungen verbunden, historische Ungerechtigkeiten zu adressieren und indigene Menschen und Gemeinschaften zu stärken, indem ihre Kontrollrechte über ihre Daten respektiert werden. Dazu gehört auch Kontrolle über Daten, die im öffentlichen Sektor, der wissenschaftlichen Forschung, oder der Gesundheitsversorgung verwendet werden. Die wirksame Umsetzung der Datensouveränität indigener Gemeinschaften kann zu besser zugeschnittenen Diensten und Maßnahmen, einem besseren Schutz der Privatsphäre

und einer größeren Achtung des indigenen Kulturerbes führen.

Indigene Datensouveränität steht somit im Einklang mit dem Ziel der Datensolidarität, eine gerechtere Aufteilung von Risiken und Vorteilen digitaler Praktiken zu erreichen und – neben der Achtung der individuellen Autonomie – auch kollektive Instrumente der Kontrolle und Aufsicht über Daten und digitale Infrastrukturen zu stärken.

Datensolidarität und indigene Datensouveränität sind auch insofern miteinander verbunden, als sie die in westlichen Daten-*Governance*-Ansätzen dominierende Abgrenzung zwischen persönlichen Daten (also jenen, die sich auf ein bestimmtes oder bestimmbares Individuum beziehen) und nicht-persönlichen Daten, die sich auf kein bestimmtes oder bestimmbares Individuum beziehen, überwinden wollen. Sowohl die Datensolidarität als auch die indigene Datensouveränität erkennen an, dass Menschen – als Einzelpersonen und als Mitglieder von Kollektiven – wichtige Interessen an Daten haben können, die im technischen Sinne nicht „personenbezogen" sind (d. h. sie beziehen sich nicht auf eine identifizierte oder identifizierbare Person und fallen daher nicht in den Geltungsbereich vieler Datenschutzregelungen weltweit).

Referenzen: Benjamin, 2019; Carroll et al., 2020; First Nations Centre, 2007; First Nations Information Governance Centre, 2014; Kukutai & Taylor, 2016; McDonald, 2022; Saxinger & First Nation of Na-Cho Nyak Dun, 2018; UN General Assembly, 2007; Wilkinson et al., 2016.

2.8 Datenlokalisierung

Datenlokalisierung bezieht sich auf die von Regierungen auferlegte gesetzliche Vorschrift, dass Daten, die innerhalb ihrer Grenzen erzeugt werden, im Inland gespeichert und verarbeitet werden müssen. Diese Vorschriften zielen darauf ab, Datensouveränität zu gewährleisten, d. h. die Daten unterliegen den Gesetzen und der Verwaltung des Landes, in dem sie erstellt wurden.

Dies ist besonders wichtig für Daten in sensiblen Bereichen wie dem Finanzwesen, dem Gesundheitswesen oder der nationalen Sicherheit, wo der Schutz der Privatsphäre und die Datensicherheit von größter Bedeutung sind. Staaten setzen die Datenlokalisierung durch, um sich vor unbefugtem Zugriff aus dem Ausland zu schützen, die Privatsphäre zu wahren und den lokalen Strafverfolgungsbehörden den Zugriff auf die Daten zu Ermittlungs- und Regulierungszwecken zu ermöglichen.

Befürworter der Datenlokalisierung argumentieren, dass der Verbleib der Daten innerhalb nationaler Grenzen Datensicherheit und Datenschutz verbessert, da die Länder ihre eigenen Vorschriften innerhalb ihrer eigenen Grenzen direkt durchsetzen können. Außerdem wird die lokale Wirtschaft durch die Schaffung von Arbeitsplätzen in Rechenzentren, beim *Cloud Computing* und bei der Entwicklung der IT-Infrastruktur gefördert. Darüber hinaus kann es aufstrebenden Volkswirtschaften helfen, lokale Technologieindustrien zu fördern, indem sichergestellt wird, dass die Datenverarbeitungsressourcen im Land bleiben.

Die Kritiker der Datenlokalisierung weisen auf mehrere Nachteile hin. Sie argumentieren, dass dies die Kosten für multinationale Unternehmen erhöhen kann, die gesetzliche Normen mehrere Länder einhalten müssen. Das kann auch den grenzüberschreitenden Datenfluss behindern und damit die globale Innovation und Zusammenarbeit einschränken. Darüber hinaus können die Anforderungen an die Datenlokalisierung den Zugang zu den fortschrittlichsten Datenverarbeitungswerkzeugen behindern, die sich häufig in anderen Regionen befinden, und so den technologischen Fortschritt innerhalb des Landes einschränken.

Im Rahmen der Datensolidarität ist die Datenlokalisierung eine willkommene Entwicklung, wenn sie zu mehr Gerechtigkeit zwischen Ländern und Weltregionen beiträgt, d. h., wenn sie von digital benachteiligten Nationen genutzt wird, um ihnen mehr Vorteile zu verschaffen. Wenn sie von reichen Nationen genutzt wird, um ihren Vorteil zu festigen, hält die Datensolidarität die Datenlokalisierung für schädlich.

Referenzen: Chander, 2020; Chander & Lê, 2014; Liu, 2022; Taylor, 2020.

2.9 Schadenslinderung

Die Schadenslinderung ist eine der drei Säulen der Datensolidarität (siehe **Tabelle 2: Die drei Säulen der Datensolidarität**). Wann immer Daten verwendet werden – auch wenn sie für Menschen und Gemeinschaften von großem Nutzen sind – besteht das Risiko, dass Einzelpersonen oder Gruppen Schaden nehmen. Wenn beispielsweise sensible persönliche Informationen offengelegt werden, kann dies zu Identitätsdiebstahl und finanziellen Verlusten führen. Die unbefugte Weitergabe von Daten kann auch zu Diskriminierung führen, da Menschen aufgrund ihrer Datenprofile ungerecht behandelt werden könnten, was ihren Zugang zu Arbeitsplätzen, Versicherungen und Dienstleistungen beeinträchtigen kann. Schließlich kann eine umfassende Datenerfassung und -überwachung die persönlichen Freiheiten aushöhlen und die freie Meinungsäußerung und andere Freiheiten einschränken, weil man befürchtet, überwacht zu werden.

Wir müssen zwar versuchen, die Risiken so weit wie möglich zu verringern. Dennoch ist es wichtig, offen anzuerkennen, dass auch dann immer noch Schäden auftreten können. Menschen, die einen Schaden aufgrund der Nutzung von Daten erlitten haben – entweder aufgrund ihrer eigenen Daten, oder von Daten Dritter, aus denen Schlüsse auf sie gezogen wurden –, müssen angemessene Unterstützung und Entschädigung erhalten. Heute ist dies oft nicht der Fall, weil rechtliche Maßnahmen nur dann ergriffen werden können, wenn man genau bezeichnen kann, wer oder welches Verhalten genau den Schaden verursacht hat. In Zeiten komplexer Datenwege und des Teilens von Daten über viele Plattformen und Ländern hinweg wird es immer schwieriger, die Wege, die Daten in ihrer Nutzung nehmen, genau nachzuvollziehen. Ebenso wird es dadurch immer schwieriger, das schädigende Verhalten genau zu identifizieren und einer natürlichen oder juristischen Person zuzurechnen.

Generell können Schäden entweder durch die Nutzung oder durch die Nichtnutzung von Daten entstehen. Schäden durch die Datennutzung können zu Verletzungen der Privatsphäre, emotionalen Schäden oder Verletzungen kultureller Rechte führen. Zu den Schäden durch die Nichtnutzung von Daten gehören körperliche Schäden, die dadurch entstehen, dass die medizinische Vorgeschichte nicht bekannt ist, dass auf Erkrankungen nicht zeitnah reagiert wird, dass wissenschaftliche Forschung behindert wird, dass Ungleichbehandlung nicht erkannt wird, oder dass die Kosten des Gesundheitssystems durch unnötige doppelte Datenerhebung und Datenanalyse steigen (weil Daten z. B. nicht zwischen mehreren Gesundheitsdienstleistern geteilt werden). Bei der Betrachtung von Risiken im Zusammenhang mit Schäden wird idealerweise das gesamte Spektrum datenbezogener Schäden

mit ihren Wahrscheinlichkeiten und Auswirkungen berücksichtigt.

Wie bereits erwähnt haben Menschen und Gruppen, die Schäden aufgrund der Nutzung oder Nichtnutzung von Daten erleiden, häufig keinen Zugang zu Unterstützung, weil es ihnen nicht möglich ist, genau nachzuvollziehen, was und wer den Schaden verursacht hat. Ein weiterer Grund für fehlende Unterstützung liegt darin, dass Schäden manchmal auch dann entstehen, wenn keine Gesetze gebrochen werden, z. B., wenn Menschen höhere Preise für die gleichen Dienstleistungen in Rechnung gestellt werden als anderen oder ihnen aufgrund von prädiktiven Analysen Dienstleistungen verweigert werden. Menschen können auch durch digitale Plattformen wie *Instagram*, *TikTok* oder *LinkedIn* Schäden erleiden, ohne dass die Inhalte illegal sind. In diesem Fall haben die betroffenen Menschen überhaupt keine Handhabe. Je mehr Daten ausgetauscht und miteinander verknüpft werden und je weniger transparent diese Prozesse sind, desto schwieriger wird es für die Betroffenen zu erkennen, was oder wer für den Schaden, den sie erlitten haben, verantwortlich ist. Und schließlich haben manche Menschen keinen Zugang zu Rechtsmitteln, weil ihnen die sozialen und wirtschaftlichen Ressourcen, so auch Wissen über ihre rechtlichen Möglichkeiten, fehlen.

Unter dem Gesichtspunkt der Datensolidarität ist es von entscheidender Bedeutung, dass Menschen, die durch die Datennutzung geschädigt wurden, Zugang zu Unterstützung haben, unabhängig davon, wo auf der Welt sie sich befinden.

Eine Möglichkeit, dies zu tun, ist die Einrichtung von Schadenslinderungsstellen. Schadenslinderungsstellen sind unabhängige Organisationen, die Beschwerden von Personen prüfen, die behaupten, durch die Nutzung ihrer eigenen Daten oder der Daten Dritter geschädigt worden zu sein. So könnte etwa gesetzlich verfügt werden, dass jede Organisation ab einer bestimmten Größe einer Schadenslinderungsstelle angeschlossen sein muss – also etwa so wie eine Versicherungspflicht.

Die Schadenslinderungsstellen sollten drei Hauptfunktionen erfüllen:

Erstens wären sie eine De-facto-Überwachungsstelle für die Schäden, die Personen melden, die ihnen entstanden sind. Die für die Datenverarbeitung verantwortlichen Personen in Unternehmen, Behörden oder anderen Organisationen können auf der Basis dieser Informationen dann die Funktionsweise der Systeme der Datenverwaltung verbessern.

Zweitens sollten Personen, die einen finanziellen Schaden erlitten haben und nicht in der Lage waren, anderweitig Unterstützung zu erhalten, in bestimmten Fällen auch die Möglichkeit haben, finanzielle Unterstützung zu erhalten. Anders als bei formalen Rechtsmechanismen muss kein Fehlverhalten oder eine direkte rechtliche Verursachung des erlittenen Schadens nachgewiesen werden.

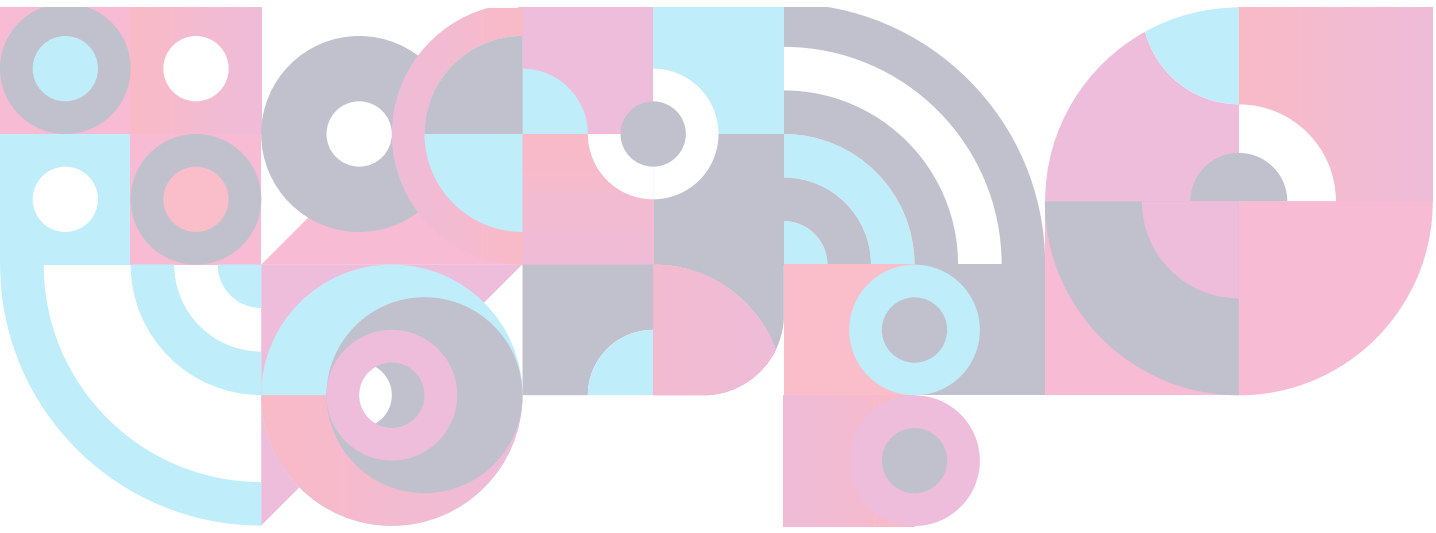
Drittens würden die Schadenslinderungsstellen Informationen darüber erhalten, wo Datenzugang im öffentlichen Interesse nicht rechtzeitig und in der erforderlichen Qualität stattfindet

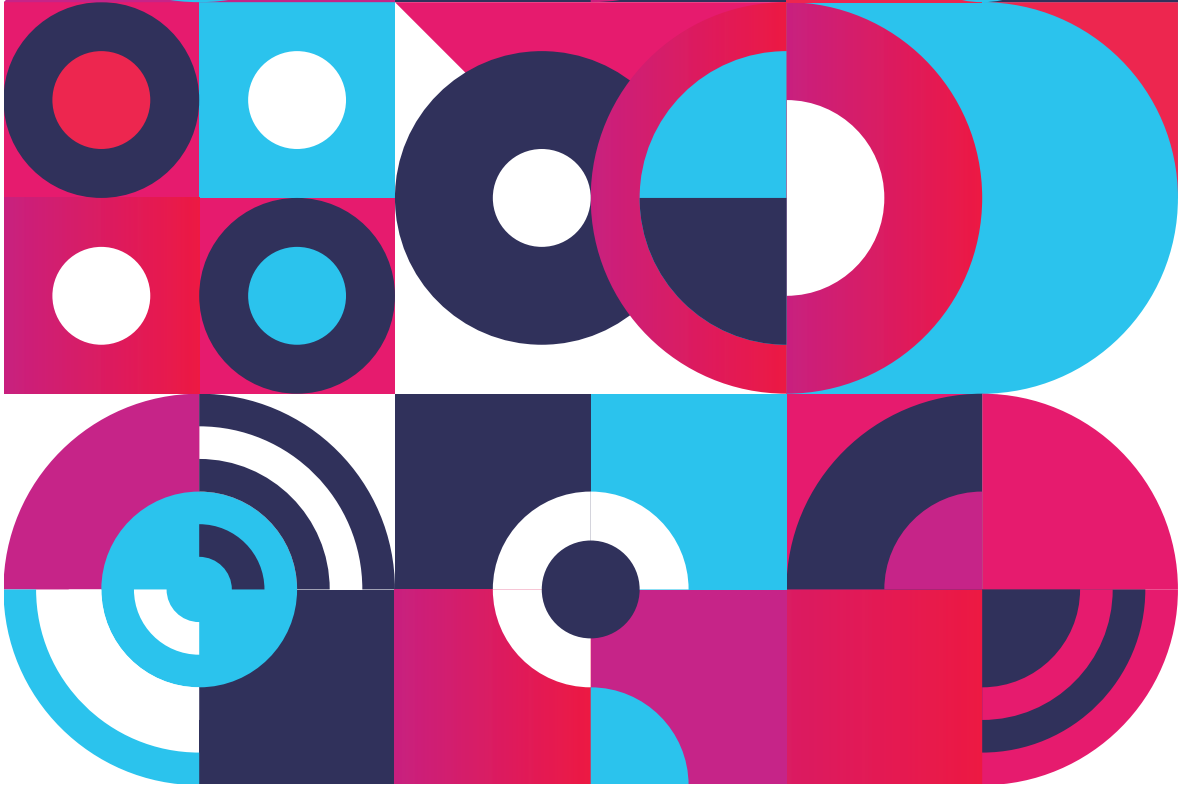
– nämlich dann, wenn Personen oder Gruppen Schaden aus der Nichtnutzung von Daten melden. In solchen Fällen würde die Schadenslinderungsstelle die potenziellen Auswirkungen der Nichtnutzung von Daten auf Gemeinschaften quantifizieren und versuchen, geeignete Maßnahmen zur Behebung des Problems zu initiieren.

Neben der Einführung von Schadenslinderungsstellen sollten weitere Maßnahmen zur Schadenslinderung erweitert werden, die es in manchen Ländern und Organisationen schon gibt. Dazu gehören Pläne zur Linderung von Datenschutzverletzungen, in denen Umsetzungspläne für die Eindämmung, Untersuchung und Behebung von Datenschutzverletzungen festgelegt sind. Evaluierungen und Überprüfungen nach einem Vorfall können helfen, die Ursachen des Schadens in bestimmten Fällen zu verstehen und die Datenverwaltung zu verbessern. Die Berichtigung von Daten und die Löschung von Daten bieten betroffenen Personen zudem die Möglichkeit, fehlerhafte Daten zu korrigieren, persönliche Daten zu löschen und weitere missbräuchliche Nutzung zu verhindern.

Unabhängig davon, welche Maßnahmen gewählt werden, muss Schadenslinderung als separate, zusätzliche Maßnahme neben der Risikominimierung stattfinden.

Referenzen: Taylor et al., 2017; McMahon et al., 2020; Prainsack et al., 2022a; b; Affleck et al., 2024.





Abschnitt 3: Gemeinsame Nutzung von Daten

3.1 Digitale und Datengemeinschaften (Daten-*Commons*)

Im Kontext der Datensolidarität sind Daten-*Commons* eine Möglichkeit, die kollektive Kontrolle über und das Eigentum an Daten und digitalen Infrastrukturen zu stärken. *Commons* sind soziale Einrichtungen zur Verwaltung gemeinschaftlicher Ressourcen bzw. Gemeingüter. Innerhalb von *Commons* werden Gemeingüter nach den Grundsätzen der Fairness, Gleichheit, Gerechtigkeit und Nachhaltigkeit verwaltet.

Gemeingüter haben eine lange rechtliche und historische Tradition in Bereichen, die von der landwirtschaftlichen Bodennutzung über Wälder bis hin zu Bildungsressourcen reichen. In der wissenschaftlichen Literatur gibt es Debatten darüber, inwieweit die Regeln von *Commons* von materiellen Gütern – wie Weideflächen oder Seen – auf teils immaterielle Ressourcen wie digitale Daten angewendet werden können. Einige Autorinnen und Autoren verwenden den Begriff der Gemeingüter in einem noch weiteren Sinne, indem sie auch Daten damit bezeichnen, die der öffentlichen Nutzung dienen. Ein so weit gefasstes Verständnis von Gemeingütern bzw. *Commons* ist problematisch, da es *Commons*-Regime, bei denen die Menschen gemeinsam Eigentümer der Ressource sind und über deren Nutzung entscheiden, mit *Open-Access*-Systemen gleichsetzt, bei denen jeder die Ressource nach Belieben nutzen und niemand ausgeschlossen werden kann.

Die Digital-*Commons*-Bewegung wuchs einerseits nach der Bankenkrise von 2008, und andererseits in den 2010er Jahren, als der Zugang zu wissenschaftlicher Literatur immer teurer wurde. Überall auf der Welt entstanden Freiwilligenorganisationen, die nichtkommerzielle Infrastrukturen zur gemeinsamen Nutzung von Ressourcen schafften. Ihr Ziel war es, eine Alternative zu den herrschenden Machtstrukturen und kommerziellen Märkten zu schaffen. Der Erfolg dieser Initiativen wurde durch die Kommerzialisierung vieler vormals gemeinnütziger Wissensressourcen beeinträchtigt, aber auch dadurch, dass Akteurinnen und Akteure in reichen Ländern und Institutionen es sich leichter leisten konnten, ihre Daten und Ressourcen allgemein zugänglich zu machen und auch „offene" Daten und Ressourcen anderer besser nutzen konnten. Diese Probleme verdeutlichen einmal mehr die Grenzen von so genannten „*Commons*"-Konzepten, bei denen es sich eigentlich um *Open-Access*-Regelungen handelt, in denen es also niemanden gibt, der oder die den Zugang anderer regulieren kann. *Open-Access*-Regime neigen dazu, einen „Matthäus-Effekt" zu entfalten: Wenn alles für alle zugänglich ist, können diejenigen, die bereits über mehr Macht und Ressourcen verfügen, mehr von der offenen Ressource nehmen. Daten-*Commons* hingegen hätten klare Regelungen darüber, wer wie viel wovon nehmen kann, und was in das *Commons* zurückgegeben werden muss.

Datensolidarität befürwortet Daten-*Commons* als eine Möglichkeit, auf lokaler, regionaler, nationaler oder transnationaler Ebene Daten oder digitale Infrastrukturen gemeinsam zu besitzen und zu verwalten. Sie unterstützt keine Regelungen, in denen Daten allen frei zugänglich gemacht werden, da dies bedeutet, dass es kein kollektives Eigentum an der Ressource gibt und jeder sie nach Belieben nutzen kann.

Digitale und Daten-*Commons*, die mit dem Geist der Datensolidarität vereinbar sind, sind etwa Plattformen, auf denen die Daten von allen, die zu den Daten beitragen, gemeinsam verwaltet werden, um Transparenz und gerechte Nutzung zu gewährleisten. Ein neuer Trend in diesem Zusammenhang ist die Einrichtung „virtualisierter Datengemeinschaften". In solchen Fällen werden die Daten nicht kopiert oder in einem einzelnen Datenbestand konsolidiert. Vielmehr verbleiben die Daten an der Quelle und sind im gesamten Netz über einen vereinbarten gemeinsamen Abfragemechanismus verfügbar. Solche virtualisierten Datenbestände unterstützen unter anderem föderatives Lernen. Sie erfüllen gemeinsam festgesetzte Kriterien in der Dateninteroperabilität. Darüber hinaus sind politische Kontrollen, Schulungen und das Engagement der Beteiligten erforderlich, um das Vertrauen zu erlernen und zu erhalten. Solche virtualisierten Datengemeinschaften werden bei transnationalen Initiativen, wie z. B. im Europäischen Gesundheitsdatenraum *(EHDS)*, immer häufiger anzutreffen sein.

Referenzen: Bollier & Helfrich, 2019; De Angelis, 2017; Dulong & Stalder, 2020; Fuster Morell, 2011; Micheli et al., 2023; Paprica et al., 2023; Prainsack, 2019a; Terzis et al., 2023.

3.2 Datengenossenschaften (Daten-Kooperativen)

Daten-Kooperativen sind Organisationen, in denen Menschen ihre Daten zum gegenseitigen Nutzen zusammenführen. Dieser Begriff wird oft synonym mit Daten-*Commons* verwendet. Beide stellen kollektive Formen des Besitzes und der Verwaltung von Daten dar. Wenn zwischen Daten-*Commons* und Daten-Kooperativen unterschieden wird, dann um die folgenden Merkmale hervorzuheben, die Kooperativen charakterisieren: freiwillige Mitgliedschaft, demokratische Kontrolle, wirtschaftliche Beteiligung, Autonomie von anderen kommerziellen oder öffentlichen Einrichtungen und eine Orientierung an öffentlichen Werten.

Durch den Zusammenschluss können die Mitglieder von Daten-Kooperativen bessere Bedingungen mit datennutzenden Organisationen aushandeln, während sie gleichzeitig eine größere Kontrolle über die Verwendung der Daten behalten. Während einige Datenkooperativen in erster Linie darauf abzielen, öffentlichen Wert (siehe **Öffentlicher Wert *[Public Value]***) zu schaffen, dienen andere (auch) dem Zweck, Menschen dabei zu helfen, ihre Daten profitabel zu verkaufen.

Wie Daten-*Commons* können auch Daten-Kooperativen dazu beitragen, Datensolidarität zu verwirklichen, wenn die Orientierung am öffentlichen Wert nicht durch partikulare oder gewinnorientierte Interessen überlagert wird.

Referenzen: Blasimme et al., 2018; Hardjono & Pentland, 2020; Micheli et al., 2023; Zhu & Marjanovic, 2022.

3.3 Datentreuhandgesellschaften *(Data Trusts)*

Datentreuhandgesellschaften (*Data Trusts*) sind rechtliche Strukturen, die die Verwendung von Daten im Namen einzelner Personen oder Gruppen von Begünstigten verwalten. Die Treuhänderinnen und Treuhänder in Datentreuhandgesellschaften treffen Entscheidungen über die Nutzung und Verwaltung von Daten auf der Grundlage der Interessen der Begünstigten. Die Treuhänderinnen und Treuhänder haben die Pflicht, im besten Interesse der Begünstigten zu handeln und sicherzustellen, dass die Daten verantwortungsvoll und ethisch korrekt verwendet werden.

Datentreuhandgesellschaften können eingerichtet werden, um verschiedene Ziele zu erreichen, wie die Erzielung kommerzieller Profite oder die Maximierung des Gemeinwohles. Datentreuhandgesellschaften bieten einen Mechanismus, mit dem Einzelpersonen und Gruppen ein gewisses Maß an Kontrolle über ihre Daten behalten können, während sie anderen Parteien deren Nutzung auf zuvor vereinbarte Weise ermöglichen.

Sogenannte „*Data Vaults*“, also „Daten-Safes“, können als technische Architektur dienen, die die Grundlage für Datentreuhandgesellschaften bildet und es Unternehmen ermöglicht, Daten sicher zu speichern und gleichzeitig vertrauenswürdigen Parteien den Zugriff auf die erforderlichen Daten zu ermöglichen. Es handelt sich dabei um eine Methode, die für große Datenumgebungen entwickelt wurde, insbesondere für solche, die sich schnell an neue Anforderungen oder Änderungen anpassen müssen. Ihr Schwerpunkt liegt auf Skalierbarkeit, Flexibilität und konsistenter Integration von Daten aus verschiedenen Quellen.

Der Hauptunterschied zwischen Datengemeinschaften und -genossenschaften einerseits und Datentreuhandgesellschaften andererseits liegt in ihren Verwaltungs- und Eigentumsstrukturen. Im Falle von Daten-*Commons* und Daten-Genossenschaften sind die Daten – zumindest moralisch oder sogar rechtlich – das gemeinsame Eigentum aller Mitglieder. Bei Datentreuhandgesellschaften hingegen verbleiben alle Rechte bei der Einzelperson. Datentreuhandgesellschaften sind also eine Art von „Daten-Tresoren“, in denen einzelne Personen ihre Daten hinterlegen, die dann von Treuhänderinnen und Treuhändern in ihrem Namen verwaltet werden. Während also Daten-Genossenschaften und Daten-*Commons* als eine Form der kollektiven Kontrolle über Daten angesehen werden können, dienen Datentreuhandgesellschaften dem Zweck, individuellen Nutzen zu maximieren. Sie behandeln Daten nicht als gemeinsames (moralisches oder

sogar rechtliches) Eigentum, sondern als individuelles Vermögen. Daher gehören Datentreuhandgesellschaften nicht zu den politischen Instrumenten, die von der Datensolidarität gefördert werden, es sei denn, sie setzen dieselben solidarischen Grundsätze durch wie die Daten-*Commons*.

Ein Beispiel für Datentreuhandgesellschaften, die sich dem öffentlichen Nutzen verschrieben haben, sind so genannte vertrauenswürdige Forschungsumgebungen (*Trusted Research Environments [TRE]*), die Forscherinnen und Forschern den Zugriff auf und die Analyse von sensiblen Daten unter Wahrung der Privatsphäre und Einhaltung ethischer Standards ermöglichen. In diesen Umgebungen werden strenge Zugangskontrollen, Datenanonymisierungstechniken und Prüfmechanismen eingesetzt, um die Daten einzelner Personen vor Missbrauch zu schützen. Durch die Förderung von Transparenz und Rechenschaftspflicht schaffen *TREs* Vertrauen bei den Betroffenen und erleichtern gleichzeitig die verantwortungsvolle Nutzung von Daten zum Nutzen der Wissenschaft und der Öffentlichkeit.

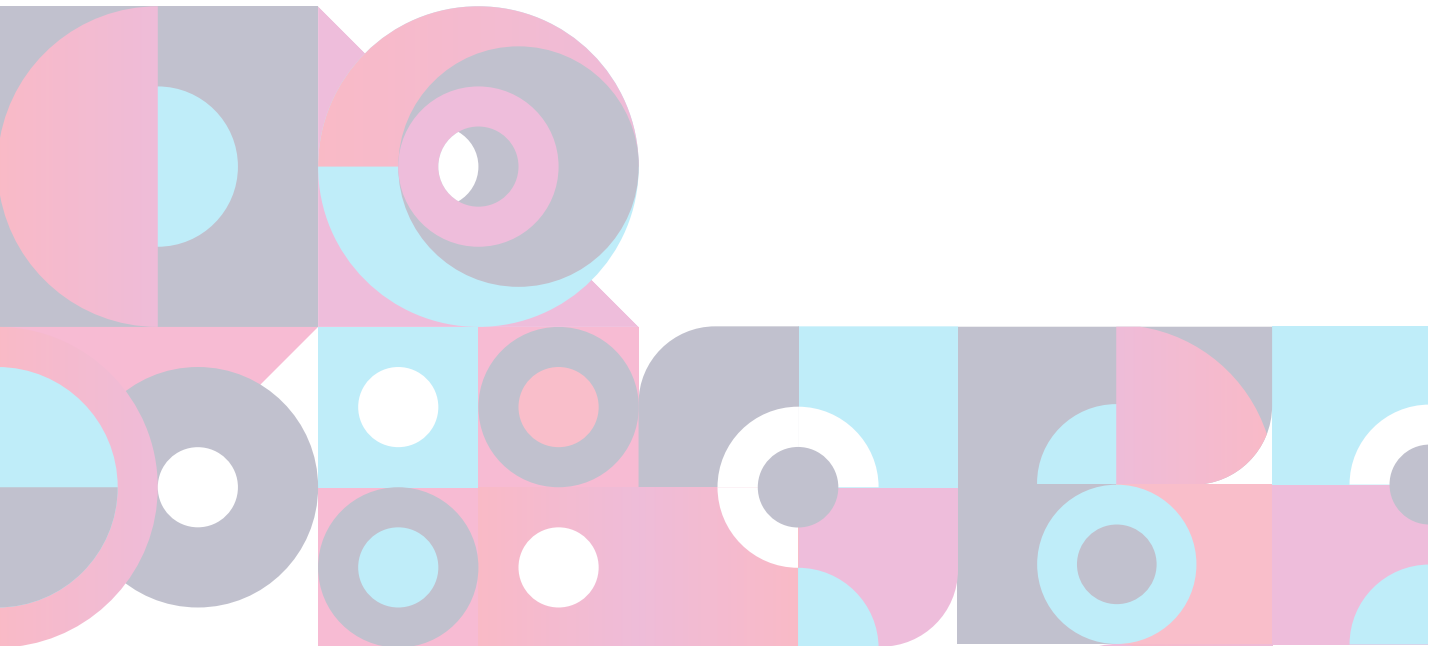
Referenzen: Hardinges et al., 2019; Delacroix & Lawrence, 2019; Element AI & Nesta, 2019; Hill, 2023; Linstedt & Olschimke, 2015; McDonald, 2019; Micheli et al., 2023; Paprica et al., 2023.

3.4 Das Teilen von Daten *(Data Sharing)*

Die Palette von Aktivitäten, die unter dem Schlagwort „Daten-Teilen“ zusammengefasst wird, ist sehr breit: Sie reicht von Forschungseinrichtungen, die Forschungsergebnisse mit anderen teilen, bis hin zu Nutzerinnen und Nutzern von sozialen Medien, die durch die Nutzung einer Plattform ihre Daten den Betreibern – wie *TikTok* oder *Facebook* – zur Verfügung stellen. Sie umfasst also sowohl das Kopieren von Daten als auch den Zugang zu den Quelldaten, ohne eine Kopie zu erstellen. Diese sehr breite Definition des Daten-Teilens macht es also unmöglich, zwischen Fällen gemeinnütziger Datennutzung und der Nutzung zum Zweck kommerzieller Profiterzielung zu unterscheiden. Für die Datensolidarität hingegen ist diese Unterscheidung von entscheidender Bedeutung.

Datensolidarität wird manchmal mit der Befürwortung des Teilens von Daten verwechselt, was nicht korrekt ist. Das Teilen von Daten ist, wie hier ausgeführt wurde, ein sehr allgemeiner Begriff, der die Bereitstellung von Daten für Dritte beschreibt, unabhängig davon, zu welchem Zweck und zu wessen Nutzen die Daten verwendet werden. Datensolidarität hingegen zielt darauf ab, die Schäden und Vorteile, die sich aus digitalen Praktiken ergeben, gerechter zu verteilen. Während also einige Fälle des Datenteilens Ausdruck oder Ergebnis von Datensolidarität sein können, sind andere dies *nicht*. Zuweilen kann sich Datensolidarität sogar darin äußern, dass Daten bestimmten Firmen oder Einrichtungen nicht zur Verfügung gestellt werden sollen – nämlich dann, wenn die Nutzung durch diese Firmen oder Einrichtungen keinen öffentlichen Wert schafft (siehe **Öffentlicher Wert *[Public Value]***). Datensolidarität kann auch darin zum Ausdruck kommen, dass bestimmte Aspekte menschlicher Gesundheit oder menschlichen Verhaltens gar nicht erst in Daten erfasst werden sollten.

Referenzen: Jussen et al., 2023; Longo & Drazen, 2016; Prainsack et al., 2022b.



3.5 Daten-Altruismus

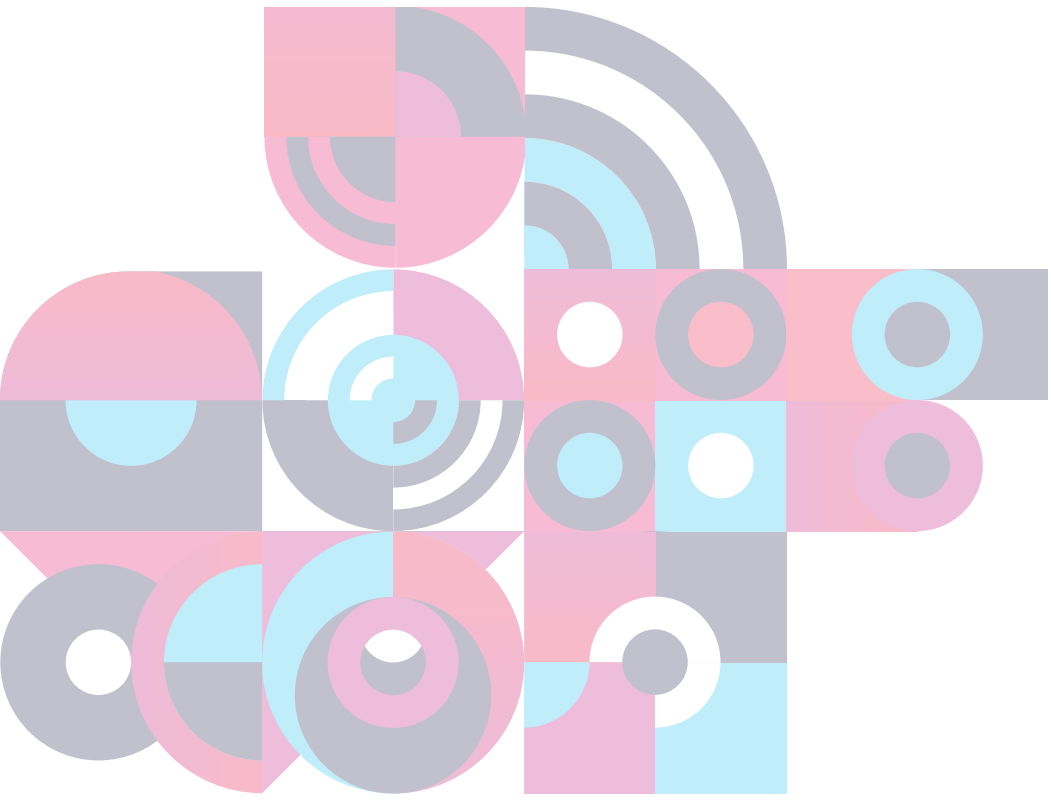
Daten-Altruismus ist ein zentrales Element der Daten-*Governance* Verordnung (*Data Governance Act [DGA]*), die am 30. Mai 2022 von der Europäischen Union verabschiedet wurde. Diese Verordnung zielt darauf ab, einen Rahmen für die Datenverwaltung in der EU zu schaffen, der sich auf die sichere Wiederverwendung von Daten des öffentlichen Sektors konzentriert und durch die Förderung der gemeinsamen Nutzung von Daten und den Abbau von Hindernissen für die Datenverfügbarkeit faire Wettbewerbsbedingungen in der Datenwirtschaft schafft. In dieser Verordnung bezieht sich Datenaltruismus auf jene Daten, die von Einzelpersonen oder Unternehmen freiwillig für das Gemeinwohl zur Verfügung gestellt werden (Kapitel IV der Verordnung). In diesem Kapitel wird detailliert beschrieben, wie Einzelpersonen und Unternehmen freiwillig Daten für das Gemeinwohl zur Verfügung stellen können, und es werden Mechanismen für Organisationen eingeführt, die solche Aktivitäten durchführen, um sich als in der EU anerkannte Datenaltruismus-Organisationen zu registrieren. Um dies zu tun, muss eine Organisation auf gemeinnütziger Basis arbeiten und unabhängig von jeder Einrichtung sein, die auf gewinnorientierter Basis arbeitet. Außerdem muss sie sicherstellen können, dass ihre Aktivitäten im Zusammenhang mit dem Daten-Altruismus über eine rechtlich unabhängige Struktur erfolgen, die von anderen Aktivitäten, die sie durchgeführt hat, getrennt ist.

Die Sichtweise der Europäischen Kommission in Bezug auf Datenaltruismus scheint auf bestimmten Annahmen darüber zu beruhen, wie Menschen motiviert werden können, ihre Daten „kostenlos“ zur Verfügung zu stellen. Es bleibt abzuwarten, ob der zusätzliche Gewinn der „zertifizierten Vertrauenswürdigkeit“ registrierter Altruismus-Organisationen und die Vorlagen für Einwilligungsformulare ausreichende Anreize für die gemeinsame Nutzung von Daten schaffen werden.

Abgesehen vom spezifischen Kontext der EU-Verordnung gibt es in der breiteren juristischen, politischen und ethischen Literatur kein gemeinsames Verständnis dessen, was Datenaltruismus bedeutet. Einige Autorinnen und Autoren verwenden den Begriff als Überbegriff für eine Reihe von Werten und Praktiken, die eng mit den Konzepten der Datenspende (siehe **Datenspende**) und dem Datenteilen verbunden sind. Aus der Perspektive der Datensolidarität ist der Begriff des Altruismus in mehrfacher Hinsicht problematisch: Erstens, weil er davon ausgeht, dass Menschen ihre Rechte an den Daten, die sie teilen, aufgeben sollten, was insbesondere im Zusammenhang mit Gesundheitsdaten keinen Sinn ergibt; nur wenige Menschen würden ernsthaft argumentieren, dass Patientinnen und Patienten, die ihre Gesundheitsdaten teilen, kein Recht mehr auf die Kontrolle dieser Daten haben sollten. Der Begriff der Solidarität, der eine dauerhafte Beziehung zwischen den Menschen von denen die Daten kommen und den Organisationen und Unternehmen, die die Daten nutzen, betont, scheint in dieser Hinsicht passender zu sein. Ein weiteres Problem mit Datenaltruismus besteht darin, dass ganze Institutionen das Gütesiegel als „altruistische Organisationen“ erhalten können. Ein solch pauschaler Ansatz

verkennt die notwendigen Nuancen, die mit den verschiedenen Arten der Datennutzung einhergehen, unabhängig davon, wer die Daten nutzt – so können auch gemeinnützige Organisationen Daten auf riskante oder anderweitig problematische Weise nutzen, oder kommerzielle Firmen mit Datennutzung öffentlichen Wert schaffen. Aus diesem Grund bindet die Datensolidarität regulatorische Konsequenzen an verschiedene Arten der Datennutzung, die auf einer Bewertung des öffentlichen Werts beruhen, wobei auch berücksichtigt wird, für welche Gruppen diese Risiken und Vorteile am wahrscheinlichsten eintreten.

Referenzen: Kraut, 2020; Prainsack et al., 2022b; European Commission, 2020; European Parliament & Council of the European Union, 2022; Raj et al., 2020; TEHDAS, 2021.



3.6 Datenspende

Die juristischen Definitionen des Begriffs der Spende, die auf das antike römische Recht zurückgehen, konzentrieren sich darauf, dass der Eigentümer einer Sache diese einer anderen Person oder Einrichtung übergibt, ohne eine Gegenleistung zu erwarten. Der letztgenannte Aspekt – dass etwas gegeben wird, ohne eine Gegenleistung zu verlangen oder gar zu erwarten – sagt uns zwei Dinge über Spenden. Erstens, dass mit einer Übertragung kein wirtschaftliches Gewinnmotiv verbunden ist. Zweitens sind Spenden nicht auf direkte und lineare Weise reziprok (gegenseitig) – auch wenn sie, wie andere Geschenke, in Netzwerke gegenseitiger moralischer und sozialer Verpflichtungen eingebettet sind. Stattdessen beruhen Spenden auf *indirekter* Gegenseitigkeit. Darüber hinaus sind Spenden rivalisierend und verbrauchbar: Wenn jemand einem Krankenhaus Geld spendet, kann sie dasselbe Geld nicht der Katastrophenhilfe spenden. Wenn jemand einer Person eine Niere spendet, kann sie dieselbe Niere nicht einer anderen Person geben. Traditionell haben Spenden zur Folge, dass es eine verbrauchbare Sache gibt, die von einer Einheit auf eine andere übertragen wird.

Es stellt sich die Frage, ob dies auch für digitale Daten, insbesondere Gesundheitsdaten, gelten kann. In Anbetracht der Tatsache, dass sich digitale Daten an mehr als einem Ort gleichzeitig befinden können und dass sie oft Spuren hinterlassen, selbst wenn sie „gelöscht“ werden, stellt sich die Frage, wo eine Spende beginnt und endet. Werden alle Kopien eines Datensatzes gespendet oder kann eine Kopie von der ursprünglichen betroffenen Person behalten werden? Das Konzept der Datenspende ist besonders verwirrend, wenn es in einem Kontext verwendet wird, in dem Menschen anderen etwas geben, zu dem sie weiterhin Zugang haben – beispielsweise, wenn eine Person die Verwendung von Daten aus einer Gesundheits-App zu Forschungszwecken gestattet.

Aus diesen Gründen vermeidet der Ansatz der Datensolidarität den Begriff der Spende im Zusammenhang mit Daten. Das Konzept der Datenspende kann jedoch sehr hilfreich sein, wenn es um die Frage geht, was mit den Daten einer Person nach deren Tod geschieht. In den meisten Staaten sind Daten verstorbener Personen weitgehend ungeregelt. Die Datenspende könnte eine Möglichkeit für Menschen sein, über das Schicksal ihrer Daten zu entscheiden, solange sie noch am Leben sind.

Soweit Autorinnen und Autoren oder politische Entscheidungsträgerinnen und Entscheidungsträger den Begriff Datenspende verwenden, hängt es von der Motivation der Person, die die Daten zur Verfügung stellt, sowie von den Zwecken und Kontexten ab, für die die Daten verwendet werden, ob ein bestimmter Fall von Datenspende als solidarische Form des Daten-Teilens gesehen werden kann.

Referenzen: Carrier, 1991; Krutzinna & Floridi, 2019; Prainsack, 2019a; Prainsack et al., 2022b.

3.7 Offene Daten *(Open Data)* / Offene Wissenschaft *(Open Science)*

Offene Daten sind alle Daten, die frei zugänglich sind und von jedermann ohne Einschränkungen (wieder-)verwendet und geteilt werden können. Die *Open-Data*-Bewegung entwickelt sich seit Jahrzehnten und hat nach und nach auch Regularien auf nationaler, europäischer und internationaler Ebene beeinflusst. Das Hauptaugenmerk liegt dabei auf der Erleichterung des Zugangs zu Daten in einem maschinenlesbaren Format. Zu diesem Zweck werden in vielen Staaten *Open-Data*-Portale und Anwendungsprogrammierschnittstellen *(Application Programming Interfaces [APIs])* entwickelt, die es Unternehmen oder Forscherinnen und Forschern ermöglichen, auf öffentliche Datensätze zuzugreifen und diese für Produktentwicklung, für die Forschung, oder für andere Zwecke zu verwenden. Eine solche „Öffnung" von Daten wird auch als Motor zur Weiterentwicklung von Wissenschaft, Technologie, Innovation und Wirtschaft betrachtet. In diesem Zusammenhang wurde *Open Data* auch von den Vereinten Nationen als eine Initiative anerkannt, die wesentlich zur Erreichung der Ziele für nachhaltige Entwicklung beitragen kann.

Open Data ist nach wie vor eng mit *Open Science* verbunden. Letztere vereint verschiedene Konzepte, Bewegungen und Praktiken, die darauf abzielen, wissenschaftliche Erkenntnisse offen und für jedermann zugänglich zu machen. Offenheit bezieht sich in erster Linie auf das Fehlen von Bezahlschranken, aber auch auf informelle Barrieren im Zusammenhang mit der Auffindbarkeit von Daten, mit digitalen Fähigkeiten und anderen Ressourcen. Was offen zugänglich gemacht werden soll, sind vor allem die Mittel und Ergebnisse der Wissensproduktion, insbesondere wissenschaftliche Daten und Veröffentlichungen. In manchen Fällen werden auch Algorithmen, Quellcodes, Software und Arbeitsabläufe „geöffnet" und damit allen zugänglich gemacht.

Der Begriff der offenen Wissenschaft ist auch eng mit der *Open-Source*-Bewegung verbunden. *Open Source* bezieht sich auf jedes Programm, dessen Quellcode der Allgemeinheit zur Nutzung oder Änderung zur Verfügung gestellt wird. In anderen Worten: es handelt sich um Software, die nicht nur einer Person oder einem Unternehmen, sondern der Allgemeinheit gehört.

Insbesondere im Hinblick auf die Erleichterung der Datennutzung, die einen bedeutenden öffentlichen Wert schafft, haben die *Open-Data-*, *Open-Science-* und *Open-Source*-Bewegungen wichtige Ziele mit der Datensolidarität gemeinsam. Gleichzeitig ist Offenheit kein Selbstzweck. Insbesondere in Fällen, in denen Offenheit auf formale Gleichheit beim Zugang abzielt, führt dies oft dazu, dass wirtschaftlich mächtigere Akteure die offen verfügbaren Ressourcen besser nutzen können als andere. Dies vergrößert die Ungleichheiten, anstatt sie zu verringern. Wenn *Open Science* nicht in den Dienst anderer Ziele wie mehr Gleichheit oder Gerechtigkeit gestellt wird, läuft sie Gefahr, lediglich kosmetische Wirkungen zu haben und sogar zur Verschärfung der Kluft zwischen Forscherinnen und Forschern und Öffentlichkeit in ressourcenreichen und ressourcenarmen Kontexten beizutragen.

Referenzen: Bezuidenhout et al., 2017; Kitchin, 2014; Levin et al., 2016; Nerlich et al., 2018; Szoszkiewicz, 2021; World Health Organization, 2020.

3.8 Europäischer Gesundheitsdatenraum *(EHDS)*

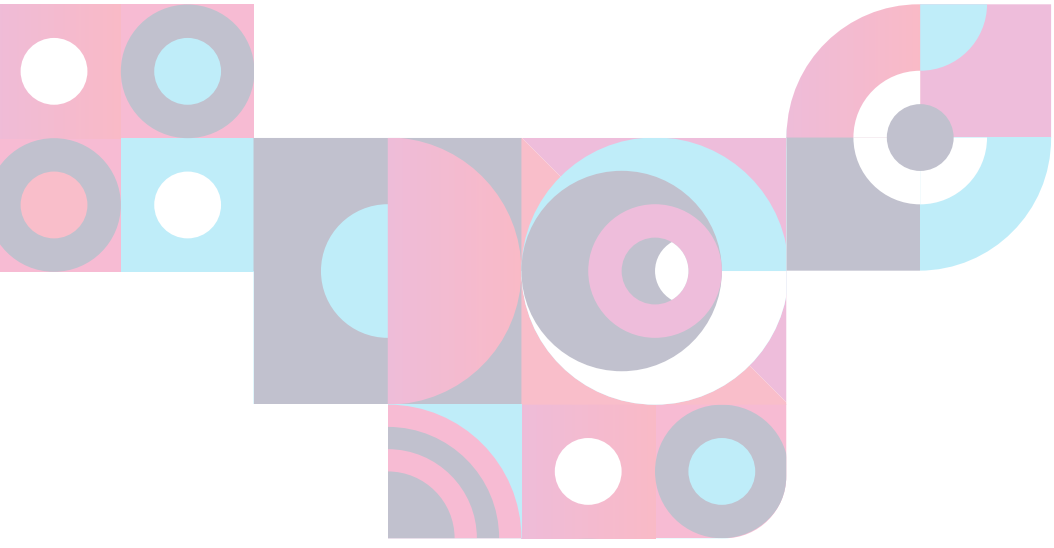
Der Europäische Gesundheitsdatenraum (*European Health Data Space [EHDS]*) ist eine Initiative der Europäischen Union, die darauf abzielt, die Zugänglichkeit, Interoperabilität und gemeinsame Nutzung von Gesundheitsdaten in den Mitgliedstaaten zu verbessern. Ein erster Entwurf wurde im Mai 2022 veröffentlicht und in verschiedenen EU-Institutionen intensiv diskutiert. Im März 2024 erzielten das Europäische Parlament, der Rat und die Europäische Kommission eine politische Einigung über den *EHDS*. Die formelle Annahme der Verordnung durch das Europäische Parlament erfolgte im April 2024. Seit 26. März 2025 ist er offiziell in Kraft getreten.

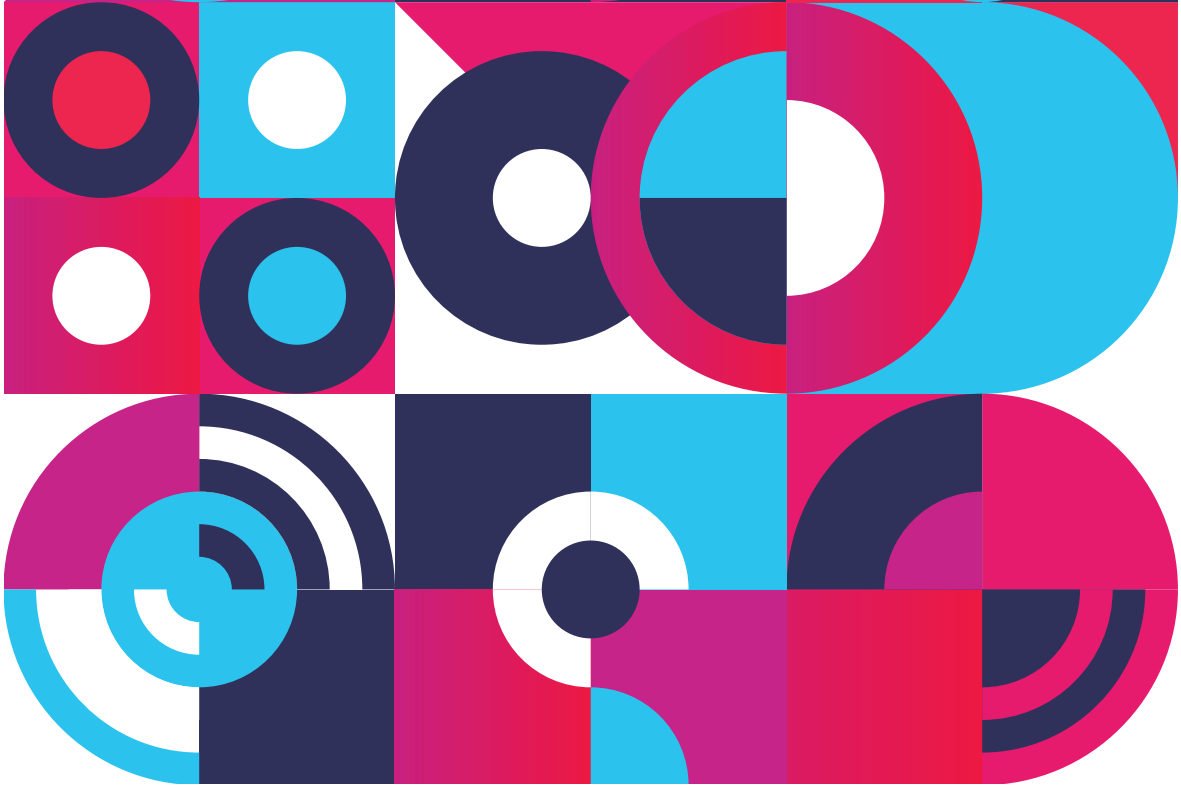
Mit dem *EHDS* sollen Gesundheitsversorgung, Forschung und Innovation durch bessere Nutzung der Daten verbessert und gleichzeitig Datenschutz innerhalb der EU-Mitgliedstaaten gewährleistet werden. Ziel ist die Schaffung eines gemeinsamen Rahmens und einer gemeinsamen Infrastruktur für den sicheren Austausch von Gesundheitsdaten, einschließlich elektronischer Patientenakten, genomischer Daten sowie Daten aus Gesundheitssystemen, Forschungseinrichtungen und anderen Quellen. Durch einen möglichst nahtlosen Austausch von Gesundheitsdaten soll der *EHDS* eine effektivere Planung der Gesundheitsversorgung, personalisierte Medizin und Gesundheitsforschungsinitiativen unterstützen und letztlich zu besseren Gesundheitsergebnissen für die europäischen Bürgerinnen und Bürger beitragen.

Kritikerinnen und Kritiker haben Bedenken hinsichtlich der potenziellen Risiken für die Privatsphäre einzelner Patientinnen und Patienten geäußert, insbesondere im Hinblick auf die zentrale Speicherung und den Austausch sensibler Informationen. Auch die Gewährleistung der Interoperabilität der verschiedenen Gesundheitsdatensysteme in den einzelnen Mitgliedstaaten stellt weiterhin eine Herausforderung dar, da einzelne Mitgliedstaaten weiterhin unterschiedliche Standards und Protokolle für den Datenaustausch haben dürfen. Darüber hinaus wurden Fragen zur *Governance*-Struktur des *EHDS* und zur Einbeziehung von Interessengruppen, einschließlich Patientinnen und Patienten, Ärztinnen und Ärzten und anderen Gesundheitsberufen in Entscheidungsprozesse aufgeworfen. Es wurde argumentiert, dass mehr Transparenz und Rechenschaftspflicht gegenüber der Öffentlichkeit erforderlich sind, um diese Bedenken auszuräumen und zu gewährleisten, dass der *EHDS* die Vorteile des Datenaustauschs mit dem Schutz der Rechte und Interessen der und des Einzelnen effektiv in Einklang bringt. Auch der Begriff des Datenaltruismus innerhalb des *EHDS* wurde als problematisch kritisiert (siehe **Datenaltruismus**).

Aus der Perspektive der Datensolidarität gibt es verschiedene Probleme mit dem *EHDS*-Vorschlag, darunter die starke Verwendung des Begriffs Altruismus: Im Gegensatz zur Solidarität, die ein relationales Konzept ist, das die gegenseitigen Bedürfnisse und Verantwortlichkeiten zwischen verschiedenen Akteuren betont, könnte der Altruismus den Eindruck erwecken, dass diejenigen, die Daten weitergeben, dies aus rein selbstlosen Gründen tun und bereit sein sollen, jegliche Kontrolle über ihre eigenen Daten aufzugeben. Darüber hinaus gibt es Bedenken, dass die Bestimmungen des *EHDS* großen Unternehmen einen noch leichteren Zugang zu Daten verschaffen und damit die Asymmetrie in Bezug auf Macht und Einfluss zwischen größeren und kleineren Unternehmen bzw. gemeinnützigen Organisationen in der Datenwirtschaft verstärken könnten.

Referenzen: European Commission, 2025; Marelli et al., 2023; Shabani, 2022.





Section 4: Ethik und Macht

4.1 Digitale Ethik und Datenethik

Digitale Ethik und Datenethik (einschließlich ethischer KI – Künstliche Intelligenz) sind wichtige Ergänzungen zur Datensolidarität. Die Digitale und die Datenethik konzentrieren sich beide auf die moralischen Verpflichtungen, die alle gesellschaftlichen Akteurinnen und Akteure haben (oder haben sollten), wenn sie strukturierte und unstrukturierte Daten sowie von Menschen bereitgestellte Daten sammeln, erzeugen, analysieren und verbreiten. Dies schließt auch die Nutzung bestehender Datenbanken sowie Entscheidungen ein, die durch KI in Bezug auf Daten im Allgemeinen und personenbezogene Daten im Besonderen getroffen werden. Sowohl Digitale Ethik als auch Datenethik beziehen sich auf die allgemeinen Grundsätze, auf denen unsere Gesellschaften aufgebaut sind, und ist von großer Bedeutung für die Schaffung von Vertrauen und die Gewährleistung von Fairness.

Die Digitalisierung des Gesundheitswesens wirft spezifische Fragen und Bedenken in Bezug auf Datennutzung, Sicherheit und Souveränität auf. Im Gesundheitsbereich ist es angesichts der raschen Entwicklung der Datafizierung (siehe **Datafizierung („Verdatung“) der Gesundheit**) und Digitalisierung besonders wichtig, einen vertrauenswürdigen Rahmen für die Datennutzung zu schaffen. Es ist von entscheidender Bedeutung, die Entwicklung der digitalen Gesundheit mit humanistischen und ethischen Werten zu untermauern, sie konkret umzusetzen und den Bürgerinnen und Bürgern die erzielten Fortschritte auf transparente Weise zu vermitteln.

Einige, insbesondere kommerzielle Akteure, nutzen Daten auf unethische Weise. So geben beispielsweise manche digitalen Plattformen die von ihren Nutzerinnen und Nutzern generierten Daten an Dritte weiter; ihr Geschäftsmodell basiert auf dem Verkauf dieser Daten, die nicht nur Informationen über einzelne Personen, sondern auch über deren Freundinnen und Freunde und soziale Netzwerke beinhalten. Zudem diskriminieren manche Algorithmen auf digitalen Plattformen oder anderen Onlinedienstleistern spezifische Personengruppen in unserer Gesellschaft. Insbesondere ist festzustellen, dass viele Akteure nachlässig in der Einhaltung von Verfahrensvorschriften sind.

Datenethische Richtlinien enthalten in der Regel einen Verweis auf ethische Grundsätze, zu denen unter anderem Transparenz, Fairness, Verantwortung, Selbstbestimmung und Datenschutz gehören. Staatliche Risikobehörden – wie *NIST*, die US-Organisation für Technologiestandards, und *DataEthics.eu* – haben Leitlinien für die praktische Anwendung unter Berücksichtigung potenzieller Schäden für Menschen, Organisationen und Systeme bereitgestellt. Ein wichtiger Schritt ist die Einführung interner Überprüfungsprozesse und -gremien zur Überwachung der ethischen Datenverwaltung. Um Daten ethisch zu nutzen, sollten Unternehmen, Behörden, und andere Organisationen über den Datenschutz hinaus unter anderem folgende Punkte berücksichtigen: die Herkunft der Daten, den Verwendungszweck, den Schutz der Daten, den Schutz der Privatsphäre der Datensubjekte (d. h. der Personen, von denen die Daten kommen) und die Aufbereitung der Daten für die Nutzung. Es ist notwendig, von politischen Diskussionen zu praktischen Lösungen überzugehen, die diese Grundsätze in die Praxis integrieren.

Für die Datensolidarität sind die Digitale Ethik und die Datenethik insofern von zentraler Bedeutung, als sie unterstreichen, dass es bei der Regulierung digitaler Technologien nicht nur um den Schutz der Privatsphäre oder die Sicherheit von Daten geht. Es geht auch darum, Bürgerinnen und Bürger, Kunden und Nutzer vor Datenpraktiken zu schützen, die sich nachteilig auf die Menschen und die Gesellschaft auswirken.

Referenzen: Cepelak, 2023; Ministère de la Santé et de la Prévention, 2022; Segalla & Rouziès, 2023; Viberg Johansson et al., 2022.

4.2 Digitaler Humanismus

Beeinflusst durch den historischen Begriff des Humanismus während der Renaissance und der Aufklärung wird dieser heute oft als Leitprinzip für menschliche Interaktion angesehen. Im Kontext digitaler Praktiken wird der Begriff des Humanismus mitunter auch auf die Interaktion zwischen Mensch und Maschine angewandt, um den Primat menschlichen Wohlergehens hochzuhalten und Werte wie Privatsphäre, Würde oder Solidarität zu betonen.

Wissenschaftlerinnen und Wissenschaftler sowie Praktikerinnen und Praktiker auf dem Gebiet des digitalen Humanismus beschäftigen sich mit Fragen wie diesen: Wie werden Gesetze und Regelwerte im Geiste humanistischer Werte entwickelt? Wie können diese im öffentlichen und privaten Sektor umgesetzt werden? Welche Anforderungen müssen beispielsweise für die Anwendung algorithmischer Entscheidungsfindung gestellt werden, um zu vermeiden, dass das Streben nach technologischer Effizienz und wirtschaftlichem Wachstum die Rechte und das Wohlbefinden von Menschen beeinträchtigt?

Ein Beispiel ist das Wiener Manifest zum digitalen Humanismus (2019). Dieses Dokument, zu dem Wissenschaftlerinnen und Wissenschaftlerinnen sowie Praktikerinnen und Praktiker aus unterschiedlichen Disziplinen beigetragen haben, definiert digitalen Humanismus als die Verknüpfung humanistischer Ideale mit kritischen Überlegungen zum technologischen Fortschritt. Es definiert ihn als interdisziplinären Ansatz zum Verständnis und zur Gestaltung des Zusammenspiels von Technologie und Mensch für eine bessere Gesellschaft.

Die Perspektive des digitalen Humanismus stellt auch einige gängige Annahmen in Frage, wie z. B. die Vorstellung, dass automatisierte Systeme die mathematischen und analytischen Fähigkeiten des Menschen übertreffen. Der digitale Humanismus wendet sich gegen ein solches Verständnis einer vermeintlich „autarken“ technologischen Entwicklung. Der digitale Humanismus betont zudem die ausschließliche Fähigkeit des Menschen, den Zweck computergestützter Tätigkeiten zu bestimmen, indem er die Prämissen und Werte, die in ihnen zur Anwendung kommen, formt. Politische Entscheidungsträgerinnen und Entscheidungsträger sollten sich auf die Möglichkeiten konzentrieren, die die digitalen Technologien zur Verbesserung der menschlichen Lebensbedingungen bieten. Mit anderen Worten: Der digitale Humanismus lehnt datengesteuerte Praktiken nicht ab, sondern möchte, dass diese – wie alle digitalen Praktiken – im Dienste der Menschen eingesetzt werden.

Die Datensolidarität hat zwar viele Gemeinsamkeiten mit dem digitalen Humanismus, ist aber in Bezug auf die wesentlichen Werte, auf die sie sich stützt, nicht auf den Humanismus beschränkt. Sie orientiert sich an einem breiteren Spektrum von Werten wie Gleichheit, Gerechtigkeit und natürlich Solidarität.

Referenzen: Autili et al., 2019; Coeckelbergh, 2024; Mittelstadt et al., 2016; Neidhardt et al., 2022; Nida-Rümelin, 2022; Nowotny, 2022; Prainsack et al., 2022b; Werthner et al., 2019; Werthner et al., 2022.

4.3 Datenbasierte Diskriminierung

Die Diskriminierung von Individuen oder Gruppen auf der Basis digitaler Daten (datenbasierte Diskriminierung) ist einer der Schäden in der digitalen Gesellschaft, den die Datensolidarität verhindern will. Angesichts der enormen Datenmengen, die täglich generiert und verarbeitet werden, werden immer mehr Entscheidungen – auch im Gesundheits- und Pflegebereich – von Datenanalysen und Algorithmen mitbestimmt. Diese Situation dringt durch den Einsatz generativer KI (Künstliche Intelligenz) in immer weitere Bereiche des privaten und öffentlichen Lebens vor. Trotz der oft behaupteten Neutralität der Technologie können KI-Systeme diskriminierende Auswirkungen haben, wenn sie zur Entscheidungsfindung eingesetzt werden. In Europa unterstreicht die Allgemeine Datenschutzgrundverordnung (DSGVO) die Notwendigkeit, Diskriminierung infolge automatisierter Entscheidungsfindung zu verhindern, und gibt den Menschen ein Recht auf aussagekräftige Informationen über die Logik, die automatisierten Entscheidungen zugrunde liegt.

Datenbasierte Diskriminierung liegt vor, wenn Einzelpersonen oder Gruppen aufgrund von Merkmalen oder Eigenschaften, die durch die Sammlung und Analyse ihrer Daten ermittelt wurden, ungerecht behandelt werden. Die Diskriminierung kann sich aus den Datenquellen ergeben, die zum Trainieren von KI-Systemen verwendet werden, sowie aus der Art und Weise, wie die Systeme genutzt werden und wie sie konzipiert wurden. Dies kann dazu führen, dass soziale Ungleichheiten fortbestehen und neue Diskriminierungsmuster im Gesundheitssystem entstehen, z. B. in Bezug auf Alter, Geschlecht, ethnische Zugehörigkeit, Religion, sexuelle Orientierung oder genetische Merkmale. Bedenken in Bezug auf Ethik, Fairness, Gerechtigkeit und Transparenz bei der Nutzung großer Datensätze müssen ausgeräumt werden. Dies geschieht am besten durch die Einbeziehung von und offene Kommunikation mit allen Beteiligten. Im Bereich des Gesundheitswesens steht besonders viel auf dem Spiel, da das Leben und die Gesundheit von marginalisierten und unterversorgten Gruppen gefährdet sein könnten.

Strukturelle Ungleichheiten, Vorurteile und Rassismus in der Gesellschaft schreiben sich häufig in Datensätzen weiter fort. Wenn etwa bestimmte Gruppen in einer Gesellschaft keinen Zugang zu bestimmten medizinischen Vorsorgeuntersuchungen

haben, dann sind ihre Daten auch in den Datensätzen in diesem Bereich nicht abgebildet. Analysen dieser Daten sind dann nur auf jene Menschen anwendbar, die bereits privilegiert genug sind, Zugang zu einer weiten Bandbreite medizinischer Versorgung zu haben.

Wenn auf diese Weise „verzerrte" Datensätze zum Trainieren von Software verwendet werden, wird die systematische Verzerrung noch verstärkt. Daher ist es besonders wichtig, bei Datensätzen zum Trainieren von Software die Frage zu stellen, wer in diesen Datensätzen fehlt. Wer ist über- und wer ist unterrepräsentiert? So kann das Risiko minimiert werden, dass Software oder andere Anwendungen, die aus den Datenanalysen stammen, bestimmte Personen oder Gruppen ungerechtfertigterweise diskriminieren. Die KI-Verordnung *(AI Act)* der Europäischen Union enthält in Artikel 10 Absatz 5 eine Bestimmung, die es Organisationen unter bestimmten Bedingungen ermöglicht, besondere Kategorien personenbezogener Daten zu verarbeiten, um ihre KI-Systeme auf Diskriminierung zu überprüfen und diese zu korrigieren.

Datensolidarität arbeitet unter anderem auf das Ziel hin, datenbasierte Diskriminierung zu bekämpfen. Im weiteren Sinne soll sie sicherstellen, dass alle Schäden – nicht nur Diskriminierung – und alle Vorteile innerhalb und zwischen Gesellschaften gerechter verteilt werden.

Referenzen: Ibrahim et al., 2020; Knight, 2021; Pot et al., 2021; Wójcik, 2022.

4.4 Datenextraktion

Unter Datenextraktion versteht man das Sammeln oder Abrufen unterschiedlicher Arten von Daten aus einer Vielzahl von Quellen, und deren anschließende analytische Verarbeitung für bestimmte Zwecke, z. B. Marketing. Dies wird als *„Web Scraping“* bezeichnet. Zu den Datenquellen gehören Daten von der Nutzung digitaler Plattformen und sozialer Medien, aber auch die Nutzung von Websites, Gesundheits-Apps, oder Information über die Aufenthaltsorte von Nutzerinnen und Nutzern portabler digitaler Geräte wie Smartphones (Geolokation). Bei der Datenextraktion für die Forschung geht es darum, relevante Daten aus verschiedenen Quellen zusammenzuführen, um sie zu analysieren, zu interpretieren und Schlussfolgerungen zu ziehen.

Die Extraktion von Mustern aus großen Mengen unstrukturierter Daten wird als *„Data Mining“* oder „Datenanalyse“ bezeichnet. Dies geschieht heute zunehmend mit Hilfe maschinellen Lernens und anderen Formen künstlicher Intelligenz. Im Gesundheitswesen spielt die Datenextraktion eine immer wichtigere Rolle in der medizinischen Forschung und auch in der Patientenversorgung. So stieg beispielsweise während der COVID-19-Pandemie der Bedarf an zuverlässigen Gesundheitsinformationen erheblich. Viele Gesundheitssysteme waren damals nicht in der Lage, den Fluss der erforderlichen Daten und Informationen zwischen Leistungserbringern und Gesundheitsbehörden zu gewährleisten, was die Erkennung von Mustern und deren Interpretation zur Gewinnung verwertbarer Erkenntnisse erschwerte. Die Datenextraktion bringt also viele Vorteile mit sich, birgt aber auch Risiken. Ein zentrales Ziel der Datensolidarität ist es, dafür zu sorgen, dass diese Vorteile und Risiken gerechter verteilt werden, als dies heute der Fall ist.

Wie bei allen Formen der Datennutzung wirft auch die Datenextraktion Fragen des Schutzes der Privatsphäre sowie ethische Fragen auf. Auf Datenextraktion basierende Forschung kann zur Diskriminierung von Personen oder Personengruppen führen oder auf andere Weise Schaden verursachen. Dies trifft nicht nur auf Datenextraktion für kommerzielle Nutzung zu, sondern auch für Nutzung durch Behören – wie etwa im niederländischen Beihilfenskandal. In diesem wurden Personen mit Migrationshintergrund fälschlicherweise beschuldigt, zu viele staatliche Beihilfen erhalten zu haben (siehe **Datafizierung („Verdatung“) der Gesundheit**). Die Aggregation und Kombination von Daten kann die Analyse erleichtern, aber auch die Identifizierung von Individuen ermöglichen, selbst wenn die Daten ursprünglich anonym waren, was zu Datenschutzverletzungen führen kann. Aggregation kann auch neue Formen der Ausbeutung mit sich bringen, wenn etwa Daten ohne Zustimmung oder sogar ohne das Wissen der Personen, von denen sie stammen, analysiert und zu Geld gemacht werden. Dies verschärft die Machtasymmetrien zwischen „normalen“ Bürgerinnen und Bürgern und datenverwertenden Unternehmen, weil letztere viel größere Möglichkeiten haben, wirtschaftlich von den Daten zu profitieren, und erstere fast das gesamte Risiko tragen.

Datensolidarität zielt darauf ab, die Risiken der Datenextraktion zu verringern. Sie will auch sicherstellen, dass die verbleibenden Risiken sowie die Vorteile, die sich aus der Extraktion, Nutzung und Wiederverwendung von Daten ergeben, innerhalb und zwischen unterschiedlichen Ländern gerecht verteilt werden.

Referenzen: Constantaras et al., 2023; Talend, ohne Datum; Taylor et al., 2021.

4.5 Datenkolonialismus

Der Datenkolonialismus zielt auf eine Entwicklung ab, die nicht mehr durch die Gewinnung von natürlichen Ressourcen oder Arbeitskräften definiert ist, sondern auf der Aneignung des menschlichen Lebens durch Daten beruht.

Das Konzept des Datenkolonialismus umfasst alle digitalen Praktiken, durch die Einzelpersonen und Gruppen (z. B. indigene Menschen und Gemeinschaften) durch die Gewinnung, Kontrolle und Nutzung ihrer Daten durch mächtigere private und öffentliche Akteure marginalisiert oder enteignet werden, sei es aus Profitgründen oder zum Zwecke der politischen Kontrolle. Dieser Prozess weist viele Gemeinsamkeiten mit der kolonialen Gewinnung von Ressourcen im Zusammenhang mit territorialen Eroberungen auf.

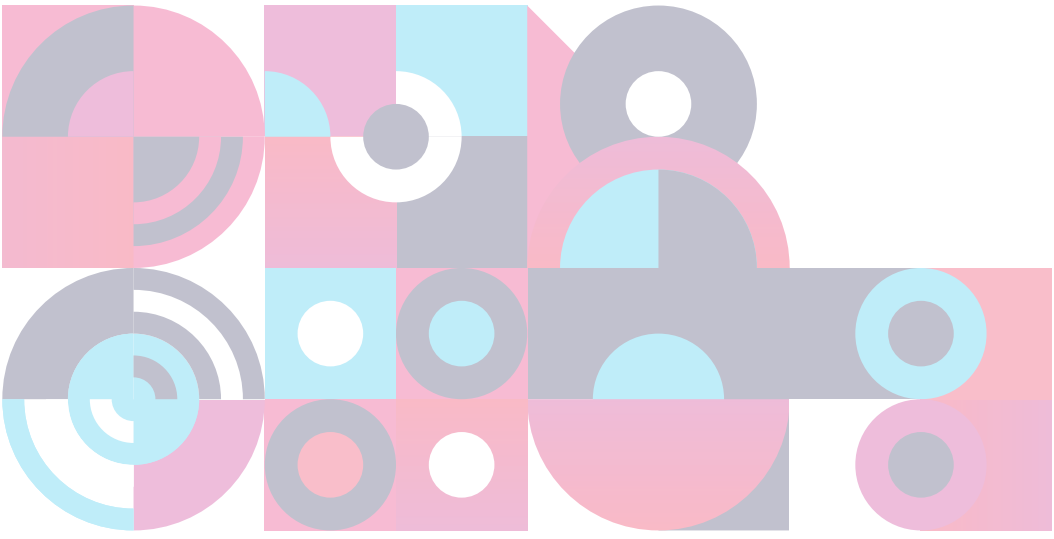
Datenkolonialismus wirkt auf vielen Ebenen. Er äußert sich unter anderem in Nutzungsbedingungen für digitale Plattformen und digitale Services, denen Menschen zustimmen müssen, wenn sie diese Services nutzen möchten, und mit denen sie häufig alle Rechte an den Daten aufgeben. Das dem Datenkolonialismus verwandte Konzept des Überwachungskapitalismus analysiert die Art und Weise, in der menschliche Verhaltensweisen, Körper und Umgebungen in eine Ressource verwandelt werden, die in Daten und in weiterer Folge in kommerzielle Gewinne umgewandelt wird. Generative KI – also Formen künstlicher Intelligenz, die Texte, Bilder, oder andere Inhalte generieren – kann Datenkolonialismus verstärken, indem sie Daten von den Urheberinnen und Urhebern von Inhalten ohne faire Entschädigung extrahiert, die Kontrolle und die Vorteile in den Händen einiger weniger konzentriert und damit bestehende Ungleichheiten vergrößert.

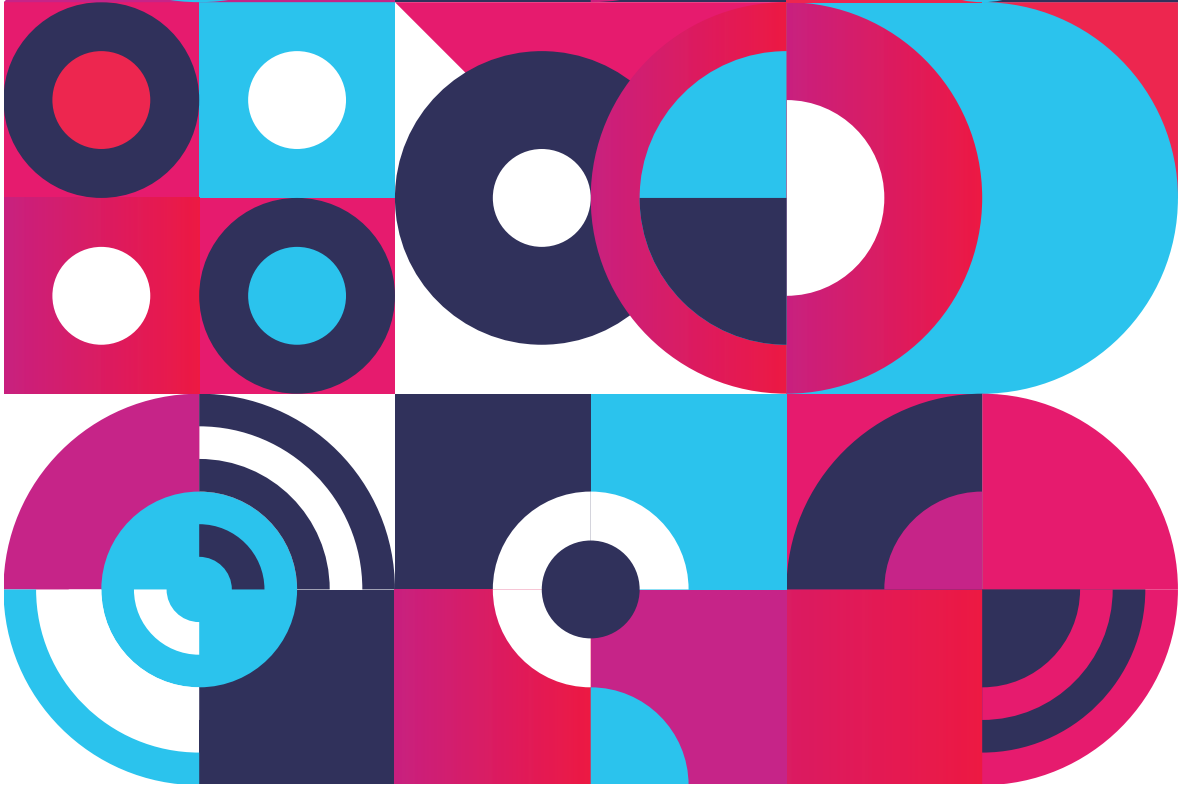
Ein weiterer extraktiver Prozess ist die globale Datenerfassung, die häufig keinen Regeln unterliegt und Daten aus vielen Ländern verarbeitet. Darauf hat die Rechtssetzung in den meisten Staaten noch keine gute Antwort gefunden. Daten bilden die Grundlage für die internationale Berichterstattung über Entwicklungsfortschritte, wie die Ziele für nachhaltige Entwicklung, und bestimmen die Zuweisung von Ressourcen. Die zunehmende Abhängigkeit von Daten aus diesen Prozessen für die Entscheidungsfindung verschärft das Problem des Datenkolonialismus: Phänomene und Faktoren, die nicht in Form von Daten gemessen und dargestellt werden können, sind für

politische Entscheidungsträgerinnen und Entscheidungsträger in der Folge unsichtbar.

Glaubwürdige und zuverlässige Daten sind für die globale Gesundheit besonders wichtig – nicht nur bei Krankheitsausbrüchen und Pandemien. Staaten und zwischenstaatliche Organisationen müssen volles Vertrauen in die Mechanismen der gemeinsamen Datennutzung haben können, insbesondere in den Wert, den diese, angesichts großer Ungleichheiten, für Länder mit niedrigem und mittlerem Einkommen bringen. Die Weltgesundheitsorganisation (WHO) hat vorgeschlagen, globale Gesundheitsdaten als öffentliches Gut zu behandeln, aber die Datensolidarität hat sich noch nicht als Konzept durchgesetzt. Im Zusammenhang mit globalen Berichterstattungspflichten wie dem *Global Burden of Disease Report (GBD)* wurden auch Bedenken geäußert, dass dadurch Macht von Institutionen in Ländern mit niedrigem Einkommen auf solche in Ländern mit hohem Einkommen übertragen wird, die Entwicklung nationaler Gesundheitsinformationssysteme behindert wird und bestimmte Formen von Wissen gegenüber anderen bevorzugt werden.

Referenzen: Birch, 2023; IHME, ohne Datum; Kim et al., 2017; Mitchell, 2021; Shiffman & Shawar, 2020; Universität Bern, 2021; Zuboff, 2019.





Abschnitt 5: Mit Blick auf die Zukunft

5.1 Die digitale Transformation des Gesundheitswesens

Digitale Technologien und KI (Künstliche Intelligenz) sind heute integrale Bestandteile des Gesundheitswesens. Im Jahr 2021 hat die *Lancet* und *Financial Times* Kommission einen dringenden Handlungsaufruf an die Entscheidungsträgerinnen und Entscheidungsträger in der Gesundheits- und Digitalpolitik gerichtet, um sicherzustellen, dass die digitale Transformation von öffentlichem Nutzen und nicht nur von privatem Profit motiviert ist. Das Ziel öffentlicher Gesundheit muss es sein, gute Gesundheitsversorgung für alle zu ermöglichen und zu verbessern. Die *Lancet* und *Financial Times* Kommissionschlug vor, den Begriff „digitale Gesundheit“ nur auf klar definierte Anwendungen in Gesundheit und Medizin anzuwenden und ein besseres Verständnis für die weiteren Auswirkungen digitaler Technologien zu entwickeln. Ethische Perspektiven auf den digitalen Wandel im Gesundheitswesen sollten auch die politischen und ökonomischen Voraussetzungen digitaler Praktiken im Blick haben und die sozialen Auswirkungen innerhalb einzelner Gesellschaften sowie auf globaler Ebene bewerten.

Digitale Transformationen sind Gesundheits-Determinanten, die mit größeren politischen, gesellschaftlichen und wirtschaftlichen Dynamiken interagieren. Die Politik muss all diese Determinanten entsprechend berücksichtigen. Digitale Praktiken und Daten werden vielleicht sogar das dominierende Prisma werden, durch das wir über Gesundheit und Wohlbefinden nachdenken. Diese Entwicklung wird durch die Datafizierung

und Digitalisierung der Gesundheit (siehe **Datafizierung („Verdatung“) der Gesundheit**), einschließlich KI und datengesteuerter Analysen in der Genomik vorangetrieben. Die Medizin wurde schon immer von wissenschaftlichen Durchbrüchen und technologischen Innovationen angetrieben. Aber die Art der Technologie in Verbindung mit dem Grad der Konvergenz, den wir jetzt erleben, und die Geschwindigkeit des Wandels sind beispiellos. Es gibt auch eine zunehmende Konvergenz zwischen der digitalen Transformation und der öffentlichen Gesundheit, die durch die COVID19-Pandemie noch verstärkt wurde. Die Pandemie hat gezeigt wie Gesundheitsrisiken und auch Datensätze Grenzen überschreiten, gleichzeitig aber bestehende Ungleichheiten und Diskriminierungen verstärken können. Die Pandemie verdeutlichte auch den Einfluss der multinationalen Technologiekonzerne und Plattformen, von denen viele bereits rasch in den Gesundheitsbereich eindrangen und nun zunehmend an Bedeutung gewinnen.

Die Grenzen der digitalen Transformation des Gesundheitswesens verschieben sich immer schneller, oft ohne Rücksicht auf gesundheitliche Chancengleichheit oder sogar Menschenrechte. Der schnelle Zugang zu Echtzeitinformationen und die Intensität der digitalen Debatte erfordern ständige Wachsamkeit.

Ohne Engagement für Solidarität, Gerechtigkeit und neue Formen der digitalen Gesundheitsbürgerschaft (siehe **Digitale Gesundheitsbürgerschaft [Digital Health Citizenship]**) könnte die Gesundheit zu einem Feld werden, in dem neue Formen des Überwachungskapitalismus und des Datenkolonialismus besonders wirksam werden (siehe **Datenkolonialismus**). Die herausforderndste Dimension des extremen Ungleichgewichts, wer von der digitalen Transformation profitiert, ist das, was Shoshana Zuboff als „Überwachungskapitalismus“ bezeichnet hat. Die Datensolidarität arbeitet auf das Ziel hin, den Wert, den Gesundheitsdaten und andere digitale Daten für die Öffentlichkeit schaffen, zu maximieren, jedoch nicht auf Kosten der Menschen und Gemeinschaften.

Referenzen: Kickbusch et al., 2021; Zuboff, 2019.

5.2 Vertrauen in Daten und digitale Plattformen

Die *Lancet* und *Financial Times* Kommission hat argumentiert, dass der Aufbau von Vertrauen zwischen allen Beteiligten des digitalen Gesundheitsökosystems eine der dringendsten Aufgaben ist. Geringes Vertrauen in Gesundheitssysteme stellt ein Risiko für die Gesundheit von Menschen dar. Datensolidarität – indem sie darauf abzielt, eine gerechtere Aufteilung der Vorteile und Risiken digitaler Praktiken zu erreichen – kann dazu beitragen, Vertrauen in Datennutzung im Gesundheitswesen aufzubauen.

Daten können über Leben und Tod entscheiden – sie stellen auch eine Reihe von ethischen und menschenrechtlichen Herausforderungen dar. Wie wir bei COVID-19 gesehen haben, führten fehlende Daten über den ethnischen Hintergrund derjenigen, die an COVID schwer erkrankten, zu Ungleichheiten in der Behandlung. Das Fehlen harmonisierter Datenerfassungsstandards erschwerte den länderübergreifenden Vergleich epidemiologischer Informationen unnötig. Fehlinformationen über die Gesundheit sind eine weitere bekannte Folge einer schlechten Datenverwaltung. Wo Menschen das Gefühl hatten, keinen ausreichenden Zugang zu Gesundheitsversorgung oder zuverlässigen Informationen zu erhalten, ging ihr Vertrauen in bestehende Systeme und Informationsquellen verloren.

Bedenken hinsichtlich der Privatsphäre, der Sicherheit und der Verletzung von Rechten tragen zu einem Mangel an Vertrauen zwischen Gemeinschaften, Gesundheitspersonal und anderen Gruppen bei. Dies beschränkt die Möglichkeit nützlicher Innovation sowie zum Teilen von Daten zwischen Organisationen, Ländern und Unternehmen, und führt zu weniger evidenzbasierten Praktiken im Gesundheitssektor.

Wie bereits erwähnt, ist Datensolidarität ein Weg, Vertrauen in Datennutzung und digitale Praktiken im Gesundheitswesen zu stärken – nicht, indem man es von den Menschen fordert oder seine Bedeutung betont, sondern indem man die Vertrauenswürdigkeit der Datennutzung erhöht. Datensolidarität bedeutet besonders riskante Datennutzung zu verbieten und diese Verbote wirksam durchzusetzen, Maßnahmen zur Schadenslinderung einzuführen, und Ungerechtigkeiten auf globaler Ebene zu reduzieren.

Referenzen: Bollyky et al., 2023; Borges do Nascimento et al., 2022; Kickbusch et al., 2021.

5.3 Datafizierung („Verdatung“) der Gesundheit

Datafizierung verwandelt verschiedene Aspekte unseres Lebens und unserer Gesundheit in Datensätze, die gespeichert, analysiert, weitergegeben und genutzt werden können. Im Gesundheitsbereich hat die Datafizierung die klinische Forschung und die Arzneimittelentwicklungsprozesse verändert. Sie unterstützt Personen im Gesundheitssektor dabei, evidenzbasierte Entscheidungen zu treffen und ermöglicht die Analyse aggregierter (de-identifizierter) Gesundheitsdaten für Gesundheitsversorgung und Forschung. Datafizierung kann dadurch dazu beitragen, die Versorgung von Patientinnen und Patienten zu verbessern und die Effizienz des Gesundheitswesens zu steigern.

Ein Durchbruch in der Datenverarbeitung ist mit der Einführung von tragbaren Geräten gelungen, die den Nutzerinnen und Nutzern helfen können, Fortschritte zu überwachen, Muster zu erkennen, Anomalien zu entdecken und datengestützte Entscheidungen über ihre Gesundheit und ihr Wohlbefinden zu treffen, die auf Echtzeit-Feedback basieren. Dies wird von einigen auch mit Sorge betrachtet, da es bedeutet, dass qualitative Aspekte der Gesundheit und des Wohlbefindens häufig in quantifizierte Daten umgewandelt werden. Menschen, die Fotos von ihren Mahlzeiten machen oder den Schrittzähler auf ihrem Smartphone mit zum Joggen nehmen, machen damit Datensätze digital nutzbar, die davor – wenn überhaupt – nur auf einem Blatt Papier existierten und kaum verknüpfbar waren. Während Patientinnen und Patienten früher mit ihrer eigenen Stimme über diese Aspekte ihres Lebens berichteten, erzählen jetzt ihre Daten die Geschichte. Darüber hinaus sind Gesundheitsdaten häufig sensibel, was bedeutet, dass ihre unbefugte Nutzung durch Dritte großen Schaden anrichten kann, der vom Verlust des Zugangs zu (privaten) Kranken- und anderen Versicherungen bis hin zu Arbeitsplatzverlusten und sozialer Stigmatisierung reicht. Darüber hinaus können selbst harmlose Datensätze, wenn sie mit anderen Datensätzen verknüpft werden, zu Rückschlüssen auf das Verhalten oder die Gesundheit von Einzelpersonen führen, die wiederum zu diskriminierenden oder anderen schädlichen Maßnahmen führen können. Manchmal liegt dies daran, dass die Algorithmen, die für die Datenanalyse verwendet werden, gesellschaftliche Voreingenommenheiten oder „Verzerrungen“ widerspiegeln (z. B. Unterrepräsentierung marginalisierter Gruppen); manchmal liegt es daran, dass die bestehenden Gesetze und Richtlinien die Menschen nicht ausreichend vor den Schäden der prädiktiven Analytik und anderer Datenanalysen schützen. Dies ist nicht nur ein Problem im Unternehmenssektor, sondern auch im

öffentlichen Bereich. Der *Robodebt*-Skandal in Australien und der niederländische Kinderbeihilfen-Fall, bei denen jeweils Menschen aufgrund eines problematischen Algorithmus von Behörden fälschlicherweise bezichtigt wurden, zu viele staatliche Hilfen erhalten zu haben und diese zurückzahlen zu müssen, zeigen, dass es auch bei der Datennutzung durch öffentliche Einrichtungen erhebliche Probleme geben kann, die schwerwiegende Folgen für die Betroffenen haben.

Vor diesem Hintergrund zielt die Datensolidarität neben der Datensicherheit und dem Schutz der Privatsphäre darauf ab, dass die Menschen eine angemessene Kontrolle über die Daten haben, an deren Produktion sie beteiligt waren. Dazu gehört, dass die Menschen – als Einzelne oder als Teil von Gemeinschaften, denen sie angehören – mitbestimmen können, welche Arten von Wissen und Informationen überhaupt in Daten umgewandelt werden sollen. Datensolidarität soll auch sicherstellen, dass kommerzielle Gewinne, die mit den Daten der Menschen erzielt werden, mit diesen Menschen geteilt werden.

References: Carney, 2019; Eubanks, 2018; Fenger & Simonse, 2024; Quantified Self Through Numbers, undated; Ruckenstein et al., 2018; ten Seldam & Brenninkmeijer, 2021; University of Sydney, 2023.

5.4 Digitale Gesundheitskompetenz *(Digital Health Literacy)*

Die allgemeine Gesundheitskompetenz wird seit langem als Schlüsselfaktor für die Gesundheit angesehen – eine geringe Gesundheitskompetenz stellt ein Risiko für die eigene Gesundheit dar. Mit dem Fortschreiten der digitalen Transformation haben digitale Kompetenz im Allgemeinen und digitale Gesundheitskompetenz im Besonderen eine ähnlich wichtige Bedeutung erlangt. Ungleichheiten bei der digitalen Kompetenz können den Zugang der Menschen zu Gesundheitsinformationen und Gesundheitsdienstleistungen beeinträchtigen, und sich damit auf ihre Gesundheit auswirken. Die Nachfrage nach grundlegenden und fortgeschrittenen digitalen Kenntnissen für Patientinnen und Patienten sowie Angehörige der Gesundheitsberufe wird in der Zukunft weiter steigen, da auch das Gesundheitswesen und Gesundheitsorganisationen den Einsatz digitaler Technologien, einschließlich künstlicher Intelligenz, ausweiten. Ein Bericht der Europäischen Region der Weltgesundheitsorganisation (WHO) über digitale Gesundheit zeigt jedoch, dass nur sehr wenige Länder aktiv in die digitale Gesundheitskompetenz investieren. Dies wird zu zunehmenden Problemen und wachsenden Ungleichheiten führen – auch aufgrund erheblicher demografischer Verschiebungen.

Ein nützlicher Ansatz für die vielen Dimensionen der digitalen Gesundheitskompetenz ist das Transaktionsmodell der E-Health-Kompetenz, dass vier Kompetenzstufen für die digitale Gesundheitskompetenz umreißt: funktional, kommunikativ, kritisch und translational. Im Zusammenhang mit der Datensolidarität kommt insbesondere der kritischen digitalen Gesundheitskompetenz besondere Bedeutung zu. Sie bezieht sich auf die Fähigkeit, die Relevanz, die Vertrauenswürdigkeit und das Risiko des Austauschs und des Empfangs gesundheitsbezogener Informationen über das digitale Ökosystem kritisch zu bewerten. Es gibt aber auch eine sehr wichtige Komponente der kommunikativen Gesundheitskompetenz, die unter dem Begriff der Bürgerkompetenz zusammengefasst wird. Sie bezieht sich auf das Wissen und die Fähigkeit zur Partizipation, sowie darauf wie Menschen in digitalen Kontexten kommunizieren und wie bewusst sie sich ihrer Rechte und Pflichten im digitalen Ökosystem sind. Die digitale Gesundheitskompetenz ist daher von großer Bedeutung für die Ausübung der digitalen Gesundheitsbürgerschaft (siehe **Digitale Gesundheitsbürgerschaft *[Digital Health Citizenship]***).

Referenzen: Kickbusch & Holly, 2023; Paige et al., 2018; Seidel et al., 2023; van Kessel et al., 2022; World Health Organization Regional Office for Europe, 2023.

5.5 Digitale Gesundheitsbürgerschaft *(Digital Health Citizenship)*

Die digitale Gesundheitsbürgerschaft definiert nicht nur eine Reihe von Rechten und Pflichten, die durch die Nutzung digitaler Technologie (z. B. Gesundheits-Apps und -Plattformen) für gesundheitsbezogene Zwecke entstehen, sondern auch den Prozess und die Formen der Interaktion und Beteiligung, die im digitalen Gesundheitsraum entstehen.

Daten-*Governance* muss demokratischer werden und einen gerechten Zugang zu Gesundheitsressourcen gewährleisten. Einzelpersonen und Gruppen müssen in der Lage sein, sich aktiv an der Gestaltung und Umsetzung digitaler Gesundheitspolitik und -technologien zu beteiligen und diese mitzugestalten und den Entscheidungsträgern, Entwicklungsagenturen, Privatunternehmen und Entwicklern Rückmeldung zu geben. Dazu gehören auch Rahmenbedingungen für die Entwicklung von digitalen Technologien und Räumen sowie die Stärkung der Widerstandsfähigkeit von Gemeinschaften gegenüber negativen Auswirkungen des digitalen Wandels. Ein wertebasierter und menschenzentrierter Ansatz zur Steuerung des digitalen Wandels im Gesundheitsbereich baut auf der digitalen Gesundheitsbürgerschaft auf, um dem so genannten „Überwachungskapitalismus“ entgegenzuwirken. Das digitale Ökosystem ist auf die Beteiligung seiner Nutzerinnen und Nutzer angewiesen – es funktioniert nur, wenn Patientinnen und Patienten sowie Bürgerinnen und Bürger bereit sind, ihre Daten zur Verfügung zu stellen. Ein wertebasierter und menschenzentrierter Ansatz wie der Ansatz der Datensolidarität würde die Nutzerinnen und Nutzer vor der Extraktion ihrer Daten und den Algorithmen, die das Online-Verhalten steuern, schützen.

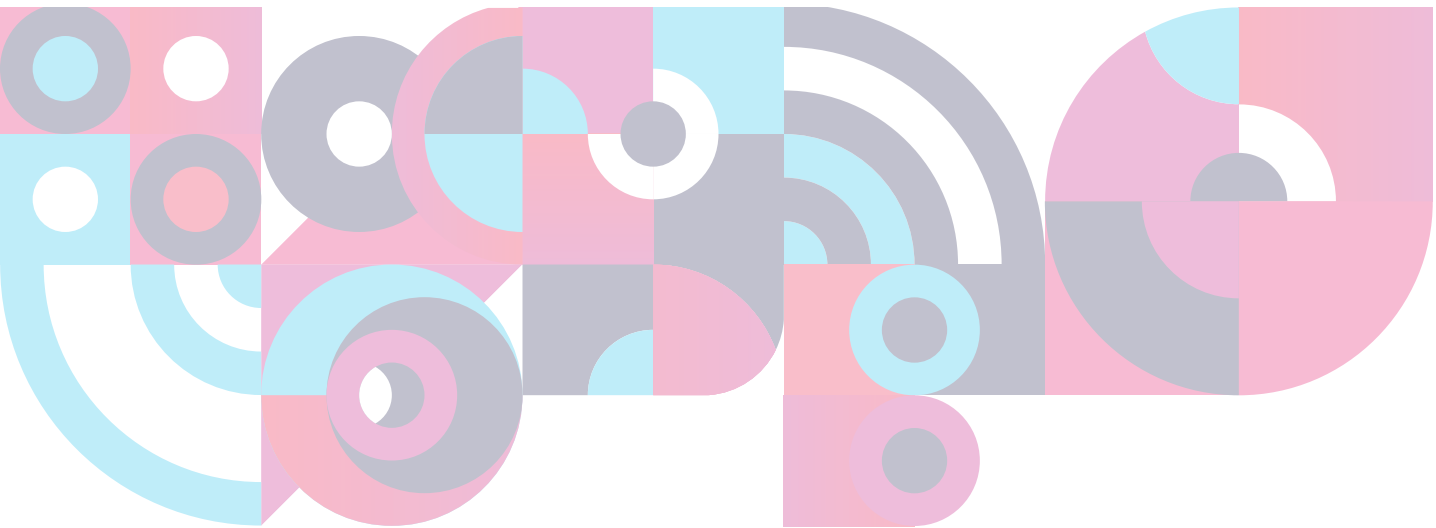
Das digitale Ökosystem bietet neue Räume für politische Partizipation und bürgerliche Debatten, auch zu Gesundheitsfragen. Ein gerechter Nutzen für die Gesundheit kann jedoch nur dann erzielt werden, wenn die Bürgerinnen und Bürger in der Lage sind, sich kritisch einzubringen, sich vor Fehlinformationen und Diskriminierung geschützt fühlen und informierte Entscheidungen in Bezug auf ihre Daten treffen können. Eine solche partizipative Daten-*Governance* muss ein entscheidendes Merkmal der digitalen Gesundheitsbürgerschaft des 21. Jahrhunderts sein. Dies könnte bedeuten, dass die Menschen, wenn es um Daten über ihren Körper oder sehr persönliche Aspekte ihres Lebens geht, ein direktes Mitspracherecht bei der Verwendung der Daten haben. Der Ansatz der Datensolidarität schlägt zudem auch eine stärkere Nutzung kollektiver Formen der Aufsicht und die Stärkung der institutionalisierten Solidarität vor. Bislang haben sich jedoch nur sehr wenige Regierungen dafür eingesetzt, die demokratischen und solidarischen Anreize und Vorteile des digitalen Gesundheitsökosystems zu stärken.

Die Forschung zur neuen „digitalen Gesundheitsbürgerschaft“ zeigt, dass die Menschen bereit sind, Informationen, Erfahrungen und Daten zu teilen – aber häufig wissen sie nicht, ob sie dies auf einer öffentlichen oder gemeinnützigen oder auf einer kommerziellen Plattform tun oder

welche Rolle Algorithmen bei ihren Entscheidungen spielen und was mit den Daten geschieht, die sie teilen. Die digitale Gesundheitsbürgerschaft erfordert Kompetenzen in den Bereichen Gesundheitskompetenz, digitale Kompetenz und umfassendere demokratische und staatsbürgerliche Kompetenz. Zivilgesellschaftliche Technologiemodelle, die sich im weitesten Sinne auf die gemeinsame Entwicklung (zwischen Nutzern, Technologieentwicklern usw.) und Nutzung digitaler Technologien zur Verbesserung der öffentlichen Beteiligung an demokratischen Prozessen und Entscheidungsprozessen beziehen, werden zunehmend als Wegbereiter für eine bessere öffentliche Politik und Leistungserbringung, auch im Gesundheitswesen, gesehen.

Eine aktive digitale Gesundheitsbürgerschaft wird oft durch die digitale Kluft – also den ungleichen Zugang zu digitalen Technologien und digitalen Fähigkeiten – behindert. Oft sind es dieselben Menschen und Gemeinschaften, die keinen Internetzugang haben, die nicht gut lesen und schreiben können und die am wenigsten Zugang zu einer hochwertigen Gesundheitsversorgung haben. Kooperative *Governance*-Modelle, die verschiedene Sektoren – öffentliche und private – zusammenbringen, müssen auch solche Gemeinschaften einbeziehen, um die sich daraus ergebenden Herausforderungen für Gerechtigkeit zu bewältigen.

Referenzen: Kickbusch, 2023; Petrakaki et al., 2021; Prainsack & Buyx, 2017; Zuboff, 2019.



Literaturverzeichnis

Adecco Group. (2023). *Understanding digital justice: How can we fight for fair technological practices.* [Online]. https://www.adeccogroup.com/future-of-work/latest-insights/understanding-digital-justice-how-can-we-fight-for-fair-technological-practices

Affleck, E., Sutherland, E., Lindeman, C., Golonka, R., Price, T., Murphy, T., Williamson, T., Chapman, A., et al. (2024). Human factor health data interoperability. *HealthcarePapers*, *21*(4), 47-55. https://doi.org/10.12927/hcpap.2024.27272

Afina, Y., Buscher, M., Krasodomski, A., Rowe, J., Sun, N., & Wilkinson, R. (2024). *Towards a global approach to digital platform regulation: Preserving openness amid the push for internet sovereignty*. Research Paper. London: Royal Institute of International Affairs. https://doi.org/10.55317/9781784135935

Autili, M., Di Ruscio, D., Inverardi, P., Pelliccione, P., & Massimo, T. (2019). A software exoskeleton to protect and support citizen's ethics and privacy in the digital world. *IEEE Access*, *7*, 62011-62021. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8712524

Benjamin, R. (2019). *Race after technology: Abolitionist tools for the New Jim Code*. Cambridge: Polity Press.

Bezuidenhout, L.M., Leonelli, S., Kelly, A.H., & Rappert, B. (2017). Beyond the digital divide: towards a situated approach to Open Data. *Science and Public Policy*, *44*(4), 464-475. https://doi.org/10.1093/scipol/scw036

Birch, K. (2023). Data. In: *Data enclaves*, 19-40. Cham: Palgrave Macmillan. https://doi.org/10.1007/978-3-031-46402-7_2

Blasimme, A., Vayena, E., & Hafen, E. (2018). Democratizing health research through data cooperatives. *Philosophy and Technology*, *31*(3), 473-479. https://doi.org/10.1007/s13347-018-0320-8

Bollier, D., & Helfrich, S. (2019). *Free, fair and alive: The insurgent power of the commons*. Gabriola Island: New Society Publishers.

Bollyky. T.J., Kickbusch, I., & Petersen, M.B. (2023). *The trust gap: How to fight pandemics in a divided country.* Foreign Affairs. [Online]. www.foreignaffairs.com/united-states/trust-gap-fight-pandemic-divided-country

Borges do Nascimento, I.J., Pizarro, A.B., Almeida, J.M., Azzopardi-Muscat, N., Gonçalves, M.A., Björklund, M., & Novillo-Ortiz, D. (2022). Infodemics and health misinformation: A systematic review of reviews. *Bulletin of the World Health Organization*, *100*(9), 544-561. https://doi.org/10.2471/BLT.21.287654

Bozeman, B. (2007). *Public values and public interest: Counterbalancing economic individualism*. Washington D.C.: Georgetown University Press. https://www.jstor.org/stable/j.ctt2tt37c

Braun, M., & Hummel, P. (2022). Data justice and data solidarity. *Patterns*, *3*(3), Article 100427. https://doi.org/10.1016/j.patter.2021.100427

Brock, A. (2020). *Distributed Blackness: African American cybercultures*. New York: New York University Press.

Broeders, D., Cristiano, F., & Kaminska, M. (2023). In search of digital sovereignty and strategic autonomy: Normative power Europe to the test of its geopolitical ambitions. *JCMS: Journal of Common Market Studies*, *61*(5), 1261-1280. https://doi.org/10.1111/jcms.13462

Bryson, J.M., Crosby, B.C., & Bloomberg, L. (2014). Public value governance: Moving beyond traditional public administration and the New Public Management. *Public Administration Review*, *74*(4), 445-456. https://doi.org/10.1111/puar.12238

Carney, T. (2019). Robo-debt illegality: The seven veils of failed guarantees of the rule of law? *Alternative Law Journal*, *44*(1), 4-10. https://doi.org/10.1177/1037969X18815913

Carrier, J.G. (1991). Gifts, commodities and social relations: A Maussian view of exchange. *Sociological Forum*, *6*(1), 119-136. https://doi.org/10.1007/BF01112730

Carroll, S.R., Garba, I., Figueroa-Rodríguez, O.L., Holbrook, J., Lovett, R., Materechera, S., Parsons, M., Raseroka, K., et al. (2020). The CARE principles for Indigenous data governance. *Data Science Journal*, *19*(1), 43-43. https://doi.org/10.5334/dsj-2020-043

Castells, M. (2002). Informational capitalism. In: Webster, F. (ed.), *Theories of the information society*, 2nd edn., 97-123. Routledge. https://doi.org/10.4324/9780203426265

Cepelak, C. (2023). *An introduction to data ethics: What is the ethical use of data?*. Datacamp. [Online]. https://www.datacamp.com/blog/introduction-to-data-ethics

Chander, A. (2020). Is data localization a solution for Schrems II?. *Journal of International Economic Law*, *23*(3), 771-784. https://doi.org/10.1093/jiel/jgaa024

Chander, A., & Lê, U.P. (2014). Data nationalism. *Emory Law Journal*, *64*(3), 677-739. https://scholarlycommons.law.emory.edu/elj/vol64/iss3/2

Chavez, P. (2022). *Toward digital solidarity*. Lawfare Media. [Online]. https://www.lawfaremedia.org/article/toward-digital-solidarity

Coeckelbergh, M. (2024). What is digital humanism? A conceptual analysis and an argument for a more critical and political digital (post) humanism. *Journal of Responsible Technology*, *17*, Article 100073. https://doi.org/10.1016/j.jrt.2023.100073

Cohen, B., Hall, B., & Wood, C. (2017). Data localization laws and their impact on privacy, data security and the global economy. *Antitrust*, *32*(1), 107-114. https://www.americanbar.org/digital-asset-abstract.html/content/dam/aba/publications/antitrust/magazine/archived/2017/fall/data-localization-laws-impact-on-privacy.pdf

Constantaras, E., Geiger, G., Braun, J.C., Mehrotra, D., & Aung, H. (2023). *Inside the suspicion machine*. Wired. [Online]. https://www.wired.com/story/welfare-state-algorithms/

Couldry, N., & Mejias, U.A. (2019). *The costs of connection: How data is colonizing human life and appropriating it for capitalism*. Stanford: Stanford University Press.

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas*, *113*, 48-52. https://doi.org/10.1016/j.maturitas.2018.04.008

Dawson, A., & Verweij, M. (2012). Solidarity: a moral concept in need of clarification. *Public Health Ethics*, *5*(1), 1-5. http://www.jstor.org/stable/26644892

De Angelis, M. (2017). *Omnia sunt communia: On the commons and the transformation to postcapitalism*. London: Zed Books. https://www.bloomsbury.com/uk/omnia-sunt-communia-9781783600625/

Delacroix, S., & Lawrence, N.D. (2019) Bottom-up data trusts: Disturbing the 'one size fits all' approach to data governance. *International Data Privacy Law*, *9*(4), 236-252. https://doi.org/10.1093/idpl/ipz014

Dulong de Rosnay, M., & Stalder, F. (2020). Digital commons. *Internet Policy Review*, *9*(4). https://doi.org/10.14763/2020.4.1530

D4DHub. (ohne Datum). *Data governance in Africa*. [Online] https://d4dhub.eu/initiatives/data-governance-in-africa

Ebeling, M.F. (2016). *Healthcare and Big Data*. London, New York: Palgrave Macmillan. https://link.springer.com/book/10.1057/978-1-137-50221-6

Element AI, & Nesta. (2019). *Data trusts: A new tool for data governance*. White Paper. https://evergreen.ca/resource-hub/wp-content/uploads/2019/07/elementai-data-trusts-july-2019.pdf

El-Sayed, S., & Prainsack, B. (2022). Success of the European Health Data Space hinges on operationalizing public value, in addition to bridging digital divides. *BMJ Rapid Response*. https://www.bmj.com/content/378/bmj-2022-071913/rr-0

El-Sayed, S., Prainsack, B., Hogan, C., Möller, T., Gyarmati, P., Jordan, B., Koesten, L., & Forgó, N. (2023). *PLUTO – Public Value Assessment Tool*. University of Vienna. [Online]. https://pluto.univie.ac.at/

Eubanks, V. (2018). *Automating inequality: How high-tech tools profile, police and punish the poor.* New York: St. Martin's Press. https://doi.org/10.4000/sdt.42117

European Commission. (2020). *Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act)*. COM(2020) 767 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767

European Commission. (2025). *Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847 (Text with EEA relevance)*. OJ L, 2025/327. *http://data.europa.eu/eli/reg/2025/327/oj*

European Parliament, & Council of the European Union. (2022). *Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance)*. OJ L 152. http://data.europa.eu/eli/reg/2022/868/oj

Fenger, M., & Simonse, R. (2024). The implosion of the Dutch surveillance welfare state. *Social Policy & Administration*, *58*(2), 264-276. https://doi.org/10.1111/spol.12998

First Nations Centre. (2007). *OCAP: Ownership, Control, Access and Possession*. Sanctioned by the First Nations Information Governance Committee. Assembly of First Nations. Ottawa: National Aboriginal Health Organization. https://icwrn.uvic.ca/wp-content/uploads/2013/08/FNC-OCAP.pdf

First Nations Information Governance Centre. (2014). *Ownership, Control, Access and Possession (OCAP): The path to First Nations Information Governance*. Ottawa: The First Nations Information Governance Centre. https://achh.ca/wp-content/uploads/2018/07/OCAP_FNIGC.pdf

Floridi, L. (2020). The fight for digital sovereignty: What it is and why it matters, especially for the EU. *Philosophy & Technology*, *33*(3), 369-378. https://doi.org/10.1007/s13347-020-00423-6

Fukumoto, E., & Bozeman, B. (2019). Public values theory: What is missing?. *American Review of Public Administration*, *49*(6), 635-648. https://doi.org/10.1177/0275074018814244

Fuster Morell, M. (2011). An introductory historical contextualization of Online Creation Communities for the building of digital commons: The emergence of a free culture movement. In: Hellmann, S., Frischmuth, P., Auer, S., & Dietrich, D. (eds.), *Proceedings of the 6th Open Knowledge Conference (OKCon) 2011*. http://ceur-ws.org/Vol-739/

Gao, H.S. (2021). Data sovereignty and trade agreements: Three digital kingdoms. In: Chander, A., & Haochen, S. (eds.), *Data sovereignty: From the Digital Silk Road to the return of the state*, 213-239. Oxford: Oxford University Press. https://doi.org/10.1093/oso/9780197582794.003.0010

Gordon, G. (2024). Digital sovereignty, digital infrastructures, and quantum horizons. *AI & Society*, *39*(1), 125-137. https://doi.org/10.1007/s00146-023-01729-7

Hardinges, J., Wells, P., Blindfold, A., Tennison, J., & Scott, A. (2019). *Data trusts: lessons from three pilots*. Open Data Institute. https://theodi.org/article/odi-data-trusts-report/

Hardjono, T., & Pentland, A. (2020). Empowering innovation through data cooperatives. In: Pentland, A., Lipton, A., & Hardjono, T. (eds.), *Building the New Economy*. Cambridge, MA: MIT Press. https://doi.org/10.21428/ba67f642.0499afe0

Harman, L. B., Flite, C. A., & Bond, K. (2012). Electronic health records: privacy, confidentiality and security. *Virtual Mentor*, *14*(9), 712-719. https://doi.org/10.1001/virtualmentor.2012.14.9.stas1-1209

He, A. (2023). *State-centric data governance in China*. CIGI Papers No. 282. Centre for International Governance Innovation. https://www.cigionline.org/static/documents/no.282.pdf

Heeks, R., & Renken, J. (2018). Data justice for development: What would it mean?. *Information Development*, *34*(1), 90-102. https://doi.org/10.1177%2F0266666916678282

Hill, E.R. (2023). *Are data trusts trustworthy? Data is vital to health innovation but there remains a common feeling of mistrust in those who hold that data. Why?*. PHG Foundation. [Online]. https://www.phgfoundation.org/blog/are-data-trusts-trustworthy/

Hummel P., & Braun M. (2020). Just data? Solidarity and justice in data-driven medicine. *Life Sciences, Society and Policy*, *16*(8), 1-18. https://doi.org/10.1186/s40504-020-00101-7

Hummel, P., Braun, M., Tretter, M., & Dabrock, P. (2021). Data sovereignty: A review. *Big Data & Society*, *8*(1). https://doi.org/10.1177/2053951720982012

Ibrahim, S.A., Charlson, M. E., & Neill, D.B. (2020). Big Data analytics and the struggle for equity in health care: The promise and perils. *Health Equity*, *4*(1), 99-101. https://doi.org/10.1089/heq.2019.0112

IHME. (ohne Datum). *Global Burden of Disease (GBD).* [Online]. https://www.healthdata.org/research-analysis/gbd

Jussen, I., Schweihoff, J., Dahms, V., Möller, F., & Otto, B. (2023). Data sharing fundamentals: Characteristics and definition. In: Bui, T.X. (ed.), *Proceedings of the 56th Hawaii International Conference on System Sciences (HICSS), 2023*, 3685-3694. http://dx.doi.org/10.24251/HICSS.2023.452

Kattel, R., & Mazzucato, M. (2018). Mission-oriented innovation policy and dynamic capabilities in the public sector. *Industrial and Corporate Change*, *27*(5), 787-801. https://doi.org/10.1093/icc/dty032

Kickbusch, I. (2023). *Digital transformations – why we must build digital health citizenship.* Governing Health Futures: The Lancet and Financial Times Commission. [Online]. https://www.governinghealthfutures2030.org/digital-transformations-why-we-must-build-digital-health-citizenship/

Kickbusch I., & Holly, L. (2023). Addressing the digital determinants of health: health promotion must lead the charge. *Health Promotion International*, *38*(3). https://academic.oup.com/heapro/article/38/3/daad059/7188360

Kickbusch, I., Piselli, D., Agrawal, A., Balicer, R., Banner, O., Adelhardt, M., Capobianco, E., Fabian, C., et al. (2021). The Lancet and Financial Times Commission on governing health futures 2030: Growing up in a digital world. *The Lancet*, *398*(10312), 1727-1776. https://doi.org/10.1016/s0140-6736(21)01824-9

Kim, J.U., Oleribe, O., Njie, R., & Taylor-Robinson, S.D. (2017). A time for new North-South relationships in global health. *International Journal of General Medicine*, *10*, 401-408. https://doi.org/10.2147/IJGM.S146475

Kitchin, R. (2014). *The data revolution: Big Data, Open Data, data infrastructures and their consequences.* Thousand Oaks, CA: Sage Publications. https://doi.org/10.4135/9781473909472

Kraut, R. 2020. Altruism. In: Zalta, E.N. (ed.), *The Stanford encyclopedia of philosophy (fall 2020 edition)*. https://plato.stanford.edu/archives/fall2020/entries/altruism/

Knight, H.E., Deeny, S.R., Dreyer, K., Engmann, J., Mackintosh, M., Raza, S., Stafford, M., Tesfaye, R., et al. (2021). Challenging racism in the use of health data. *The Lancet. Digital health*, *3*(3), e144-e146. https://doi.org/10.1016/S2589-7500(21)00019-4

Koontz, L. (2017). *Information privacy in the evolving healthcare environment*, 2nd edn. CRC Press. https://doi.org/10.1201/b21867

Krutzinna, J., & Floridi, L. (2019). Ethical medical data donation: A pressing issue. In: Krutzinna, J. & Floridi, L. (eds.), *The ethics of medical data donation. Philosophical studies series, vol. 137*, 1-6. Cham: Springer. https://doi.org/10.1007/978-3-030-04363-6_1

Kukutai, T., & Taylor, J. (eds.). (2016). *Indigenous data sovereignty: Toward an agenda*. Canberra: Australian National University Press.

Leonelli, S. (2020). *Scientific research and Big Data*. In: Zalta, E.N. (ed.), *The Stanford encyclopedia of philosophy (summer 2020 edition)*. https://plato.stanford.edu/archives/sum2020/entries/science-big-data

Levin, N., Leonelli, S., Weckowska, D., Castle, D., & Dupré, J. (2016). How do scientists define openness? Exploring the relationship between Open Science policies and research practice. *Bulletin of science, technology & society, 36*(2), 128-141. https://doi.org/10.1177/0270467616668760

Linstedt, D., & Olschimke, M. (2015). *Building a scalable data warehouse with Data Vault 2.0*. Morgan Kaufmann. https://www.sciencedirect.com/book/9780128025109/building-a-scalable-data-warehouse-with-data-vault-2-0

Liu, J. (2022). China's data localization. In: Hong, Y., & Harwit, E. (eds.), *China's globalizing internet. History, power and governance*, 83-102. London: Routledge. https://doi.org/10.4324/9781003319184

Longo, D.L., & Drazen, J.M. (2016). Data sharing. *The New England Journal of Medicine, 374*(3), 276-277. https://doi.org/10.1056/NEJMe1516564

Mazzucato, M., & Ryan-Collins, J. (2022). Putting value creation back into 'public value': from market-fixing to market-shaping. *Journal of Economic Policy Reform, 25*(4), 345-360. https://doi.org/10.1080/17487870.2022.2053537

Marelli, L., Stevens, M., Sharon, T., Van Hoyweghen, I., Boeckhout, M., Colussi, I., Degelsegger-Márquez, A., El-Sayed, S., et al. (2023). The European Health Data Space: Too big to succeed?. *Health Policy, 135*, Article 104861. https://doi.org/10.1016/j.healthpol.2023.104861

McDonald, S. (2019). *Reclaiming data trusts*. Centre for International Governance Innovation [Online]. https://www.cigionline.org/articles/reclaiming-data-trusts/

McDonald, S. (2022). *A digital sovereign, by any other name*. Available at SSRN: https://ssrn.com/abstract=4035822 or http://dx.doi.org/10.2139/ssrn.4035822

McMahon, A., Buyx, A., & Prainsack, B. (2020). Big Data governance needs more collective responsibility: The role of harm mitigation in the governance of data use in medicine and beyond. *Medical Law Review, 28*(1), 155-182. https://doi.org/10.1093/medlaw/fwz016

Meynhardt, T. (2009). Public value inside: What is public value creation? *International Journal of Public Administration, 32*(3-4), 192-219. https://doi.org/10.1080/01900690902732632

Micheli, M., Farrell, E., Carballa-Smichowski, B., Posada-Sánchez, M., Signorelli, S., & Vespe, M. (2023). *Mapping the landscape of data intermediaries. Emerging models for more inclusive data governance*. Luxembourg: Publications Office of the European Union. https://publications.jrc.ec.europa.eu/repository/handle/JRC133988

Ministère de la Santé et de la Prévention. (2022). *Digital health actions and initiatives under the French Presidency of the Council of the European Union during the first semester of 2022*. Press Kit. https://esante.gouv.fr/sites/default/files/media_entity/documents/french-presidency-pfue-2022_en.pdf

Mitchell, J., Ker, D., & Lesher, M. (2021). *Measuring the economic value of data*. Going Digital Toolkit Note, No. 20. https://goingdigital.oecd.org/data/notes/No20_ToolkitNote_MeasuringtheValueofData.pdf

Mittelstadt, B.D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society, 3*(2). https://doi.org/10.1177/2053951716679679

Mittelstadt, B. (2017). From individual to group privacy in Big Data analytics. *Philosophy & Technology, 30*(4), 475-494. https://doi.org/10.1007/s13347-017-0253-7

Moore, M.H. (1995). *Creating public value: Strategic management in government*. Cambridge, MA: Harvard University Press. https://www.hup.harvard.edu/books/9780674175587

Nabatchi, T. (2012). Putting the 'public' back in public values research: Designing participation to identify and respond to values. *Public Administration Review, 72*(5), 699-708. https://doi.

org/10.1111/j.1540-6210.2012.02544.x

Nabatchi, T. (2018). Public values frames in administration and governance. *Perspectives on Public Management and Governance*, *1*(1), 59-72. https://doi.org/10.1093/ppmgov/gvx009

Neidhardt, J., Werthner, H., & Woltran, S. (2022). It is simple, it is complicated. In: Werthner, H., Prem, E., Lee, E.A., & Ghezzi, C. (eds.), *Perspectives on digital humanism*, 335-342. Cham: Springer. https://doi.org/10.1007/978-3-030-86144-5_46

Nerlich, B., Hartley, S., Raman, S., & Smith, A. (eds.). (2018). *Science and the politics of openness*. Manchester: Manchester University Press. https://manchesteruniversitypress.co.uk/9781526106469/

Nida-Rümelin, J. (2022). Digital humanism and the limits of Artificial Intelligence. In: Werthner, H., Prem, E., Lee, E.A., & Ghezzi, C. (eds.), *Perspectives on digital humanism*, 71-75. Cham: Springer. https://doi.org/10.1007/978-3-030-86144-5_10

Noble, S.U. (2018). *Algorithms of oppression: How search engines reinforce racism*. New York: New York University Press.

Nowotny, H. (2022). Digital humanism: Navigating the tensions ahead. In: Werthner, H., Prem, E., Lee, E.A., & Ghezzi, C. (eds.), *Perspectives on digital humanism*, 317-322. Springer: Cham. https://doi.org/10.1007/978-3-030-86144-5_43

OECD. (2016). *Recommendation of the Council on Health Data Governance*. OECD/LEGAL/0433. Paris: OECD Publishing. https://legalinstruments.oecd.org/public/doc/348/348.en.pdf

Okinawa, K. (2024). *Future of data governance in Asia and operationalisation of 'Data Free Flow with Trust'*. ERIA Policy Brief No. 2024-01. https://www.eria.org/uploads/Data-Free-Flow-with-Trust.pdf

Paige, S.R., Stellefson, M., Krieger, J.L., Anderson-Lewis, C., Cheong, J., & Stopka, C. (2018). Proposing a transactional model of eHealth literacy: Concept analysis. *Journal of Medical Internet Research*, *20*(10), e10175. https://doi.org/10.2196/10175

Paprica, P.A., Crichlow, M., Maillet, D.C., Kesselring, S., Pow, C., Scarnecchia, T.P., Schull, M.J., Cartagena, R.G., et al. (2023). Essential requirements for the governance and management of data trusts, data repositories and other data collaborations. *International Journal of Population Data Science*, *8*(4). https://doi.org/10.23889/ijpds.v8i4.2142

Peng, S., Silverstein, M., Suitor, J.L., Gilligan, M., Hwang, W., Nam, S., & Routh, B. (2018). Use of communication technology to maintain intergenerational contact: Toward an understanding of 'digital solidarity'. In: Neves, B.B., & Casimiro, C. (eds.), *Connecting families?*, 159-180. Bristol: Policy Press. http://dx.doi.org/10.1332/policypress/9781447339946.003.0009

Petrakaki, D., Hilberg, E., & Waring, J. (2021). The cultivation of digital health citizenship. *Social Science & Medicine*, *270*, Article 113675. https://doi.org/10.1016/j.socscimed.2021.113675

Plotkin, D. (2020). *Data stewardship: An actionable guide to effective data management and data governance*, 2nd edn. London: Academic Press.

Pot, M., Kieusseyan, N., & Prainsack, B. (2021). Not all biases are bad: equitable and inequitable biases in machine learning and radiology. *Insights Into Imaging*, *12*(1), Article 13. https://doi.org/10.1186/s13244-020-00955-7

Prainsack, B. (2019a). Logged out: Ownership, exclusion and public value in the digital data and information commons. *Big Data & Society*, *6*(1). https://doi.org/10.1177/2053951719829773

Prainsack, B. (2019b). Data donation: How to resist the iLeviathan. In: Krutzinna, J., & Floridi, L. (eds.), *The ethics of medical data donation. Philosophical studies series, vol. 137*, 9-22. Cham: Springer. https://doi.org/10.1007/978-3-030-04363-6_2

Prainsack, B. (2022). Beyond vaccination mandates: Solidarity and freedom during COVID-19. *American Journal of Public Health*, *112*(2), 232-233. https://doi.org/10.2105%2FAJPH.2021.306619

Prainsack, B., & Buyx, A. (2011). *Solidarity: Reflections on an emerging concept in bioethics*. London: Nuffield Council on Bioethics. https://www.nuffieldbioethics.org/publications/solidarity

Prainsack, B., & Buyx, A. (2016). Thinking ethical and regulatory frameworks in medicine from the perspective of solidarity on both sides of the Atlantic. *Theoretical Medicine and Bioethics*, *37*(6), 489-501. https://doi.org/10.1007/s11017-016-9390-8

Prainsack, B., & Buyx, A. (2017). *Solidarity in biomedicine and beyond*. Cambridge, UK: Cambridge University Press. https://doi.org/10.1017/9781139696593

Prainsack, B., El-Sayed, S., Forgó, N., Szoszkiewicz, Ł., & Baumer, P. (2022a). Data Solidarity: A blueprint for governing health futures. *The Lancet Digital Health*, *4*(11), e773-e774. https://doi.org/10.1016/S2589-7500(22)00189-3

Prainsack, B., El-Sayed, S., Forgó, N., Szoszkiewicz, Ł., & Baumer, P. (2022b). *White Paper: Data solidarity*. Geneva: The Lancet & Financial Times Commission on Governing Health Futures. https://www.governinghealthfutures2030.org/wp-content/uploads/2022/12/DataSolidarity.pdf

Prainsack, B., & El-Sayed, S. (2023). Beyond individual rights: How data solidarity gives people meaningful control over data. *The American Journal of Bioethics*, *23*(11), 36-39. https://doi.org/10.1080/15265161.2023.2256267

Public Health Agency of Canada. (2022). *Pan-Canadian Health Data Strategy: Toward a world-class health data system*. Expert Advisory Group – Final Report. https://www.canada.ca/content/dam/phac-aspc/documents/corporate/mandate/about-agency/external-advisory-bodies/list/pan-canadian-health-data-strategy-reports-summaries/expert-advisory-group-report-03-toward-world-class-health-data-system/expert-advisory-group-report-03-toward-world-class-health-data-system.pdf

Quantified Self Through Numbers. (ohne Datum). *What is Quantified Self?*. [Online]. https://quantifiedself.com/about/what-is-quantified-self/

Raj, M., De Vries, R., Nong, P., Kardia, S.L.R., & Platt, J.E. (2020). Do people have an ethical obligation to share their health information? Comparing narratives of altruism and health information sharing in a nationally representative sample. *PLOS ONE*, *15*(12), e0244767. https://doi.org/10.1371/journal.pone.0244767

Rieder, G., & Simon, J. (2017). Big Data: A new empiricism and its epistemic and socio-political consequences. In: Pietsch, W., Wernecke, J., & Ott, M. (eds.), *Berechenbarkeit der Welt?: Philosophie und Wissenschaft im Zeitalter von Big Data*, 85-105. Wiesbaden: Springer. https://doi.org/10.1007/978-3-658-12153-2_4

Roberts, T., & Bosch, T. (eds.). (2023). *Digital citizenship in Africa: Technologies of agency and repression*. New York: Zed Books. http://dx.doi.org/10.25969/mediarep/20034

Ruckenstein, M., & Schüll, N.D. (2018). The datafication of health. *Annual Review of Anthropology*, *46*, 261-278. https://doi.org/10.1146/annurev-anthro-102116-041244

Samochowiec, J., & Müller, A. (2021). *Are smartwatches eroding solidarity? Scenarios for a data-driven healthcare system*. Zürich: Gottlieb Duttweiler Institute. http://doi.org/10.59986/JTWO8035

Sangiovanni, A., & Viehoff, J. (2023). Solidarity in social and political philosophy. In: Zalta, E.N., & Nodelman, U. (eds.), *The Stanford encyclopedia of philosophy (summer 2023 edition)*. https://plato.stanford.edu/archives/sum2023/entries/solidarity/

Saxinger, G., & First Nation of Na-Cho Nyak Dun. (2018). Community based participatory research as a long-term process: Reflections on becoming partners in understanding social dimensions of mining in the Yukon. *The Northern Review*, *47*, 187-207. https://doi.org/10.22584/nr47.2018.009

Scholz, S.J. (2008). *Political solidarity*. University Park: Pennsylvania State University Press.

Sciences Po. (ohne Datum). *Digital and data sovereignty*. [Online]. https://www.sciencespo.fr/public/chaire-numerique/en/thematic-research/digital-and-data-sovereignty/

Seidel, E., Cortes, T., & Chong, C. (2023). *Digital health literacy*. Patient Safety Network. [Online]. https://psnet.ahrq.gov/primer/digital-health-literacy

Segalla, M., & Rouziès, D. (2023). *The ethics of managing people's data*. Harvard Business Review. [Online]. https://hbr.org/2023/07/the-ethics-of-managing-peoples-data

Shabani, M. (2022). Will the European Health Data Space change data sharing rules?. *Science*, *375*(6587), 1357-1359. https://doi.org/10.1126/science.abn4874

Shiffman, J., & Shawar, Y. R. (2020). Strengthening accountability of the global health metrics enterprise. *The Lancet*, *395*(10234), 1452-1456. https://doi.org/10.1016/S0140-6736(20)30416-5

Shults, L.M. (2024). Avoiding parasitical uses of global solidarity. *Frontiers in Human Dynamics*, *6*, 1305952. https://doi.org/10.3389/fhumd.2024.1305952

Sorbie, A. (2021). The public interest. In: Laurie, G. et al. (eds.), *The Cambridge handbook of health research regulation*, 65-72. Cambridge: Cambridge University Press. https://doi.org/10.1017/9781108620024.009

Stalder, F. (2013). *Digital solidarity*. London: Mute Books & Post-Media Lab. https://www.metamute.org/sites/www.metamute.org/files/u1/Digital-Solidarity-Felix-Stalder-9781906496920-web-fullbook.pdf

Struett, T., Aaronson, S.A., & Zable, A. (ohne Datum). *Data governance mapping project, year 4*. Digital Trade & Data Governance Hub. https://globaldatagovernancemapping.org/images/DataGovHub-Year-4/short-4th-report.pdf

Szoszkiewicz, L. (2021). Open data: Toward achieving and measuring the Sustainable Development Goals. In: Leal Filho, W. et al. (eds), *Industry, innovation and infrastructure. Encyclopedia of the UN Sustainable Development Goals*. Cham: Springer. https://doi.org/10.1007/978-3-319-71059-4_129-1

Talend. (ohne Datum). *What is data extraction? Definition and examples*. [Online]. https://www.talend.com/resources/data-extraction-defined/

Taylor, K.S., Mahtani, K.R., & Aronson, J.K. (2021). Summarising good practice guidelines for data extraction for systematic reviews and meta-analysis. *BMJ Evidence-Based Medicine*, *26*(3), 88-90. https://doi.org/10.1136/bmjebm-2020-111651

Taylor, L. (2017). What is data justice? The case for connecting digital rights and freedoms globally. *Big Data & Society*, *4*(2). https://doi.org/10.1177/2053951717736335

Taylor, L., Floridi, L., & Van der Sloot, B. (eds.). (2017). *Group privacy: New challenges of data technologies*. Cham: Springer.

Taylor, R.D. (2020). 'Data localization': The Internet in the balance. *Telecommunications Policy*, *44*(8), Article 102003. https://doi.org/10.1016/j.telpol.2020.102003

TEHDAS. (2021). *Presentation of a first set of data altruism definitions, use cases and findings*. [Online]. https://tehdas.eu/app/uploads/2021/09/tehdas-presentation-of-a-first-set-of-data-altruism-definitions-use-cases-and-findings.pdf

ten Seldam, B., & Brenninkmeijer, A. (2021) *The Dutch benefits scandal: A cautionary tale for algorithmic enforcement*. EU Law Enforcement. [Online]. https://eulawenforcement.com/?p=7941

Terzis, P., & Santamaria Echeverria, O.E. (2023). Interoperability and governance in the European Health Data Space regulation. *Medical Law International*, *23*(4), 368-376. https://doi.org/10.1177/09685332231165692

Tietoevry. (2023). *Digital sovereignty. Adapting to a challenging digital landscape*. https://www.tietoevry.com/siteassets/files/tech-services/tech-services-digital-sovereignty-whitepaper-v1-2023.pdf

Transform Health. (2022). *Statement ahead of the 75th World Health Assembly*. [Online]. https://transformhealthcoalition.org/transform-health-world-health-assembly-statement/

Turkel, E., & Turkel, G. (2016). Public value theory: Reconciling public interests, administrative autonomy and efficiency. *Review of Public Administration and Management*, *4*(2). https://doi.org/10.4172/2315-7844.1000189

UHC 2030. (ohne Datum). *Taking action for universal health coverage. The UN High-Level Meeting on UHC 2023*. [Online]. https://www.uhc2030.org/un-hlm-2023/

UN General Assembly. (2007). *United Nations Declaration on the Rights of Indigenous Peoples: resolution / adopted by the General Assembly*. A/RES/61/295. https://www.refworld.org/legal/resolution/unga/2007/en/49353

United Nations. (ohne Datum). *Office of the Secretary-General's Envoy on Technology*. Global Digital Compact. [Online]. https://www.un.org/techenvoy/global-digital-compact

Universität Bern. (2021). *Security implications of digitalization*: *The dangers of data colonialism and the way towards sustainable and sovereign management of environmental data*. Report for the Federal Department of Foreign Affairs. https://boris.unibe.ch/157323/1/Security_implications_of_digitalization.pdf

University of Sydney. (2023). *Unraveling Robodebt: Legal failures, impact on vulnerable communities and future reforms*. [Online]. https://www.sydney.edu.au/law/news-and-events/news/2023/12/13/unraveling-robodebt-legal-failures-impacts.html

U.S. Department of State. (2024). *Building digital solidarity: The United States International Cyberspace & Digital Policy Strategy*. [Online]. https://www.state.gov/building-digital-solidarity-the-united-states-international-cyberspace-and-digital-policy-strategy/

van Dijck, J. (2014). Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology. *Surveillance & Society*, *12*(2), 197-208. https://doi.org/10.24908/ss.v12i2.4776

van Kessel, R., Wong, B.L.H., Clemens, T., & Brand, H. (2022). Digital health literacy as a super determinant of health: More than simply the sum of its parts. *Internet interventions*, *27*, Article 100500. https://doi.org/10.1016/j.invent.2022.100500

van Till, S.A.L., Smids, J., & Bunnik, E.M. (2023). Access to effective but expensive treatments: An analysis of the solidarity argument in discussions on funding of medical treatments. *Bioethics*, *37*(2), 111-119. https://doi.org/10.1111/bioe.13108

Verhulst, S.G. (2023). Operationalizing digital self-determination. *Data & Policy*, *5*, Article e14. https://doi.org/10.1017/dap.2023.11

Viberg Johansson, J., Bentzen, H.B., & Mascalzoni, D. (2022). What ethical approaches are used by scientists when sharing health data? An interview study. *BMC Medical Ethics*, *23*, Article 41. https://doi.org/10.1186/s12910-022-00779-8

Walker, K. (ohne Datum). *From a splintering net to digital solidarity*. Foreign Policy. [Online]. https://sponsored.foreignpolicy.com/google/from-a-splintering-net-to-digital-solidarity/

Werthner, H., Lee, E.A., Akkermans, H., Vardi, M., Ghezzi, C., Magnenat-Thalmann, N., Nowotny, H., Hardman, L., et al. (2019). *Vienna Manifesto on Digital Humanism*. [Online]. https://dighum.ec.tuwien.ac.at/dighum-manifesto/

Werthner, H., Prem, E., Lee, E.A., & Ghezzi, C. (eds.). (2022). *Perspectives on digital humanism*. Cham: Springer International Publishing. https://library.oapen.org/handle/20.500.12657/51945

Wilkinson, M.D., Dumontier, M., Aalbersberg, I.J., Appleton, G., Axton, M., Baak, A., Blomberg, N., Boiten, J.-W., et al. (2016). The FAIR Guiding Principles for scientific data management and stewardship. *Scientific Data*, *3*(1), Article 160018. https://doi.org/10.1038/sdata.2016.18

Wójcik, M.A. (2022). Algorithmic discrimination in health care: An EU law perspective. *Health and Human Rights Journal*, *24*(1), 93-103. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9212826/

Woods, A.K. (2018). Litigating data sovereignty. *The Yale Law Journal*, *128*(2), 328-406. Available at SSRN: https://ssrn.com/abstract=3256422

World Health Organization. (2021). *Global strategy on digital health 2020-2025*. Geneva: World Health Organization. https://www.who.int/docs/default-source/documents/gs4dhdaa2a9f352b0445bafbc79ca799dce4d.pdf

World Health Organization. (2020). WHO *data principles*. [Online]. https://data.who.int/about/data/who-data-principles

World Health Organization Regional Office for Europe. (2023). *Digital health in the WHO European Region: The ongoing journey to commitment and transformation*. https://www.who.int/andorra/publications/m/item/digital-health-in-the-who-european-region-the-ongoing-journey-to-commitment-and-transformation

Young, I.M. (1990). *Justice and the politics of difference*. Princeton, NJ: Princeton University Press.

Zhu, J., & Marjanovic, O. (2022). A taxonomy of data cooperatives. In: *PACIS 2022 Proceedings*, 257. https://aisel.aisnet.org/pacis2022/257

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. London: Profile Books. https://profilebooks.com/work/the-age-of-surveillance-capitalism/

Digital Transformations for Health Lab (DTH-Lab)
Hosted by: The University of Geneva
Campus Biotech, Chemin des Mines 9
1202 Geneva, Switzerland
Email: team@dthlab.org

www.DTHLab.org