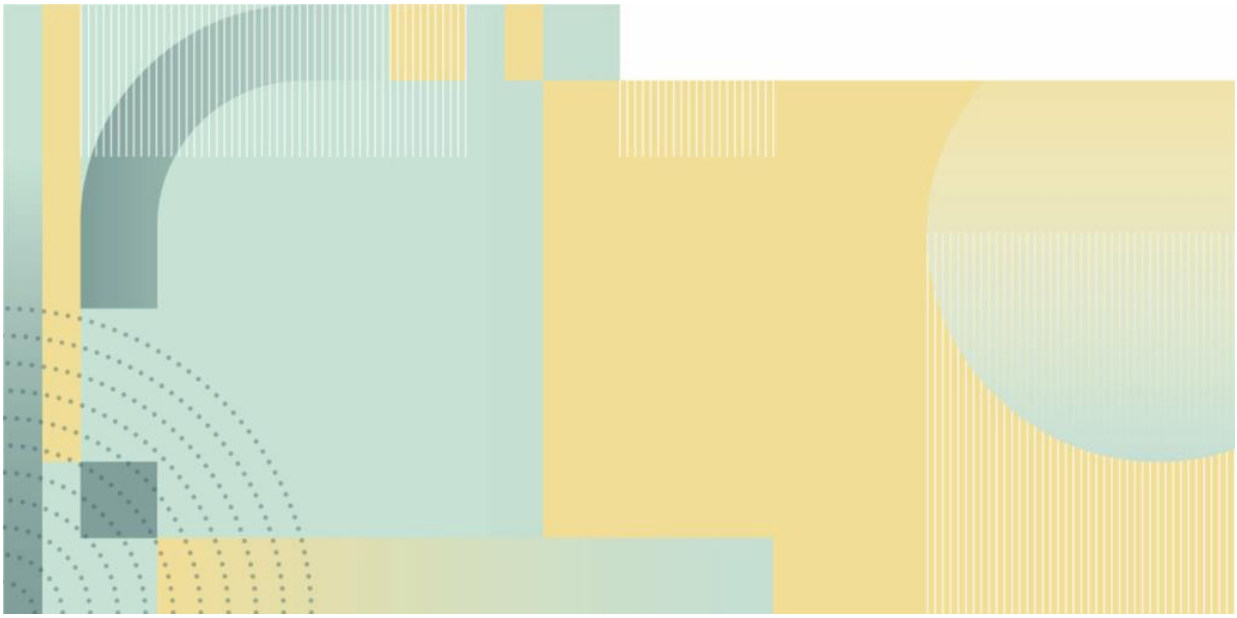
KURZSTUDIE
DIGITALE SOUVERÄNITÄT UND NACHHALTIGKEIT
Juli 2022



Analyse der Zusammenhänge zwischen Datensouveränität und Nachhaltigkeit

CO:DINA Forschungslinie Digitale Souveränität und Nachhaltigkeit

Autor*innen

Dr. Johannes Franke

Dr. Peter Gailhofer

Kurz gesagt

Datensouveränität ist ein schillernder Begriff, der sehr unterschiedlich verwendet wird. Der Beitrag untersucht die Implikationen verschiedener Souveränitäts-verständnisse für die Erreichung von Nachhaltigkeits-zielen und unterzieht auf dieser Grundlage gegenwärtige Regulierungsbestrebungen der EU einer kritischen Würdigung.

Diese Studie wurde für CO:DINA als Auftragsarbeit von den Partnern UfU e.V. und Öko-Institut e.V. erstellt.

UfU
Unabhängiges Institut für Umweltfragen

Öko-Institut e.V.
Institut für angewandte Ökologie
Institute for Applied Ecology

Inhaltsverzeichnis

Einleitung

Die digitale und die grüne Transformation sind die zwei großen Herausforderungen unserer Zeit. Gleichwohl werden Digitalisierung und Nachhaltigkeit bislang nicht ausreichend zusammengedacht, beide Prozesse verlaufen weitgehend unverbunden und zudem sehr unterschiedlich. Die grüne Transformation ist nicht nur dringend notwendig, sondern auch – dies steht spätestens seit dem „Klimabeschluss" des Bundesverfassungsgerichts[1] fest – (verfassungs-)rechtlich geboten. Dennoch tut sich die Politik in weiten Teilen schwer, formulierte Ziele mit wirkungsvollen Maßnahmen zu unterlegen und den Transformationsprozess wirklich in Gang zu bringen. Demgegenüber läuft die Digitalisierung auf Hochtouren und schafft permanent neue Fakten. Sie verläuft dabei aber weitgehend ungesteuert und folgt einer Marktlogik, die wenig Rücksicht auf ökologische und soziale Bedürfnisse nimmt. Wenn sich dies grundsätzlich ändern und die digitale auch die grüne Transformation unterstützen soll, genügt es nicht, auf das Nachhaltigkeitspotential einzelner digitaler Innovationen zu hoffen. Vielmehr wird es darauf ankommen, Digitalisierung und Nachhaltigkeit strukturell zu verknüpfen, und zwar sowohl konzeptionell als auch durch konkrete regulatorische Maßnahmen.

Vor diesem Hintergrund diskutiert die vorliegende Kurzstudie unterschiedliche Konzepte und mögliche regulatorische Ausgestaltungen von Datensouveränität im Hinblick auf die Erreichung von Nachhaltigkeitszielen. Die Diskussion um Datensouveränität bildet einen wichtigen Ausschnitt aus dem weiteren Diskurs um digitale Souveränität (Fritzsche et al., 2022). Im Kern geht es um die Frage, wer auf welche Daten zu welchen Zwecken zugreifen darf – und wer darüber wie entscheidet. Für eine nachhaltige Gestaltung der Digitalisierung sind diese Weichenstellungen von grundlegender Bedeutung. So macht es einen erheblichen Unterschied, ob kommerzielle Unternehmen, Verbraucher*innen, gemeinnützige Akteure, Wissenschaftler*innen oder staatliche Stellen darüber entscheiden, wie bestimmte Daten genutzt und mit wem sie geteilt werden. Entscheidungen können zudem auf unterschiedliche Weise, etwa individuell oder kollektiv, staatlich oder privat getroffen werden. Die konkrete Ausgestaltung von Datensouveränität ist dabei eine politische Regulierungsaufgabe.

[1] BVerfG, Beschluss vom 24.3.2021, 1 BvR 2656/18 u.a.

Die Kurzstudie analysiert zunächst unterschiedliche Konzepte von Datensouveränität und befragt sie hinsichtlich ihrer Implikationen für (ökologische) Nachhaltigkeitsziele. Sie unterscheidet dabei zwischen öffentlicher und individueller Datensouveränität und differenziert diese Oberkategorien weiter aus. Es zeigt sich, dass es aus Nachhaltigkeitsperspektive weniger darum geht, sich für ein einzelnes Konzept von Datensouveränität zu entscheiden, als vielmehr darum, unterschiedliche Ansätze und die Handlungsbeiträge verschiedener (privater und öffentlicher) Akteure sinnvoll zu verknüpfen. Auf dieser Grundlage untersucht der Beitrag, wie Datensouveränität durch staatliche bzw. europäische Regulierung nachhaltigkeitsorientiert ausgestaltet werden kann. Hierfür werden aktuelle Regulierungsvorschläge der EU im Hinblick auf Datenzugangsrechte der öffentlichen Hand, wirtschaftlich ausgerichtete Rechtspositionen und zivilgesellschaftliche Mitgestaltungsrechte einer kritischen Würdigung unterzogen.

Datensouveränität: Konzepte, Diskurse und Zusammenhänge mit Nachhaltigkeit

Datensouveränität ist ein schillernder Begriff, der je nach Verwendungskontext ganz unterschiedliche normative Vorstellungen zum Ausdruck bringen kann (Franke, 2021, S. 9; Franke & Gailhofer, 2021). Die Differenzen, die sich in den verschiedenen Diskursen um Datensouveränität beobachten lassen, betreffen dabei sowohl das Subjekt als auch den Inhalt von „Souveränität“. Die Frage lautet also: wer ist souverän und in welchem Sinne?

Diese Fragestellung ist für eine Untersuchung der Zusammenhänge zwischen Datensouveränität und Nachhaltigkeit von fundamentaler Bedeutung. Denn hinter dem wohlklingenden, zugleich aber unscharfen Souveränitätsbegriff können sich ganz unterschiedliche (politische) Vorstellungen und Interessen verbergen, die Nachhaltigkeitsbelange unterstützen, ihnen aber auch zuwiderlaufen können. Im Folgenden werden daher verschiedene Verwendungen des Begriffs der Datensouveränität, die derzeit in unterschiedlichen Diskursen zu beobachten sind, dargestellt und aus Nachhaltigkeitsperspektive bewertet. Dabei geht es nicht um eine vollständige Bestandsaufnahme, sondern um einen systematisierenden Überblick als Ausgangspunkt für weitere Überlegungen zu einer nachhaltigkeitsorientierten Ausgestaltung von Datensouveränität.

Öffentliche und individuelle Datensouveränität

Eine erste Weichenstellung besteht in der Unterscheidung zwischen öffentlicher und individueller Datensouveränität (Franke & Gailhofer, 2021). Die Differenzierung betrifft das Souveränitätssubjekt: während die individuelle Datensouveränität das Individuum als Akteur in den Mittelpunkt stellt, bezieht sich die öffentliche Datensouveränität auf die Unabhängigkeit und Handlungsfähigkeit von EU, Staaten und Kommunen.

Selbstverständlich ist diese Unterscheidung nicht immer trennscharf. Die Vorstellung einer kategorischen Trennung von Staat und Gesellschaft ist lange überholt und einer komplexen Aufgaben- und Verantwortungsteilung gewichen, in der staatliche und gesellschaftliche Akteure in ganz unterschiedlichen Formen zusammenwirken (Trute, 1999). Gleichwohl ist die Unterscheidung zwischen öffentlicher und individueller Datensouveränität weiterhin ein sinnvoller Ausgangspunkt, weil (grundrechtsgebundene) staatliche Akteure und (grundrechtsberechtigte) Individuen jeweils anderen Handlungsrationalitäten folgen (Voßkuhle, 2003, S. 295 f.).

Letzten Endes wird eine Untersuchung von Datensouveränität aus der Perspektive der Nachhaltigkeit freilich beide Seiten in den Blick nehmen müssen, so wie auch insgesamt eine nachhaltigkeitsorientierte Digitalisierung nur durch eine Kombination staatlicher und privater Beiträge gelingen kann. Hierfür kommt den Staaten – einschließlich der EU – eine Gewährleistungs- oder Regulierungsverantwortung zu, die auch die Gestaltung von Datensouveränität umfasst (Franke & Gailhofer, 2021). Denn es ist ganz wesentlich der Gesetzgeber, der durch die rechtliche Rahmensetzung festlegt, wer in welchem Sinne datensouverän ist. Dies wird bei einer Betrachtung der verschiedenen Spielarten sowohl von öffentlicher als auch von privater Datensouveränität deutlich.

Öffentliche Datensouveränität

Im Rahmen der öffentlichen Datensouveränität lassen sich vor allem zwei Diskurse identifizieren. Zum einen geht es um die Unabhängigkeit des europäischen Hoheits- und Wirtschaftsraums, zum anderen um die Handlungsfähigkeit von Verwaltung und Kommunen.

Geo- und industriepolitische Datensouveränität

Ein geo- und industriepolitisches Verständnis von Datensouveränität ist Teil eines breiteren Diskurses um die digitale Souveränität Deutschlands und Europas. Insbesondere auf der europäischen Ebene wird digitale Souveränität vielfach vor allem im Sinne strategischer Autonomie verstanden, als Unabhängigkeit von den (Vor-)Leistungen „fremder Mächte", d.h. Drittstaaten, aber auch außereuropäische Digitalkonzerne (vgl. Fritzsche et al., 2022, S. 6 ff.).

Diese Perspektive auf digitale Souveränität ist auch in der Debatte um Datensouveränität präsent und schlägt sich dort vor allem im Ziel unabhängiger europäischer Datenräume nieder (Europäische Kommission, 2020, S. 5, 25 ff.; Bundesregierung, 2021, S. 9, 11 ff.). Durch den Aufbau solcher Datenräume soll für europäische Unternehmen eine Alternative zu den großen (amerikanischen) Cloud-Anbietern geschaffen werden; Flaggschiff dieser Initiative ist das Projekt Gaia-X. Dabei geht die geo- und industriepolitische Interpretation von öffentlicher Datensouveränität Hand in Hand mit einem primär ökonomischen Verständnis der individuellen Datensouveränität europäischer Unternehmen (dazu unten, 0). Diese sollen in die Lage versetzt werden, Daten in einem geschützten Raum „souverän", d.h. nach eigenen Präferenzen, miteinander teilen zu können.[2] Insgesamt verfolgt dieses Souveränitätsverständnis also das Ziel, zugleich die Bedürfnisse europäischer Unternehmen und die geopolitischen Interessen der EU zu befördern (Bauer & Erixon, 2020, S. 6). Es ist von einem Konkurrenzdenken in „Wirtschaftsblöcken" geprägt, bei dem es darum geht, die Union und „ihre" Unternehmen im globalen Wettbewerb zu stärken.

Daneben wird im Zusammenhang mit europäischen Datenräumen der notwendige Schutz europäischer Standards, insbesondere im Hinblick auf das vergleichsweise hohe Datenschutzniveau, angeführt (Europäische Kommission, 2020, S. 4 f., 10 ff.). Insofern geht es neben geopolitisch-ökonomischer Unabhängigkeit auch um Souveränität im Sinne einer Fähigkeit zur Durchsetzung der eigenen rechtlichen Standards. Eine ähnliche Perspektive steht bei der nachfolgend dargestellten Datensouveränität von Verwaltung und Kommunen im Vordergrund.

[2] Das Zusammenspiel dieser industriepolitischen und ökonomischen Souveränitätsvorstellungen wird besonders deutlich bei BMWi (2020).

Datensouveränität von Verwaltung und Kommunen

Für Verwaltung und Kommunen wird (öffentliche) Datensouveränität als Bedingung für ihre Handlungs- und Steuerungsfähigkeit diskutiert. Sowohl die Europäische Kommission als auch die Bundesregierung diagnostizieren insofern, dass für die Wahrnehmung öffentlicher Aufgaben häufig nicht genügend Daten aus dem Privatsektor oder aus anderen staatlichen Einrichtungen zur Verfügung stehen und sehen entsprechenden Handlungsbedarf (Europäische Kommission, 2020, S. 9; Bundesregierung, 2021, S. 56 f.).

Der Zugang zu Daten für die öffentliche Hand ist sowohl für den Gesetzesvollzug (Gailhofer & Franke, S. 534, 539) zentral als auch bei der Wahrnehmung von Aufgaben der (kommunalen) Daseinsvorsorge, gerade im Kontext einer zunehmenden Datafizierung des öffentlichen Raums unter dem Schlagwort „Smart Cities“ (vgl. Partnerschaft Deutschland, 2020). Eine ausreichende Datengrundlage ermöglicht erst eine effektive Durchsetzung von Gesetzen und eine wirkungsvolle Gestaltung des Gemeinwesens. Datensouveränität bedeutet hier die Möglichkeit der öffentlichen Hand, informierte und damit wirkungsvolle Entscheidungen treffen zu können – eine Perspektive, die in ähnlicher Gestalt auch auf Ebene der individuellen Datensouveränität (siehe unten, 0.) eine Rolle spielt.

Implikationen für Nachhaltigkeitsziele

Welche Implikationen haben die dargestellten Spielarten öffentlicher Datensouveränität nun für die Erreichung von Nachhaltigkeitszielen?

Der *geo- und industriepolitisch* ausgerichtete Diskurs um Datensouveränität wird eng mit der Wahrung, Durchsetzung und Verbreitung „europäischer Werte“ verknüpft und dann auch mit (ökologischen) Nachhaltigkeitszielen in Verbindung gebracht. Ein solcher (positiver) Zusammenhang wird allerdings kaum erklärt oder gar hergeleitet, sondern vielmehr apodiktisch behauptet, wie der folgende Auszug aus der europäischen Datenstrategie beispielhaft verdeutlicht (Europäische Kommission, 2020, S. 5):

> „Ziel ist die Schaffung eines einheitlichen europäischen Datenraums (…), in dem sowohl personenbezogene als auch nicht-personenbezogene Daten, darunter auch sensible Geschäftsdaten, sicher sind und in dem Unternehmen auch leicht Zugang zu einer nahezu unbegrenzten Menge hochwertiger industrieller Daten erhalten. *Hierdurch* sollen das Wachstum

> und die Wertschöpfung gesteigert *und gleichzeitig* die CO2-Emissionen und der ökologische Fußabdruck der Menschen verringert werden." (Hervorhebungen von uns)

Warum die Schaffung eines europäischen Datenraums und ein einfacher Datenzugang für Unternehmen gleichsam automatisch auch die CO2-Emissionen und den ökologischen Fußabdruck der Menschen verringern sollen, wird nicht erklärt und ist auch nicht plausibel. Die Entwicklung nachhaltiger Produkte und Dienstleistungen hängt nicht primär von der Existenz eines Datenraums, sondern maßgeblich von den dort geltenden regulatorischen Rahmenbedingungen ab. Soweit dieser Regulierungsrahmen entsprechende Vorgaben macht oder Anreize setzt, bieten Datenräume tatsächlich Chancen für die Erreichung von Nachhaltigkeitszielen. Ohne solche Vorgaben bleibt indes nur die vage Hoffnung auf verantwortungsvolles unternehmerisches Handeln. Dies lässt sich an einem Vergleich mit dem Datenschutz veranschaulichen. Das hohe Datenschutzniveau in der EU hebt die Kommission in ihrer Datenstrategie ebenfalls als Argument für die Schaffung europäische Datenräume hervor (Europäische Kommission, 2020, S. 1, 11 f.), insofern allerdings nachvollziehbar und begründet: Denn unionsrechtliche Regulierungen wie insbesondere die Datenschutzgrundverordnung (DSGVO) schaffen einen rechtlichen Rahmen, der für das Handeln im Datenraum „Spielregeln" festlegt. Ohne diese Vorgaben wäre ein höheres Datenschutzniveau im europäischen Datenraum eine bloße Behauptung.

Eine europäische (öffentliche) Datensouveränität, die ihren Namen verdient, muss damit mehr sein als die bloße Bereitstellung von Infrastrukturen für Private in der Hoffnung, diese würden schon freiwillig zu Nachhaltigkeit und Gemeinwohl beitragen. Souveränität beinhaltet vielmehr (Regulierungs-)Verantwortung. Sie muss sich in der aktiven regulatorischen Gestaltung geschaffener Datenräume äußern.[3] Regelungen wie die DSGVO verwirklichen in diesem Sinne tatsächlich eine europäische Datensouveränität, die ebenso in Bezug auf Nachhaltigkeitsziele umzusetzen ist.

Eine effektive Regulierung und ihre Durchsetzung ist wiederum selbst auf einen hinreichenden Datenzugang angewiesen. Dies ist Kern des Diskurses um die *Datensouveränität von Verwaltung und Kommunen*. Freilich ist die bloße staatliche Kontrolle von oder die Zugriffsmöglichkeit auf Daten noch nicht

[3] Die Gestaltung hoheitlich oder mit hoheitlicher Unterstützung geschaffener Märkte ist seit jeher Aufgabe des Regulierungsrechts, dazu statt vieler Voßkuhle (2003), S. 307 ff.

hinreichend, um Nachhaltigkeitsziele zu fördern. Entscheidend ist vielmehr, zu welchen – rechtlich zu definierenden[4] – Zwecken der Staat auf (bestimmte) Daten zugreifen kann. Nachhaltigkeitszielen dient die Datensouveränität von Verwaltung und Kommunen immer dann, wenn es etwa um die effektive Durchsetzung umweltrechtlicher oder sonst nachhaltigkeitsbezogener Regelungen, um die Konzipierung neuer derartiger Regulierungsinstrumente oder um die Gestaltung einer nachhaltig-digitalen kommunalen Daseinsvorsorge (vgl. Beer et al., 2021) geht. Ein Datenzugriff ist hier notwendig, um demokratisch legitimierte – und in diesem Sinne „souveräne" – Entscheidungen in diesen Bereichen weiterhin effektiv treffen und durchsetzen zu können (Gailhofer & Franke, 2021, S. 539).

Damit ergibt sich bei einer nachhaltigkeitsorientierten Bewertung der Diskurse zur öffentlichen Datensouveränität zweierlei: Zum einen werden gesellschaftliche Transformationsprozesse nicht allein durch die Schaffung unabhängiger Datenräume, sondern erst durch deren Regulierung gelingen, in der sich die Souveränität des Gesetzgebers äußert. Zum anderen sind eine effektive nachhaltigkeitsorientierte Regulierung und deren Durchsetzung auf einen angemessenen Datenzugang der öffentlichen Hand angewiesen.

Individuelle Datensouveränität

Unter dem Begriff einer individuellen Datensouveränität können idealtypisch drei unterschiedliche Ideen und Diskurse um eine Datensouveränität differenziert werden: erstens wird Datensouveränität als v.a. datenschutzrechtlich auszugestaltendes Recht auf informationelle Selbstbestimmung begriffen; zweitens wird diese als häufig eigentumsrechtlich interpretiertes Verwertungsrecht an Daten verstanden; drittens kann eine an Bedeutung gewinnende Idee der Datensouveränität identifiziert werden, die diese als bürgerliche Gestaltungskompetenz begreift.

[4] Für den Zugang zu privat gehaltenen Daten ist eine solche Festlegung schon deswegen erforderlich, weil es sich hierbei um einen Eingriff zumindest in die Allgemeine Handlungsfreiheit (Art. 2 Abs. 1 GG) handelt, der einer gesetzlichen Grundlage bedarf, vgl. zum umfassenden Schutzbereich der Allgemeinen Handlungsfreiheit BVerfGE 80, 137 – Reiten im Walde.

Datensouveränität als „negatives" Recht auf informationelle Selbstbestimmung

Der Ursprung des Begriffs der Datensouveränität wird auf datenschutzrechtliche Kontexte der individuellen Datensouveränität zurückgeführt. Dieser wurde erstmalig mit dem Projekt der Einführung der elektronischen Gesundheitskarte (eGK) eingebracht, bei der die freiwillige Zustimmung (Einwilligung) der Patient*innen zur Erhebung und Verarbeitung, sowie das Recht auf die Löschung von personenbezogenen Daten als Datensouveränität bezeichnet wurde (Seidel 2014). Ein solcher Begriff der Datensouveränität ist zentral auf die informationelle Selbstbestimmung von Personen ausgerichtet, und soll deren persönliche Privatsphäre schützen, indem die Verwendung von personenbezogenen Daten grundsätzlich von der Einwilligung der Datensubjekte in die konkrete Datennutzung abhängig gemacht wird und diesen eine Reihe weiterer Rechte gegenüber Datennutzern eingeräumt werden. In seiner „Reinform"[5] beinhaltet dieser Begriff ein *negatives* Verständnis von Datensouveränität, das den Schwerpunkt auf den Ausschluss anderer von der Nutzung der eigenen persönlichen Informationen legt (Hummel, Braun & Dabrock 2019). Weiterentwicklungen dieses Souveränitätsbegriffs wollen über ein Ausschlussrecht hinausgehen und verstehen diese als eine den *„Chancen und Risiken von Big Data angemessene verantwortliche informationelle Freiheitsgestaltung"*. (Deutscher Ethikrat 2018) Auch wenn solche Weiterentwicklungen des personenbezogenen Souveränitätsbegriffs eine gewisse Dynamisierung des Datenschutzes im Hinblick auf Nutzungskontexte wie auch -chancen vorsehen und damit den Besonderheiten von Big Data damit besser gerecht werden,[6] zielt dieses Souveränitätsverständnis im Kern weiter auf die *„interaktive Persönlichkeitsentfaltung unter Wahrung von Privatheit in einer vernetzten Welt"* ab (Deutscher Ethikrat 2018).

[5] Diese „Reinform" existiert in der Praxis zwar nicht: so ermöglicht das Datenschutzrecht, das ein solches Souveränitätsverständnis umsetzt, auch „positiv" die kommerzielle Verwertung der eigenen Daten; datenschutzrechtliche Einwilligungen können auch gezielt eingesetzt werden, um personenbezogene Daten für solche Anwendungen oder Akteuren zu „spenden", die bestimmte, aus der Sicht der Datensubjekte befürwortete Ziele verfolgen.

[6] Etwa weil es sich von unter den Bedingungen von Big Data überholten Vorstellungen einer spezifischen, vorgegebenen Sensibilität bestimmter Daten und hierauf rekurrierender besonderer Schutzmechanismen löst und stärker auf die jeweiligen Verwendungszusammenhänge, Verantwortlichkeiten und Prozesse fokussiert, Deutscher Ethikrat, Stellungnahme Big Data und Gesundheit, 2018, 258.

Datensouveränität als eigentumsanaloge Freiheit zur ökonomischen Verwertung von und Verfügung über Daten

Weit verbreitet ist ein Verständnis von Datensouveränität, das diese als individuelle und exklusive Freiheitsgestaltung im Sinne ökonomischer Nutzungs- und Verwertungsrechte versteht (Gailhofer & Franke 2021; Franke & Gailhofer 2021). Datensouveränität in diesem Sinne hat, wie ein datenschutzrechtliches Verständnis, eine „negative" Komponente,[7] insofern sie dem Subjekt der Datensouveränität ermöglicht, andere von der Datennutzung auszuschließen. Sie wird dann aber im Sinne von quasi-eigentumsrechtlichen Rechtspositionen, wie dem Schutz von Urheberrechten oder auch Geschäftsgeheimnissen begriffen. Solche Ansätze weisen bestimmten Subjekten der Datensouveränität, z.B. den „Datenerzeugern" die Entscheidung zu, von der Datennutzung zu profitieren, über den Zugang Dritter und über die Zwecke der Datennutzung zu entscheiden. Gleichzeitig hat ein quasi-eigentumsrechtliches Souveränitätsverständnis aber auch eine „positive" Komponente: Exklusive Verwertungsrechte sollen, analog zu geistigen Eigentumsrechten wie z.B. Patenten, Anreize schaffen, Daten zu teilen und damit zur Entstehung von Datenmärkten und zur besseren Verfügbarkeit von Daten beitragen. Datensouveränität wird in diesem Sinne so verstanden, dass die Entscheidung, an wen und wozu die Datennutzung übertragen wird, vor allem im Sinne der ökonomischen Präferenzen des Dateninhabers und den Gesetzmäßigkeiten von Angebot und Nachfrage getroffen werden soll (Gailhofer 2021).

Eine rechtliche Zuweisung von Daten zu einem ursprünglichen Datenhalter als „Eigentümer" gibt es bislang nicht; zumindest in der Form eines quasi-dinglichen Eigentumsrechts ist eine solche auch nicht zu erwarten. Nichtsdestrotz ist ein Verständnis von Datensouveränität als „eigentumsanaloge", ökonomisch verstandene Freiheitsgestaltung in der Praxis vorherrschend.[8] Die Exklusivität der Datennutzung, ebenso wie die entgeltliche Übertragung von entsprechenden „Rechten" wird durch Verträge[9] und/oder technische

[7] S.o. S. 11.

[8] S. etwa die Definition der „International Data Spaces Association", die meint, dass Datensouveränität "enables you to self-determine how, when and at what price others may use it across the value chain", https://internationaldataspaces.org/why/data-sovereignty/.

[9] Ein dementsprechend „gelebtes" Verständnis von Datensouveränität und ihren Subjekten zeigt sich z.B in der vertraglichen Praxis. im Umgang mit Agrardaten, vgl. den

Vorkehrungen vorgenommen und abgesichert, Verbraucher „bezahlen" vermeintlich kostenfreie Angebote im Internet mit ihren personenbezogenen Daten. „Datenbroker" handeln im großen Stil mit Daten, Datenmärkte sind in der digitalisierten Wirtschaft maßgebende Größen,. Ein „eigentumsanaloger" Begriff von Datensouveränität wird auch durch europäische Infrastrukturen zum „Teilen" von Daten umgesetzt: So stellt das europäische Projekt Gaia X vor allem eine technische Infrastruktur für Datenmärkte dar, die auf klar definierte Nutzungsrechte für den „souveränen" Austausch von Daten setzt.[10] Der „selbst-souveräne" Umgang mit Datenrechten und dezentrale Möglichkeiten der Vermarktung sind auch prägende Motive im Diskurs um Blockchain-Technologie und dem „Web3".[11]

Datensouveränität als bürgerliche Gestaltungskompetenz

In Anlehnung an unterschiedliche, vergleichsweise junge Ansätzen kann Datensouveränität als bürgerliche oder zivilgesellschaftliche Gestaltungskompetenz begriffen werden. Solche Ansätze werden in Auseinandersetzung mit wahrgenommenen Problemen des persönlichkeitsrechtlichen oder „eigentumsanalogen" Datenrechtsverständnisses im Kontext der Digitalisierung entwickelt.

---

von Interessenvertretern der Landwirschaft erarbeiteten "EU Code of conduct on agricultural data sharing by contractual agreement", der das Recht des Datenerzeugers anerkennt, "whether they are a farmer or another party, to benefit from and/or be compensated for the use of data created as part of their activity. It also recognises the need to grant the data originator a leading role in controlling the access to and use of data from their business and to benefit from sharing the data with any partner that wishes to use their data. Therefore, the contract should clearly establish the benefits for the data originator", 8, online zugänglich unter: https://fefac.eu/wp-content/uploads/2020/07/eu_code_of_conduct_on_agricultural_data_sharing-1.pdf.

[10] Diese soll es jedem Unternehmen ermöglichen „selbst zu entscheiden, wo seine Daten gelagert werden und von wem sowie zu welchem Zweck sie verarbeitet werden dürfen", „die Grundlage eines Marktplatzes zur Monetarisierung von Betriebsdaten in industriellen Wertschöpfungsnetzwerken" schaffen und gleichzeitig „Anreize zum Datenaustausch über die verschiedenen Akteure hinweg" generieren, BMWi, Das Projekt Gaia X. Eine vernetzte Infrastruktur als Wiege eines vitalen, europäischen Öko-Systems, online verfügbar unter: https://www.bmwi.de/Redaktion/DE/Publikatio-nen/Digitale-Welt/das-projekt-gaia-x.pdf?__blob=publicationFile&v=16 2019) 15 ff; s. dazu schon Gailhofer (2021), 25. S.a. https://internationaldataspaces.org/we/gaia-x/.

[11] S. nur https://hackernoon.com/web-30-is-about-ownership-and-self-sovereignty.

So wird einerseits von den Defiziten eines persönlichkeitsrechtlichen Verständnisses dahingehend ausgegangen, dass dieses den Risiken der datengetriebenen Digitalisierung für die Rechte der Bürger*innen nicht genüge. Das liegt insbesondere – und offensichtlich – darin, dass eine auf informationelle Selbstbestimmung ausgerichtete Datensouveränität nur insoweit vermitteln kann, als es um personenbezogene Daten geht. Der Bezug zu identifizierbaren Personen ist für die digitalen Dynamiken der Datenverarbeitung, also z.B. Big Data-Analysen, oder das Training „intelligenter" Systeme häufig nicht ausschlaggebend: diese produzieren Erkenntnisse, Einsichten und entsprechende Vorschläge, die auf statistischer Ebene und in stark aggregierter Form relevant werden. Für entsprechende Datennutzungen wird es also unproblematisch sein, wenn Daten anonym erhoben, oder vollständig anonymisiert werden und damit die informationelle Selbstbestimmung nicht mehr betreffen.[12] Gerade weil die (maschinellen) Entscheidungen, die auf der Grundlage aggregierter Daten getroffen werden, für die Freiheitssphären der (ursprünglichen) Datensubjekte in vielerlei Hinsicht große Bedeutung haben können – z.B. weil sie die Planung von Infrastrukturen, oder die Verteilung von Ressourcen betreffen – meinen einige, dass ein solches Verständnis dem Anspruch auf „souveräne" Mitbestimmung der Bürger nicht genügt (Viljoen 2020).

Ein in seinem Begründungsansatz alternativer, in seinen Schlussfolgerungen aber vergleichbarer Ansatz, rekonstruiert Datensouveränität, ausgehend von einem „eigentumsanalogen" Rechtsverständnis, als zivilgesellschaftliche Gestaltungsfreiheit unter den Bedingungen der Digitalisierung. Die Rechtsmacht des Inhabers eines Eigentumsrechts soll demnach als Verrechtlichung seiner personalen Handlungskompetenz und Verbürgung von Handlungsalternativen des Bürgers verstanden werden (Fezer 2018). „Eigentum" sei demnach positiv, also nicht als „Habenstruktur", sondern als „Handlungsstruktur" (Fezer 2018) und als „personaler und demokratischer Funktionsbegriff" zu begreifen. Das traditionelle Rechtsverständnis zur Übertragbarkeit des Eigentumsgegenstands bedeute datenrechtlich zivilgesellschaftliche Mitwirkung der Bürger bei der Art und Weise der Organisation des Datengeschehens (Fezer, 2018, z. Ganzen a. Gailhofer 2021).

[12] Eine hinreichende Anonymisierung führt etwa auch dazu, dass der Grundsatz der Zweckbindung nicht mehr anwendbar ist, vgl. Erwägungsgrund 26 DSGVO (BFDI 2020)

Der Umstand, dass die entscheidende Bedeutung von Daten für grundlegende menschliche Rechte und Bedürfnisse und die zunehmend digitalisierte Gesellschaft nicht auf personenbezogene Daten beschränkt ist, führt dazu, dass eine bürgerliche Datensouveränität sich auch auf Daten beziehen muss, die einen Personenbezug nicht (mehr) aufweisen (Gailhofer 2021) Die Erkenntnis, dass die Nutzung von Daten, unabhängig von deren Herkunft, gravierende Folgen für Bürger*innen haben, verändert auch die Vorstellung davon, wie Datensouveränität ausgeübt werden sollte: Anstatt „exklusive", individuelle Rechte auf Unterlassung oder Zahlung zu schaffen, geht es nun darum, dass all diejenigen, deren Interessen durch die Nutzung von Daten betroffen sind, die Zwecke und Bedingungen der Datennutzung mit ausgestalten könnten. Die Frage, wie solche bürgerlichen Ansprüche umgesetzt und abgesichert werden können, zeigt wiederum das Zusammenspiel und die Wechselbezüglichkeit individueller und kollektiver oder öffentlicher Datensouveränität: Entsprechende Überlegungen setzen auf öffentliche Institutionen oder Governance-Strukturen, die Mitbestimmung der Subjekte der Datensouveränität und die Aushandlung der überindividuellen Dimensionen der Datennutzung organisieren können. Konzepte etwa zu kommunalen Datentreuhändern (Pietron, Gailhofer & Sommer 2022). „souveräne" Datenspenden verwaltenden „datenaltruistische Organisationen"[13] oder öffentliche „Datenagenturen" (Fezer 2018) können dementsprechend als Vorschläge zur Umsetzung von Datensouveränität als bürgerlicher Gestaltungskompetenz betrachtet werden.

Implikationen für Nachhaltigkeitsziele

Um die Implikationen unterschiedlicher Datensouveränitätsverständnisse auf Nachhaltigkeitsziele abzuschätzen, müssen die intelligenten datengetriebenen Anwendungen in den Blick genommen werden, die unsere zunehmend digitalisierte Zukunft steuern und für die Erreichung von Umweltzielen relevant werden können. Solche Anwendungen sind – wie vielfach beschrieben – keine neutralen Instrumente, sondern stets in gewisser Weise tendenziös: Sie können unterschiedliche Werte, Ziele oder Präferenzen priorisieren und im Ergebnis zu einer grünen Transformation beitragen oder stattdessen umweltschädliche Wachstumsmuster verstärken. Daten sind der maßgebliche Input-Faktor für diese Anwendungen. . Daher liegt es nahe, dass ein konkretes Verständnis der Datensouveränität und die unterschiedlichen Rechte, Anreizstrukturen und

[13] S.u. S. 29 ff.

Handlungslogiken, die mit einem solchen einhergehen, eine prägende Rolle dabei spielen, welche Werte oder Ziele sich in der digitalen Transformation durchsetzen.

Konkreter können Auswirkungen eines bestimmten Verständnisses von Datensouveränität auf Nachhaltigkeitsziele im Hinblick auf mindestens zwei unterschiedliche Wirkungsdimensionen von Daten auf Einsatz und Funktionsweise datengetriebener Assistenten abgeschätzt werden.

Einerseits sind Zugang zu und Entscheidungsrechte über Daten zentral für die Frage, ob digitale Anwendungen oder Assistenten im Einklang oder im Widerspruch mit Umweltzielen funktionieren, weil sie die Gestaltungsmacht spezifischer Akteure als Entwickler, Anbieter und Verwender datengetriebener Anwendungen stärken. **Datensouveränität, als Recht zur Entscheidung über das „Ob", „wie" und „durch wen" der Nutzung von Daten beinhaltet auch die Freiheit, über die Zwecke datengetriebener Anwendungen im Einklang mit Umweltzielen zu entscheiden.** Eine Untersuchung der vorliegenden Frage hat sich also darauf konzentrieren, inwieweit es für die Umsetzung von Nachhaltigkeitszielen einen Unterschied macht, welchen Akteuren dieses Recht zugesprochen wird. Macht es also im konkreten Anwendungsfeld einen Unterschied, ob große, häufig transnationale Unternehmen aus Nachhaltigkeitssicht relevante Anwendungen entwickeln, ob diese auf ökonomische Akteure als Nutzer ausgerichtet sind, oder ob sie von öffentlichen oder zivilgesellschaftlichen Akteuren, initiiert, entwickelt, und genutzt werden?

Zweitens wird Datensouveränität in einer Welt datengetriebener Entscheidungsassistenten aber nicht nur als ein Faktor relevant, der die *aktive Gestaltungsmacht* spezifischer Akteure zur Entscheidung über die Datennutzung stärkt. Arbeiten zur Algorithmenethik oder zu verantwortungsvoller KI setzen sich seit längerem mit solchen automatisierten Entscheidungen auseinander, bei denen die Verantwortung für „falsche" Entscheidungen nicht mehr ohne weiteres menschlichen Akteuren zugeordnet werden kann, sondern auf einen defizitären Dateninput als Teil der „Lernumgebung" intelligenter Systeme zurückzuführen sind: Als data-biases in diesem Sinne werden v.a. Diskriminierungsrisiken verstanden, die entstehen, weil z.B. in der prädiktiven Polizeiarbeit bereits die Datengrundlage vorhergehende Diskriminierungen widerspiegelt, die dann durch algorithmenbasierte Entscheidungen fortgeführt und verstärkt werden (s. Gailhofer/Franke, 2021). Solche Entscheidungen widersprechen dann nicht

deshalb (sozialen) Nachhaltigkeitszielen, weil Designer, Entwickler oder Nutzer den Systemen bewusst andere Optimierungsziele vorgeben, sondern weil die Daten, auf deren Grundlage die entsprechenden Systeme lernen, vorhergegangenes normativ fragwürdiges Verhalten und die dieses Verhalten orientierenden, diskriminierenden Ziele oder Präferenzen widerspiegeln.

Nach alldem wird die Frage, wer ausgestattet mit welchen Datenrechten als Datensouverän zu betrachten ist, noch lange nicht obsolet. Vielmehr wird der „Datensouverän" umso mehr *passiv* zum orientierenden Maßstab der Entscheidungen intelligenter Systeme, als diese automatisch solche Entscheidungen treffen, die vormalig eben von natürlichen Personen getroffen wurden. Der „Datensouverän" wird zum normativ maßgebenden Faktor algorithmenbasierten Entscheidens, weil er der analoge Bezugspunkt seines digitalen Zwillings ist. Ein digitaler Zwilling ist die digitale Repräsentation, Nachbildung oder das Modell von analogen Personen (einschließlich ihrer Ideen), Organisationen, sozialen oder ökologischen Systemen und Prozessen. Ein persönlicher digitaler Zwilling (Personal Digital Twin, PDT) ist die virtuelle Version eines Individuums (einer natürlichen Person), die auf der Grundlage seiner digitalen Fußabdrücke erstellt wird (Nativi et. al., 2022). Seine Grundlage sind digitale Daten, die algorithmisch zusammengestellt und verarbeitet werden, um bestimmte Ziele zu erreichen oder Präferenzen zu optimieren.[14] Die Erhebung der Daten und deren Verarbeitung (einschließlich Anpassungen der Algorithmen) erfolgt zunehmend durch eine auf künstlicher Intelligenz basierende Darstellung und Simulation, die nicht vollständig überwacht und erklärt werden kann. Ein digitaler Zwilling lässt Diagnosen, Prognosen, Simulationen zum Verhalten, den Präferenzen und die Entwicklungstendenzen einer Bevölkerung bis hin zur Ebene des Einzelnen zu. Auf seiner Grundlage können automatisierte Vorschläge und Entscheidungen getroffen werden, die sich wiederum auf die analoge Welt auswirken, indem sie die menschliche Wahrnehmung strukturieren und begründen, oder unmittelbar genutzt werden, um menschliche Bedürfnisse zu

[14] Persönliche digitale Zwillinge (PDTs) werden in der Industrie bereits in großem Umfang eingesetzt, z. B. zur Erstellung von Verhaltensmodellen einzelner Kunden von Online-Diensten (Nativi et. al., 2022). In der Industrie sollen durch digitale Zwillinge die Auswirkungen von Änderungen an industriellen Systemen und Prozessen simuliert werden könne, ohne tatsächliche Störungen zu riskieren (https://www.computerwoche.de/a/was-ist-ein-digital-twin,3550133); mittlerweile werden digitale Zwillinge aber in allen denkbaren Kontexten diskutiert, etwa auch zur Simulation von Abläufen in der Smart City und in der natürlichen Umwelt (Blair, 2021)

befriedigen und individuelles Verhalten und gesellschaftliche Prozesse zu steuern.(s. hierzu a. Scholz et. al. 2022).

Ein Begriff der Datensouveränität wird sich zukünftig einerseits daran messen lassen müssen, ob er natürlichen Personen hinreichend Einfluss auf die bewusste Ausgestaltung ihres persönlichen digitalen Zwillings verleiht. Für die vorliegende Frage ist aber v.a. zentral, dass ein konkretes Verständnis von Datensouveränität ausschlaggebend dafür sein wird, welche Akteur(stypen), welche gesellschaftlichen Dimensionen und Dynamiken im digitalen Zwilling repräsentiert werden. Es wird einen großen Unterschied machen, ob sich die „Datenspuren", bzw. der „digitale Fußabdruck" von Konsument*innen oder Unternehmen, also von Akteuren, die mehr oder weniger rational individuelle Kosten-Nutzen-Kalküle verfolgen, als vorherrschendes Element des digitalen Zwillings etabliert, oder etwa die Verhaltensdaten von Akteuren, die sich in politische Debatten einbringen und ggf. sogar konkret an kollektiven Entscheidungen über die Ziele des Einsatzes datengetriebener Anwendungen partizipieren.

Abstrakter kann man sagen, dass spezifische Nutzungs- und Verwertungsrechte an Daten zu bestimmten Verwertungsdynamiken führen, die wiederum eine spezifische Verfasstheit des digitalen Zwillings bedingen. Anreize zur Produktion einseitiger Datenbestände können zu einer „repräsentativen Verzerrung" des digitalen Zwillings führen. Solche Verzerrungen wären dann aus sozial-ökologischer Sicht relevant, wenn Aspekte eines ökologischen Gemeinwohls im digitalen Zwilling unterrepräsentiert sind (sozial-ökologischer data-bias) (Gailhofer & Franke 2021).

Vor diesem Hintergrund können für die dargestellten Verständnisse individueller Datensouveränität eine Reihe von Rückschlüssen gezogen werden.

So könnte ein Verständnis von Datensouveränität, das im Sinne des hier zuerst angesprochenen, „negativen" Rechts auf informationelle Selbstbestimmung vor allem Verbraucher in ihrem alltäglichen Verhalten in digitalisierten Umwelten ermächtigen will, durchaus als Instrument zur Stärkung von Nachhaltigkeitszielen genutzt werden. Datensouveränität würde dann, als ein Teilaspekt einer Konsumentensouveränität, als ein Bündel von Rechten aufgeklärter Verbraucher zu begreifen, die durch die bewusste Kanalisierung

ihrer Datenspur etwa zielgenau Nachhaltigkeitsakteure stärken können.[15] Ein nachhaltiger digitaler Konsum aktualisiert den digitalen Zwilling zugleich mit Blick auf Verhaltensmuster und Präferenzen, die dazu beitragen könnten, dass algorithmenbasierte Entscheidungen, z.B. von Empfehlungsalgorithmen, Nachhaltigkeitsziele berücksichtigen. Ein solcher Ansatz steht im Einklang mit der stärker ökologischen Ausrichtung des Konsument*innenbildes auf europäischer Ebene, wie es z.B. im Entwurf einer neuen Verbraucherrechterichtlinie zum Ausdruck kommt.[16]

Wie oben dargestellt, wird die Relevanz eines Souveränitätsbegriffs, der diese datenspezifische Konsument*innensouveränität durch die Schaffung „negativer Rechte" auf informationelle Selbstbestimmung herstellen will, aber schon dadurch begrenzt, dass eine Vielzahl der relevanten Daten nicht personenbezogen sind und damit nicht (mehr) unter Entscheidungsrechte fallen, die durch das Datenschutzrecht vermittelt werden. Zudem wird ein, auch im Hinblick auf die eigene Datenspur sozial-ökologisch aufgeklärtes, Konsument*innenverhalten auch ein sehr hohes Maß an Informationen und ein weitreichendes Verständnis komplexer datenökonomischer Zusammenhänge erfordern. In diesem Sinne betont etwa die Datenethikkommission, dass der Einzelne durch Anzahl und Komplexität der ihm abverlangten Entscheidungen bezüglich einer datenschutzrechtlichen Einwilligung ebenso wie durch die Unabschätzbarkeit aller Auswirkungen einer Datenverarbeitung systematisch überfordert wird (Datenethikkommission 2019, 96). Was sich hier v.a. auf Auswirkungen auf die informationelle Selbstbestimmung des Einzelnen bezieht, muss umso mehr gelten, wenn im Sinne von Umweltzielen nicht „nur" die Folgen der hinterlassenen Datenspur für die Verbraucher selbst, sondern auch die für ein sozial-ökologisches Gemeinwohl berücksichtigt werden müssen.

[15] Z.B. erzielt die Kooperative TheGoodData erzielt monatlich durch die Daten von etwa 300 NutzerInnen einen Erlös von 1.100 Euro, der für einen gemeinnützigen Zweck gespendet wird, (Palmetshofer et.al., 2017, 25); natürlich können Verbraucher ihre datenschutzrechtliche Einwilligung aber auch so nutzen, dass sie z.B. bei ihrem Surfverhalten im Internet gemeinwohlorientierten Anbietern umfangreiche Nutzungsrechte übertragen, die datenschutzrechtliche Einwilligung bei großen Datenmonopolen aber unterlassen.

[16] Europäische Kommission, COM(2022) 143 final, Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Änderung der Richtlinien 2005/29/EG und 2011/83/EU hinsichtlich der Stärkung der Verbraucher für den ökologischen Wandel durch besseren Schutz gegen unlautere Praktiken und bessere Informationen

Schließlich ist zu berücksichtigen, dass Verbraucher*innen selbst, wo sie optimal informiert sind, häufig im Sinne des homo oeconomicus ihren Nutzen maximieren und sozial-ökologische Folgen dieses Handelns außer Acht lassen werden. Umweltökonomische Ansätze bieten, wie anderweitig vorgeschlagen (Gailhofer & Franke, 2021), gute Hinweise für eine solche Beurteilung.[17] Jüngere Studien liefern auch erste empirische Belege in diesem Sinne und zeigen etwa, dass selbst ökologisch eingestellte Verbraucher*innen kaum bereit sind, höhere Kosten für die Nutzung von weniger umwelt- und klimaschädlichen KI-Anwendungen zu akzeptieren. (König, Wurster & Sievert 2022). In gängigen Kontexten, in denen Verbraucher*innen mit ihren Daten für die Nutzung von digitalen Anwendungen oder Dienstleistungen „bezahlen", spricht daher wenig dafür, dass die ökologische Qualität dieser Anwendungen, oder die weitere (nachhaltige oder weniger nachhaltige) Nutzung der „bezahlten" Daten für die Kosten-Nutzen-Kalkulation der Verbraucher*innen eine große Rolle spielen.

Vergleichbare Überlegungen sind vor allem für die Beurteilung eines „eigentumsanalogen" Verständnisses von Datensouveränität relevant: Ein Verständnis datensouveräner Akteure als Träger primär ökonomischer Freiheiten bringt typischerweise eine zentrale Rolle von Datenmärkten und damit verbundenes Marktversagen bei der Zuordnung (Allokation) von Daten mit sich: „rationale" Akteure veräußern ihre Daten nach dem Prinzip der Gewinnmaximierung, Angebot und Nachfrage geben den Ausschlag dafür, welche Daten erhoben, verfeinert und ggf. Dritten zugänglich gemacht werden. Dieser Allokationsmechanismus stärkt zudem große, datenreiche Tech-Unternehmen. Deren technologischer Vorsprung, sowie datenökonomische Feedback- Netzwerk- und Skaleneffekte bringen es mit sich, dass diese regelmäßig eine attraktivere Gegenleistung für Daten werden liefern können (Gailhofer & Scherf 2019). Bei allen Bemühungen solcher Konzerne, beispielsweise auf erneuerbare Energien umzustellen, besteht wenig Raum für die Annahme, dass diese ihre Innovationen vorrangig im Sinne sozial-ökologischer Ziele, und weniger am Share-holder Value entwickeln und einsetzen (Clutton-Brock et. al. 2021). Öffentliche oder zivilgesellschaftliche Akteure, die typischerweise eine Datenverwendung im (ökologischen) Gemeinwohlinteresse anstreben, dürften demgegenüber vergleichsweise

[17] Danach orientieren sich Personen in ökonomischen Austauschverhältnissen am individuellen Nutzen und Kosten (I-preferences), während Auswirkungen ihres Verhaltens auf Dritte oder die Gesellschaft (we-preferences), Hansjürgens 2015.

schlechte Chancen haben, auf Datenmärkten um relevante Daten zu konkurrieren.

Das faktisch bedeutsame, „eigentumsanaloge" Verständnis von Datensouveränität hat auch Implikationen für den *digitalen Zwilling*: So führen ökonomische Anreize für die Erzeugung und das „Teilen" von Daten auf Datenmärkten zu einem Angebotsdefizit an Daten, die aus ökologischer Sicht besonders wichtig sind (ESA 2018, Gailhofer et. al., 2022). Ein digitaler Zwilling, der demgegenüber fast ausschließlich ökonomisch orientierte Verhaltensmuster, Handlungslogiken[18] und gesellschaftlichen Dynamiken repräsentiert, hat Folgen für die Funktionalität digitaler Anwendungen und Systeme. Es gibt zunehmende Anhaltspunkte dafür, dass eine „Private Sector AI" (Slee 2020) die Konsumpräferenzen, oder die Nutzenkalkulationen von privaten Unternehmen optimiert, ökologisch vor allem problematische Effekte generiert: So zeigen z.B. Untersuchungen von KI-Anwendungen von Smart Farming, dass diese, wenn sie auf der Basis von Trainingsdaten und in einem datenreichen Kontext ökonomisch starker, großer Industriebetriebe trainiert werden, in einem anderen Umfeld (z. B. einem kleinen Bauernhof) zu fehlerhaften und schädlichen Ergebnissen führen können (Galaz et. al. 2021). KI-basierte Applikationen zur *„predictive maintenance"* komplexer Industrie-Anlagen könnten zu erheblichen Ressourceneinsparungen führen, indem diese die Nutzungszeit von Verschleißteilen optimiert. Hierfür bedarf es jedoch der Optimierung der Anwendungen am Ziel der Ressourceneinsparung. Sofern solche Systeme dagegen im Sinne ökonomischer Präferenzen eingesetzt werden, Instandhaltungskosten einzusparen oder verschleißbedingte Ausfälle zu vermeiden, sind im Vergleich höhere Umweltbelastungen zu beobachten (Carlson & Sakao 2020, s.a. Gailhofer & Franke 2021)

Schließlich steht insbesondere ein „eigentumsanaloges" Souveränitätsverständnis auch in einem Spannungsverhältnis sowohl zu einer öffentlichen Datensouveränität und einem sozial-ökologisch informierten Begriff digitaler Konsumentensouveränität. Denn deren Ziel, durch den Zugang zu Daten eine am Gemeinwohl ausgerichtete Gestaltungsmacht zu stärken wird durch exklusive Datenrechte naturgemäß beschränkt. Regulierungsvorschläge und nachhaltige Anwendungsoptionen für datengetriebene Technologien, wie z.B.

[18] Vgl.. etwa https://dlt.mobi/web3-infrastructure/: [T]he controller of the SSDT [Self Sovereign Digital Twin™] can participate as an autonomous economic agent in trusted transactions through issuing VCs and Verifiable Presentations (VPs).

der digitale Produktpass, haben generell damit zu kämpfen, dass aus rechtlichen oder tatsächlichen Gründen der Zugang zu relevanten, privat gehaltenen Daten fehlt. Eine Stärkung exklusiver Rechte im Sinne eines eigentumsanalogen Verständnisses von Datensouveränität würde diese Probleme weiter verschärfen.[19]

Ein Verständnis von Datensouveränität als bürgerliche Gestaltungskompetenz könnte in mehrfacher Hinsicht Defizite vorherrschender Begriffe beseitigen. Zunächst geht mit einem bürgerlichen Datenrechtsverständnis naturgemäß ein Wechsel der Souveränitätssubjekte einher. Es soll ganz vorrangig dem einseitigen Diktat der unternehmerischen Geschäftsmodelle und „willkürlichen Sichzueigenmachen der Bürgerdaten im Wege einer tatsächlichen Gestaltungsmacht durch die Datenunternehmen" entgegenwirken und eine „Gegenmacht als bürgerliche Vetoposition" schaffen (Fezer 2018). Der Datensouverän, dessen Präferenzen und Bedürfnisse in einem *digitalen Zwilling* repräsentiert und stetig aktualisiert werden, ist nach diesem Begriff kein homo-oeconomicus, der ausschließlich seinen individuellen Nutzen maximiert, sondern ein „homo politicus", der über die Ziele und Risiken der Datennutzung in zivilgesellschaftlichen Diskursen deliberiert und dadurch an der „Art und Weise der Organisation des Datengeschehens" mitwirkt.

Zum anderen soll die Institutionalisierung von Datenrechten und ihrer Ausübung die Möglichkeit kollektiver oder repräsentativer Entscheidungen in bestimmten Verfahren eröffnen. Dadurch sollen gerade auch die praktischen Probleme, die exklusive Verfügungsrechte aufwerfen – wie die Unsummen der generierten Daten, die Unüberschaubarkeit deren Vernetzung und die Unpraktikabilität einer isolierten Rechtewahrnehmung (Fezer 2018, 72) – und die normativen Herausforderungen, die aus Datenmärkten folgen, durch eine zentralisierte Verwaltungsstruktur gelöst werden. Ein Verständnis von Datensouveränität als bürgerliche Gestaltungskompetenz ist damit darauf angelegt, gerade auch solche Ziele und Wertorientierungen in die Dynamiken der Datenverwertung

[19] Auch die Grenzen, die ein persönlichkeitsrechtliches Souveränitätsverständnis für wünschenswerte Nutzungen von Daten darstellt, werden verschiedentlich betont. So erschwerten die Vorgaben des Datenschutzrechts, z.B. die formalen Vorgaben an die Einwilligung, insbesondere aber auch Regelungen zur Löschung, Widerruf und Datenportabilität wünschenswerte Datennutzungen im Gemeinwohlsinne. Dass diese Probleme durch entsprechende Regelungen im Data Governance Act nicht angegangen würden, belaste entsprechende Modelle altruistischen Datenteilens, s. Veil https://www.cr-online.de/blog/2021/10/28/data-governance-act-iii-datenaltruismus/.

einspeisen, die Einzelinteressen oder individuellen Präferenzen der Datenproduzenten übergeordnet sind (z. Ganzen s. Gailhofer & Scherf 2019)

Zentral problematisieren damit die entsprechenden Vorschläge die systematische Vernachlässigung von Gemeinwohlaspekten durch ökonomische Allokationsmechanismen wie Datenmärkte; Entscheidungsrechte an Daten sollen so zugeordnet und verfahrensmäßig organisiert werden, dass kollidierende Nutzungszwecke und -interessen politisch ausgehandelt und (grund-)rechtliche Vorgaben bei der Datennutzung berücksichtigt werden. Im Hinblick auf Umweltziele sollen also die Verwertungsdynamiken der Datenökonomie also politisiert und damit besser an Maßstäben des (ökologischen) Gemeinwohls ausgerichtet werden (Gailhofer et. al. 2022).

Nachhaltigkeitsorientierte Ausgestaltung von Datensouveränität

Die bisherige Analyse hat gezeigt, dass das Verhältnis zwischen Datensouveränität und Nachhaltigkeit ambivalent ist. Unterschiedliche, teils gegenläufige Interpretationen von Datensouveränität sind mit Nachhaltigkeitszielen mal mehr, mal weniger kompatibel. Entscheidend ist, dass die Herstellung von Datensouveränität nicht automatisch zu sozialen oder ökologischen Ergebnissen führt, sondern einer nachhaltigkeitsorientierten Ausgestaltung bedarf, mit dem Ziel einer produktiven Verknüpfung öffentlicher und privater Handlungsbeiträge. Dies verlangt die staatlich-hoheitliche Integration von Nachhaltigkeitsbelangen in die „Datenrechtsordnung“ und ihre Durchsetzung auf der einen Seite, Freisetzung der dezentralen gesellschaftlichen Kräfte zur Mitwirkung am Gemeinwohl auf der anderen. Damit sind Zusammenspiel und Wechselbezüglichkeit individueller und öffentlicher Datensouveränität angesprochen.

Zusammenspiel und Wechselbezüglichkeit individueller und öffentlicher Datensouveränität

Aus einer klassisch liberalen Perspektive[20] stehen individuelle und öffentliche Datensouveränität zunächst in einem Spannungsverhältnis. Öffentliche Datensouveränität verlangt eine (nachhaltigkeitsbezogene) Gestaltung der Digitalisierung im öffentlichen Interesse, die mit individuellen Freiheiten kollidieren kann und wird. So beschränken verbindliche Vorgaben zur Bereitstellung und Nutzung bestimmter Daten die Freiheit der Dateninhaber, mit diesen Daten nach ihrem eigenen Belieben zu verfahren. Auf der anderen Seite kann eine nachhaltigkeitsorientierte Ausgestaltung individueller Datensouveränität die Bürger*innen aber auch zur Mitwirkung am Gemeinwesen befähigen und zu informierten eigenen Entscheidungen ermächtigen (siehe oben,S. 13 ff.). In dieser Hinsicht führt Regulierung – als Ausübung öffentlicher Datensouveränität – zu einem Freiheits- und Souveränitätsgewinn des oder der Einzelnen, indem sie neue Handlungs- und Gestaltungsmöglichkeiten eröffnet, die das „freie Spiel der Kräfte" nicht gewährleisten würde.

Darin kommt eine Wechselbezüglichkeit öffentlicher und individueller Datensouveränität zum Ausdruck, die in der besonderen sozialen Bedeutung von Daten für die Gestaltung des Gemeinwesens begründet liegt und die bereits im berühmten „Volkszählungsurteil" anklingt, mit dem das Bundesverfassungsgericht das Recht auf informationelle Selbstbestimmung begründete:[21]

> „Der Einzelne hat *nicht ein Recht im Sinne einer absoluten, uneinschränkbaren Herrschaft über „seine" Daten*; er ist vielmehr eine sich innerhalb der sozialen Gemeinschaft entfaltende, auf Kommunikation angewiesene Persönlichkeit. Information, auch soweit sie personenbezogen ist, stellt ein *Abbild sozialer Realität* dar, das nicht ausschließlich dem Betroffenen allein zugeordnet werden kann. Das Grundgesetz hat (…) die Spannung Individuum - Gemeinschaft im Sinne der *Gemeinschaftsbezogenheit und Gemeinschaftsgebundenheit der Person* entschieden."

[20] Eine solche betont die individuelle Freiheit vom Staat, fokussiert auf die Grundrechte als Abwehrrechte und postuliert eine weitreichende Trennung staatlicher und gesellschaftlicher Sphäre, dazu die Darstellung bei Grimm (1994), S. 615 ff.

[21] BVerfG, Urt. v. 15.12.1983, 1 BvR 209/83, Rn. 148 = BVerfGE 65, 1 (43 f.), Hervorhebungen von uns.

Diese Ausführungen aus dem Jahr 1983 entstammen einer Zeit, in der das heutige Ausmaß und die Allgegenwärtigkeit der Erhebung und Verarbeitung von Daten noch nicht absehbar waren. In der Entscheidung ging es um die Abwehr einer – im konkreten Fall weitgehend zulässigen – einzelnen staatlichen Erhebung personenbezogener Daten, nicht um die heute notwendige umfassende Gestaltung einer Datengesellschaft und -ökonomie, die sowohl personenbezogene als auch nicht personenbezogene Daten umfasst. Gleichwohl enthält die zitierte Urteilspassage Aussagen, die für die gegenwärtigen Herausforderungen und den Diskurs um Datensouveränität weiterhin gültig und wichtig sind.

Dies gilt zunächst für die Absage an ein absolutes Herrschaftsrecht des oder der Einzelnen – auch (individuelle) Datensouveränität ist von vornherein nicht als Recht auf eine beliebige privatautonome Entscheidung über den Ausschluss von der Datennutzung zu verstehen. Dass das Bundesverfassungsgericht die normative Zuordnung („seine" Daten) zudem in Anführungszeichen setzt, verweist zudem auf die grundsätzliche Schwierigkeit, Daten einer bestimmten einzelnen Person zuzuordnen. Dies ist im Hinblick auf die unmittelbare Erhebung personenbezogener Daten, wie sie der Entscheidung zugrunde lagen, sogar noch vergleichsweise unproblematisch. Weitaus grundsätzlicher stellt sich die Frage unter den heutigen Bedingungen, in denen private Unternehmen unvorstellbare Mengen von Daten im öffentlichen Raum erheben und als Geschäftsgeheimnisse privatisieren (Zuboff, 2019, S. 128 ff.). Diese Daten sind teilweise personenbezogen, teils nicht, häufig sind sie verhaltensgeneriert, also erst durch die Nutzer*innen von Endgeräten geschaffen. Wem „gehören" diese Daten also? Den Unternehmen, die sie faktisch beherrschen, den Nutzer*innen, die sie generieren, oder der Öffentlichkeit, die sie betreffen? In der Diskussion und auch als Ausgangspunkt regulatorischer Abwägungen sollte nicht vorschnell die erste Variante zugrunde gelegt werden.

Für den Zusammenhang zwischen Datensouveränität und Nachhaltigkeit zentral ist auch die weitere Aussage des Bundesverfassungsgerichts, Daten seien ein „Abbild sozialer Realität". Diese Erkenntnis gilt nicht nur fort, sondern ist zu erweitern – Daten sind heutzutage nicht nur Abbild, sondern ganz wesentlich Gestaltungsmittel sozialer Realität (Viljoen, 2021). Wer zu welchen Zwecken Zugriff auf welche Daten hat, entscheidet darüber, wie die Verarbeitung dieser Daten (z.B. durch algorithmische Entscheidungen) Einfluss auf das Verhalten der Menschen hat. Es macht ersichtlich einen erheblichen Unterschied, ob beispielsweise die in der „Smart City" anfallenden Bewegungsdaten von einem

Privatunternehmen kontrolliert werden, das sie an Werbekunden verkauft, oder ob die Daten im öffentlichen Interesse für nachhaltige Mobilitätskonzepte verwendet werden.

Sowohl die gesamtgesellschaftliche Bedeutung von Daten als auch ihr kommerzieller Wert resultieren zudem maßgeblich aus der Zusammenführung und Kategorisierung einer Vielzahl von Daten, die durch das untereinander abgeglichene Verhalten zahlreicher Personen dezentral erzeugt werden (Viljoen, 2021, S. 609 ff.). Der spezifische Wert dieser Daten resultiert mithin aus der vom Bundesverfassungsgericht betonten „Gemeinschaftsbezogenheit und Gemeinschaftsgebundenheit der Person". Dies ist ein Argument sowohl für die Regulierung und Nutzung von Daten im öffentlichen Interesse als Ausprägung öffentlicher Datensouveränität als auch für die Beteiligung und Einbindung der Bürger*innen als Ausprägung individueller Datensouveränität.

Zusammenfassend lässt sich festhalten, dass eine nachhaltigkeitsbezogene Ausgestaltung von Datensouveränität angesichts der besonderen sozialen Bedeutung von Daten geboten ist und auch Einschränkungen individueller Herrschaftsrechte rechtfertigen kann – sowohl zugunsten staatlicher als auch gesellschaftlicher Handlungsmacht. Ausgewählte Ansätze für eine solche Ausgestaltung werden im Folgenden untersucht, wobei gegenwärtige Regulierungsbestrebungen der EU kritisch gewürdigt werden.

Datenzugangsrechte der öffentlichen Hand

Öffentliche Datenzugangsrechte ermöglichen der öffentlichen Hand insbesondere[22] den Zugriff auf private bzw. unternehmerische Datenbestände. Sie sind ein wichtiges Instrument zur Herstellung öffentlicher Datensouveränität, indem sie staatlichen Stellen das notwendige Regulierungswissen verschaffen und die Durchsetzung bestehender Vorgaben ermöglichen (siehe oben, S. 8 ff.).

Für den Zugriff auf von Privatunternehmen erhobene Daten stehen dem Staat verschiedene Instrumente zur Verfügung. Eine insbesondere im kommunalen Kontext interessante Option liegt darin, Pflichten zur Datenteilung mit der Vergabe öffentlicher Aufträge zu verbinden (Mozorov & Bria, 2018, S. 33 ff.;

[22] Der Zugriff auf die Daten anderer Behörden oder Hoheitsträger kann für die öffentliche Hand ebenfalls eine wichtige Rolle spielen, soll aber hier nicht im Vordergrund stehen. Datenübermittlungspflichten zwischen Behörden finden sich etwa für geologische Daten in §§ 9 ff. des Geologiedatengesetzes. Auch Open Data-Verpflichtungen der öffentlichen Hand kommen anderen Behörden zugute.

Piétron, Gailhofer & Sommer, 2022, S. 35). Öffentliche Auftraggeber können private Auftragnehmer im Rahmen der Ausschreibungsbedingungen vertraglich verpflichten, die im Rahmen des Auftrages anfallenden Daten mit bestimmten Behörden zu teilen oder sogar als Open Data bereitzustellen. Eine weitere Möglichkeit ist die ordnungsrechtliche Regelung, also die Festlegung von „Datenherausgabepflichten" als gesetzliche Pflicht. Bei deren Konzeption sind Gemeinwohl- bzw. Nachhaltigkeitsinteressen gegen das private – etwa als Geschäftsgeheimnis geschützte – Interesse an einer Zurückhaltung der Daten abzuwägen. Im Folgenden sollen derartige ordnungsrechtliche Pflichten im Vordergrund stehen, die sich in den derzeitigen Regulierungsbestrebungen der EU-Kommission wiederfinden.

Datenzugangsrechte der öffentlichen Hand im Entwurf eines Data Act

Datenzugangsrechte der öffentlichen Hand zu privat gehaltenen Daten sind im bisherigen Diskurs um eine Datenregulierung eher unterbelichtet. Während die öffentliche Hand im Rahmen der Open Data Gesetzgebung[23] mit guten Gründen auf eine verstärkte Transparenz und die Offenlegung der bei ihr vorhandenen Daten verpflichtet wird, sind die Anforderungen an den Informationsfluss umgekehrter Richtung weitaus schwächer ausgestaltet. Damit soll nicht suggeriert werden, dass Private allgemeinen und im Wesentlichen voraussetzungslosen Informationsbereitstellungspflichten unterworfen werden sollten, wie sie für die öffentliche Hand im Open-Data-Bereich gelten. Eine derart pauschale Verpflichtung wäre grundrechtlich kaum zu rechtfertigen und der Nutzen der resultierenden unüberschaubaren „Datenflut" mindestens zweifelhaft. Zielgerichtete und zweckgebundene Pflichten zur Datenherausgabe sind vor dem Hintergrund der Bedeutung einer ausreichenden Datengrundlage für eine wirksame Nachhaltigkeitspolitik hingegen grundsätzlich gut begründbar.

Erste Ansätze in eine solche Richtung enthält der Entwurf eines europäischen Datengesetzes (Data Act, DA-E), der den Anspruch formuliert, „einen fairen Datenzugang und eine faire Datennutzung" zu gewährleisten.[24] Zwar liegt der

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

[24] Europäische Kommission, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Datengesetz), 23.2.2022, COM(2022) 68 final.

Fokus des Entwurfs auf Datenbereitstellungspflichten gegenüber anderen Privaten, insbesondere können die Nutzer*innen datenerzeugender Produkte und Dienste Zugang für sich selbst sowie die Weitergabe an Dritte verlangen (vgl. Art. 4 f., 8 ff. DA-E).[25] Doch auch für öffentliche Stellen ist ein Datenzugangsrecht vorgesehen, das an die Voraussetzung einer „außergewöhnlichen Notwendigkeit" geknüpft ist, bei deren Vorliegen die Verordnung das öffentliche Interesse am Datenzugang höher gewichtet als das private Interesse an der Zurückhaltung der Daten (Art. 14 ff. DA-E).

Eine solche „außergewöhnliche Notwendigkeit" ist zunächst gegeben, wenn Daten zur Bewältigung eines öffentlichen Notstands erforderlich sind (Art. 15 lit. a) DA-E). Die Erwägungsgründe nennen hier beispielhaft Notlagen im Bereich der öffentlichen Gesundheit oder Naturkatastrophen.[26] Darüber hinaus können Daten auch präventiv zur Verhinderung eines öffentlichen Notstands oder nachlaufend zu dessen Bewältigung eingefordert werden, beides allerdings nur zeitlich befristet (Art. 15 lit. b) DA-E). Schließlich besteht ein Zugangsrecht einer öffentlichen Stelle auch dann, wenn diese anderenfalls daran gehindert wäre, eine bestimmte, gesetzlich ausdrücklich vorgesehene Aufgabe im öffentlichen Interesse zu erfüllen und die Daten nicht auf andere Weise – insbesondere durch Erwerb auf dem Markt zu Marktpreisen oder den Erlass entsprechender Rechtsvorschriften – beschafft werden können (Art. 15 lit. c) DA-E).[27] Stets müssen die öffentlichen Stellen personenbezogene Daten und Geschäftsgeheimnisse schützen (Art. 19 DA-E)[28] und – soweit es nicht um die akute Bewältigung eines öffentlichen Notstandes geht – einen finanziellen Ausgleich zahlen (Art. 20 DA-E). Granularität und Umfang der verlangten Daten müssen mit Blick auf den verfolgten Zweck stets verhältnismäßig sein (Art. 17 Abs. 2 lit. b) DA-E).

[25] Siehe dazu noch unten, S. 28 ff.

[26] Erwägungsgrund (57) DA-E.

[27] Besteht eine andere Beschaffungsmöglichkeit, ist eine Verpflichtung aufgrund der genannten Vorschrift dennoch möglich, sofern sie den Datenaufwand bei den bereitstellenden oder anderen Unternehmen erheblich verringert. Diese Rückausnahme dürfte aber wohl von eher untergeordneter Bedeutung sein.

[28] Ergänzt wird dieser Schutz um das an öffentliche Stellen gerichtete Verbot, die erhaltenen Daten als Open Data bereitzustellen (Art. 17 Abs. 3 DA-E).

Kritische Würdigung

Die praktische Bedeutung des beschriebenen „Backup"-Zugangsrechts (von Grafenstein, 2022, S. 27 f.) der öffentlichen Hand dürfte bei derzeitiger Ausgestaltung begrenzt sein. Zwar sind die Datenzugangsrechte der öffentlichen Hand nicht auf akute Notstandssituationen beschränkt, sondern können auch vor oder nach solchen Notlagen zur Anwendung kommen. Jedoch legt die Notwendigkeit der Befristung des Zugangs nahe, dass es auch in diesem Zusammenhang wohl nur um singuläre Ereignisse gehen soll, nicht aber z.B. um allgemeinere Präventionsaufgaben, wie sie insbesondere bei der Bekämpfung des Klimawandels dauerhaft notwendig sind.[29] Auf den ersten Blick weitreichend erscheint die Möglichkeit, Daten zur Erfüllung einer bestimmten gesetzlichen Aufgabe im öffentlichen Interesse herauszuverlangen, zumal die Aufgabe nicht einmal von besonders hohem Gewicht sein muss.[30] Allerdings verlangt der Wortlaut des Verordnungsentwurfes, dass die öffentliche Stelle ohne Datenzugriff an der Erfüllung der jeweiligen Aufgabe „gehindert" und nicht etwa bloß (stark) beeinträchtigt wäre. Zudem dürfte der Vorbehalt, dass die Daten nicht anderweitig und insbesondere nicht auf dem Markt zu Marktpreisen beschafft werden können, die praktische Bedeutung der Vorschrift deutlich begrenzen. Immerhin erscheint es aber plausibel, dass die im Hintergrund drohende hoheitliche Verpflichtung die Bereitschaft privater Unternehmen erhöht, der öffentlichen Hand überhaupt Daten bereitzustellen.

Aus Nachhaltigkeitsperspektive sollte die Datensouveränität der öffentlichen Hand angesichts der umfassenden Transformationsaufgaben und der „Datenüberlegenheit" des Privatsektors weiter gestärkt werden. Beispielsweise ist angesichts der fortschreitenden Klimakrise die nachhaltige und zügige Umgestaltung ganzer Sektoren (z.B. Verkehr und Landwirtschaft) notwendig, die auf eine umfassende Datengrundlage angewiesen ist. Dies dient zwar nicht der Verhütung konkret absehbarer singulärer Katastrophen, ist aber zwingend erforderlich, wenn Häufigkeit und Ausmaß derartiger Katastrophen global auf ein vertretbares Maß (konkretisiert durch die Temperaturziele des Pariser Abkommens) reduziert werden sollen. Angesichts der immer weiter

[29] Dafür spricht auch Erwägungsgrund (57) DA-E, der als Beispiel große Naturkatastrophen, die durch den Klimawandel verschärft werden nennt, aber eben nicht den Klimawandel selbst.

[30] Erwägungsgrund (58) DA-E nennt als Beispiel die rechtzeitige Erstellung einer amtlichen Statistik.

zunehmenden Dringlichkeit sowie der globalen Bedrohung hochrangiger Rechtsgüter wären weitergehende Zugangsrechte der öffentlichen Hand rechtlich zulässig, die Individualrechte (oder: die individuelle Datensouveränität) der betroffenen Unternehmen müssten in der Abwägung zurückstehen. Dies gilt jedenfalls, wenn – wie in Art. 19 DA-E vorgesehen – der Datenzugang zweckgebunden und der Schutz personenbezogener Daten und von Geschäftsgeheimnisse ausreichend gewährleistet ist. Bei der Abwägung ist auch zu bedenken, dass eine rasche und effektive Transformation gerade auch im Interesse der im jeweiligen Sektor tätigen Unternehmen liegt, damit später nicht deutlich härtere Maßnahmen notwendig werden.[31]

Vor diesem Hintergrund sollten Datenzugangsrechte der öffentlichen Hand gegenüber Privaten zielgerichtet gestärkt werden, soweit es um die nachhaltige Transformation der Wirtschaftsordnung geht. Dies ist im Rahmen horizontaler Regelwerke wie dem Data Act möglich, oder aber – möglicherweise treffsicherer – in sektoralen Regelungen und kann als Zugangsrecht auf Anfrage oder proaktive Veröffentlichungspflicht ausgestaltet sein. Ein Beispiel für eine sektorale proaktive Veröffentlichungspflicht sind die Neuregelungen in §§ 3a ff. des Personenbeförderungsgesetzes (PBefG), welche auch private Dienstleistungserbringer im öffentlichen Personenverkehr verpflichten, bestimmte Mobilitätsdaten über einen zentralen „Nationalen Zugangspunkt" verfügbar zu machen. Die Zugänglichmachung dieser Daten soll ausdrücklich auch Länder und Kommunen bei der Gestaltung eines klimafreundlicheren Verkehrs unterstützen und z.B. die Entwicklung datenbasierter, multimodaler Mobilitätsdienste weiter voranzutreiben (vgl. § 3b Abs. 1 Nr. 2 PBefG).[32] Derartige Regelungsansätze sind fortzuentwickeln und auszubauen; sowohl in sachlicher (weitere Sektoren) als auch persönlicher (weitere Akteure, z.B. Digitalkonzerne) Hinsicht.

Ermöglichung und Förderung zivilgesellschaftlicher Mitgestaltung

Wenn die gesellschaftlichen Kräfte für eine nachhaltig-digitale Transformation mobilisiert werden sollen, darf sich individuelle Datensouveränität nicht in der bloßen Abwehr von Eingriffen oder einem Eigentümerbelieben erschöpfen.

[31] In diesem Sinne auch der „Klimabeschluss", vgl. BVerfG, Beschluss vom 24.3.2022, 1 BvR 2656/18 u.a., Rn. 249 f.

[32] So die Gesetzesbegründung, BT-Drs. 19/26175, S. 38.

Notwendig ist vielmehr eine nachhaltigkeitsorientierte Ausgestaltung und institutionelle Einbettung individueller Handlungsmöglichkeiten, die eine zivilgesellschaftliche Mitgestaltung ermöglicht und fördert.[33]

Hierfür kommen grundsätzlich verschiedene Instrumente in Betracht. So können gemeinnützige Akteure einen privilegierten Zugang zu bestimmten Daten erhalten oder Anreize für eine Verwendung oder Bereitstellung von Daten zu Nachhaltigkeitszwecken geschaffen werden. Im Folgenden sollen zwei Regelungskomplexe aus den aktuellen Regulierungsvorschlägen der Europäischen Kommission näher betrachtet werden, die individuelle Datensouveränität ausgestalten. Dies sind zum einen die Regelungen im Data Act zu den Rechten von Nutzern bestimmter datenerzeugender Produkte, und zum anderen die Regelungen im Data Governance Act zu Datentreuhändern und insbesondere „datenaltruistischen Organisationen".

Neue Nutzer*innenrechte im Data Act

Der Data Act etabliert ein neues Datenrecht für die Nutzer*innen von Produkten, die in das sogenannte Internet der Dinge eingebunden sind. Als Beispiele nennt der Verordnungsentwurf „Fahrzeuge, Haushaltsgeräte und Konsumgüter, Medizin- und Gesundheitsprodukte oder landwirtschaftliche und industrielle Maschinen".[34] Das neue Datenrecht der Nutzer*innen beruht auf der Erwägung, dass die von derartigen Produkten generierten Daten nicht allein auf die (Entwicklungs-)Leistung des Herstellers, sondern eben auch auf die Nutzung des Produkts zurückzuführen sind. Das Datenrecht der Nutzer*innen tritt als „eingeschränktes Datenerzeugerrecht" (Piétron, Gailhofer & Sommer, 2022 [im Erscheinen], S. 35) daher neben das weiterhin bestehende Recht des Entwicklers oder der Herstellerin.[35]

Die Nutzer*innen haben nach dem Entwurf sowohl das Recht, die vom Produkt generierten Daten selbst einzusehen und zu nutzen, als auch die Befugnis, Dateninhaber*innen (d.h. Hersteller*innen und Entwickler*innen) anzuweisen, Daten an Dritte weiterzugeben (Art. 4, Art. 5 DA-E). Dabei haben die

[33] Siehe bereits oben, 0 und 0. Allgemein zur „Ermöglichungsfunktion" des Rechts vgl. Hoffmann-Riem (2016), S. 50.

[34] Erwägungsgrund (14) DA-E. Nicht erfasst sind hingegen Smartphones und andere Geräte, deren Hauptfunktion die Speicherung und Verarbeitung von Daten ist (Art. 2 Nr. 2 DA-E).

[35] Europäische Kommission, Vorschlag Data Act, COM(2022) 68 final, S. 16.

Nutzer*innen grundsätzlich das Recht frei zu bestimmen, für welchen Zweck sie die Daten verwenden bzw. inwieweit sie Dritten die Nutzung gestatten. Neben der Einhaltung des Datenschutzes und Vorgaben für den Schutz von Betriebs- und Geschäftsgeheimnissen gibt es vor allem die Vorgabe, dass weder Nutzer*innen noch Dritte die Daten nutzen dürfen, um Konkurrenzprodukte zu dem datenerzeugenden Produkt zu entwickeln (Art. 4 Abs. 4, Art. 6 Abs. 2 lit. d) DA-E). Eine Verwendung für Anschlussdienste (z.B. Reparatur und Wartung) ist hingegen zulässig und ausdrücklich erwünscht, auch in Konkurrenz zum Produkthersteller.[36] Die Nutzer*innen sind grundsätzlich auch darin frei, welchen Dritten sie ihre Daten zur Verfügung stellen. Eine Ausnahme gilt lediglich für „Gatekeeper" – große Digitalkonzerne wie Google, Facebook, Amazon & Co. –, denen die Daten nicht bereitgestellt werden dürfen (Art. 5 Abs. 2, Art. 6 Abs. 2 lit. d) DA-E).

Für die Bereitstellung von Daten an Dritte (nicht aber für die Bereitstellung gegenüber dem Nutzer) dürfen Dateninhaber*innen eine „angemessene Gegenleistung" verlangen. Ist der Dritte ein kleines oder mittleres Unternehmen (KMU), so darf diese Gegenleistung nicht höher sein als die Kosten, die unmittelbar mit der Datenbereitstellung verbunden sind (Art. 9 Abs. 2 DA-E). Dies soll verhindern, dass KMU übervorteilt werden und Wettbewerbsnachteile erleiden.

Datentreuhänder und „Datenaltruistische Organisationen" im Data Governance Act

Einzelne Regelungen im Vorschlag der Europäischen Union für ein Datengovernance-Gesetz können als erste Ideen dazu begriffen werden, wie den kollektiven oder „relationalen" Implikationen der Datennutzung durch die Schaffung von datenverwaltenden Institutionen oder Organisationen rechtlich Rechnung getragen werden kann. Der Entwurf für einen Daten-Governance-Act normiert Vorgaben für unterschiedliche Datenintermediäre. Datenaltruistische Organisationen sollen ausdrücklich zur Verfolgung von Zielen im allgemeinen Interesse gegründet werden können und die Datenspenden von Bürgern und Unternehmen unabhängig von kommerziellen Interessen verwalten.[37] Dadurch soll insbesondere ein höheres Maß an Vertrauen in die Datenbereitstellung

[36] Vgl. Europäische Kommission, Vorschlag Data Act, COM(2022) 68 final, S. 16, 18.

[37] Pietron, Gailhofer &Sommer (2022), 21.

gewährleistet und damit dazu beigetragen werden, dass mehr Daten von betroffenen Personen und Unternehmen zur Verfügung gestellt werden, um wiederum ein höheres Entwicklungs- und Forschungsniveau zu erreichen.[38]

Zugleich enthält der Vorschlag auch Regelungen zu kommerziellen Data-Sharing-Dienste, die das Vertrauen in die gemeinsame Nutzung personenbezogener und nicht personenbezogener Daten stärken und die Transaktionskosten im Zusammenhang mit B2B- und C2B-Datenaustausch mindern sollen (siehe die Begründung unter Punkt 5).[39] Auch diesbezüglich werden eine Reihe von Vorgaben geregelt, die die Fairness des Datenaustauschs sicherstellen sollen. Es bleibt aber abzuwarten, wie sich ein Nebeneinander von eigentumsanaloger und bürgerlicher Datensouveränität im Hinblick auf die dargestellten Probleme von Datenmärkten auswirken werden.

Kritische Würdigung

Die *Datenzugangsrechte im Data Act* sollen ausweislich der Begründung des Verordnungsentwurfs primär die Datenwirtschaft befördern und „Europa zu einem führenden Akteur der datenagilen Wirtschaft" machen.[40] Darin klingt vor allem die oben dargestellte geo- und industriepolitische Deutung öffentlicher Datensouveränität an, die häufig in enger Verbindung mit einem ökonomischen Verständnis individueller Datensouveränität steht (siehe oben, 0). Allerdings bricht der Data Act mit der bislang vorherrschenden Perspektive, dass produktgenerierte Daten ausschließlich den Herstellern zugewiesen sind und eröffnet durch Nutzer*innenrechte den Kreis derjenigen, die über die Verwendung der Daten bestimmen können. Damit gestaltet er individuelle Datensouveränität in einer Weise aus, die deutliche Parallelen zur Herleitung und Interpretation als „bürgerliche Gestaltungskompetenz" aufweist (siehe oben, 0).

Allerdings bleibt diese Gestaltungskompetenz im derzeitigen Regulierungsvorschlag beliebig, sie wird nicht im Interesse einer gemeinwohlorientierten und nachhaltigen Datennutzung gelenkt, sondern primär als Instrument für Marktoptimierung und Verbraucherschutz gesehen.[41]

[38] S. den Vorschlag für einen europäischen Daten-Governance Act, COM(2020) 767 final, 6; s.a. schon Gailhofer & Franke, ZUR 2021.

[39] V. Grafenstein, HHIG Discussion Paper Series 2022/2, 31.

[40] Europäische Kommission, Vorschlag Data Act, COM(2022) 68 final, S. 1.

[41] Vgl. Europäische Kommission, Vorschlag Data Act, COM(2022) 68 final, S. 16.

Nur vereinzelt klingt auch das Potential für (andere) Gemeinwohlbelange an, etwa dass die Mobilisierung der Daten des Privatsektors auch im Interesse von Klima-, Umwelt- und Ressourcenschutz erfolgt.[42] Etwas konkreter werden in den Erwägungsgründen verbesserte Reparatur- und Wartungsmöglichkeiten durch den Datenaustausch angesprochen[43] sowie darauf hingewiesen, dass die Nutzer*innen neben Unternehmen auch Forschungseinrichtungen oder gemeinnützige Organisationen mit Daten versorgen können.[44] Allein: privilegiert werden derartige Verwendungszwecke und Akteure bislang nicht. Dies sollte geändert werden, um die mit dem Data Act grundsätzlich überzeugend „geschaffene" digitale Souveränität der Nutzer*innen nachhaltigkeitsorientiert auszugestalten bzw. zu lenken (Piétron, Gailhofer & Sommer, 2022, S. 41). Fremd ist dem Data Act eine solche Vorgehensweise nicht: KMU werden, wie dargestellt, dadurch privilegiert, dass sie für Daten höchstens die Kosten der unmittelbaren Bereitstellung zahlen müssen (Art. 9 Abs. 2 DA-E). Diese Privilegierung auf gemeinnützige Organisationen und Forschungseinrichtungen auszuweiten wäre mindestens erforderlich; überzeugender wäre freilich eine Pflicht zur kostenfreien Bereitstellung gegenüber solchen Akteuren, weil und soweit sie mit der Nutzung der Daten keine Profitinteressen verfolgen. Privilegierungen wären ferner für bestimmte Verwendungszwecke – etwa die mehrfach angesprochene Reparatur – denkbar, hier kämen aber auch Einschränkungen in Betracht. Beispielsweise könnte die Bereitstellung von Daten für die Entwicklung bestimmter umwelt- und klimaschädlicher Produkte verboten werden.

Gemeinwohlorientierte Intermediäre, wie sie im Entwurf für den Datengovernance-Act erstmalig vorgeschlagen werden, könnten dabei helfen, neue Formen der Allokation von Daten zu erproben, die nicht in erster Linie auf ökonomische Anreize und Dynamiken bauen, sondern eine politische Auseinandersetzung und Mitbestimmung der Bürger*innen über die Zwecke und Rahmenbedingungen der Nutzung von Daten ermöglichen. Intermediäre können als Antwort auf unterschiedliche Probleme einer Ausübung individueller Datensouveränität betrachtet werden und stellen insbesondere eine Ausgestaltungsoption für ein partizipatives Souveränitätsverständnis dar: Sie können die bürgerliche Deliberation über legitime Zwecke und Rahmenbedingungen der Datennutzung organisieren, (rechtliche,

[42] Europäische Kommission, Vorschlag Data Act, COM(2022) 68 final, S. 8.

[43] Erwägungsgründe (14) und (19) DA-E.

[44] Erwägungsgrund (29) DA-E.

gesellschaftliche, ökologische, technologische) Risiken und Potenziale der Datennutzung eruieren und damit die gesellschaftliche Debatte über normative Rahmenbedingungen für die digitale Transformation strukturieren.[45] Soweit sie mit hinreichenden Mitteln ausgestattet werden, könnten Intermediäre auch die (kontinuierliche) Rechtskonformität der Datennutzung sicherstellen.

Allerdings ist es zweifelhaft, ob die Regelungen im Datengovernance-Act geeignet sind, eine echte Alternative im Sinn einer sozial-ökologisch ausgerichteten Datensouveränität zu etablieren. Datenaltruistische Organisationen stehen dort neben Vorgaben für ökonomisch ausgerichtete Intermediäre, die dazu beitragen sollen, Daten im Sinne ihrer Halter zu verwerten. Ob sich „altruistische" Handlungslogiken gegenüber damit parallel weiterhin bestehenden Datenmärkten in nennenswertem Umfang durchsetzen können, bleibt abzuwarten. Plausibler scheint die Annahme, dass insbesondere hochwertige Daten weiter auf Datenmärkten geteilt werden und ein altruistisches Datenteilen auf bestimmte Sektoren, Datentypen und Use-cases beschränkt bleibt. Dass Institutionen und Governance-Strukturen des Daten-Teilens auch eine echte Alternative zu vorherrschenden datenökonomischen Allokationsmechanismen darstellen können, um eine bürgerliche und öffentliche Datensouveränität zu etablieren, zeigen Vorschläge und Experimente auf kommunaler Ebene: So schlagen Pietron et. al. vor, dass Datenintermediäre wie Datentreuhänder oder Datengenossenschaften Daten im Auftrag ihrer Mitglieder, kommunaler Unternehmen oder ganzer Kommunen für einen bestimmten Bereich verwalten und vor dem unberechtigten Zugriff von staatlichen und privaten Akteuren schützen könnten. Datentreuhänder könnten beispielsweise als „kommunale Datenagentur", aber auch als Verein oder Genossenschaft ausgestaltet werden und Entscheidungen zur Verwendung und Zuordnung von Daten zu bestimmten Akteuren in einem repräsentativ-demokratischen Verfahren treffen (vgl. Piétron 2021, Pietron et. al. 2022).

[45] Digitale Tools können die partizipatorischen Ausgestaltung von Datenspenden erleichtern. Im Projekt „Decode" wird beispielsweise eine technische „Governance"-Lösung erprobt, die den Dateninput von Bürgern über eine App mit partizipativen Prozessen koppelt: Beispielsweise können Bürger „ihre" Daten für Großprojekte oder Verkehrsanwendungen zur Verfügung stellen, zu denen sie auch abgestimmt und mit anderen Stakeholdern diskutiert haben, vgl. https://decodeproject.eu/pilots.html.

Fazit und Ausblick

Die Europäische Kommission spricht zurecht von „twin challenges“: Die digitale Transformation wird ihr Versprechen, Wohlstand, Wohlbefinden und gesellschaftliche Entwicklung voranzubringen nicht einlösen, wenn sie sich nicht an Umweltzielen ausrichtet. Die grüne Transformation ist ohne wirksame nachhaltigkeitspolitische Steuerung der digitalen Transformation nicht zu haben.

Die entscheidende Frage, ob die mit diesen „twin challenges“ verbundenen Steuerungsaufgaben bewältigt werden können, darf als eine im eigentlichen Sinne politische verstanden werden: es geht darum, Mittel, Einfluss und Entscheidungsmacht derjenigen Akteure in der Digitalisierung zu stärken, die es mit der Entwicklung und Nutzung wirklich nachhaltiger Technologien ernst meinen. Entsprechend werden sich die sozial-ökologisch schädlichen Folgen digitaler Innovationsdynamiken und die Risiken digital verstärkter Wachstumsmuster nicht mindern lassen, wenn nicht der bisher vorherrschende Einfluss eben der Akteure gemindert wird, die diese Dynamiken anstoßen und von ihnen profitieren. Aber es geht nicht nur um Akteure, sondern auch darum, ob es gelingt, digitalökonomische und soziotechnische Rationalitäten und Anreizstrukturen mit Nachhaltigkeitszielen und den grund- und menschenrechtlich verbürgten, ökologischen Existenzbedingungen in Einklang zu bringen.

Diskurse um die Datensouveränität und deren rechtliche Ausgestaltung stehen im Zentrum dieser politischen Fragestellung. Denn die in diesen Diskursen konkurrierenden Begriffsverständnisse haben grundsätzliche Implikationen für die Nachhaltigkeit. Diese Nachhaltigkeitsimplikationen der Datensouveränität lassen sich unter zwei übergeordnete Kategorien fassen:

Erstens beinhaltet Datensouveränität, als Recht zur Entscheidung über das „Ob“, „wie“ und „durch wen“ der Nutzung von Daten auch die Freiheit, über die Zwecke

datengetriebener Anwendungen im Einklang mit Umweltzielen zu entscheiden. Der „Datensouverän" entscheidet also, solange und soweit menschliche Entscheidungen in den zunehmend automatisierten Umwelten der digitalen Transformation eine Rolle spielen, auch darüber, ob digitale Innovationen im Sinne der Nachhaltigkeitstransformation entwickelt und eingesetzt werden, oder nicht. Daraus folgt, dass es rechtspolitischen Ansätzen, die sich an den Zielen der grünen Transformation orientieren, in erster Linie um die Stärkung der Datensouveränität und damit um Datenzugangs- und -nutzungsrechte von Akteuren in Staat und Zivilgesellschaf stärken, die diese im Sinne des ökologischen Gemeinwohls einsetzen. Wird Datensouveränität dagegen wie bisher vor allem als *eigentumsanaloges Nutzungs- und Verwertungsrecht* verstanden, werden weiter vor allem Angebot und Nachfrage auf Datenmärkten darüber bestimmen, welche Akteure über Daten verfügen und damit auch über die Ziele der Datennutzung entscheiden. Nachhaltigkeitsziele bleiben, solange sie sich nicht in ökonomischen Werten niederschlagen, in solchen Dynamiken der Datenallokation außen vor.

Zweitens hat die Frage nach der Datensouveränität im Zeitalter Künstlicher Intelligenz und zunehmend automatisierter algorithmenbasierter Entscheidungen noch eine weitere Dimension: Die Frage, ob in Industrie oder Landwirtschaft, im individuellen Konsumverhalten oder in der kommunalen Planung ökologisch akzeptable Entscheidungen getroffen werden, wird in immer geringerem Umfang von bewusst handelnden, natürlichen Personen entschieden. Stattdessen prägen zunehmend digitale Assistenten menschliche Entscheidungen durch datengetriebene Informationen, Prognosen und Simulationen. In immer mehr Bereichen, ob im Smart Home, im autonomen Fahren, in der Industrie 4.0 oder in der automatisierten Verkehrssteuerung wird absehbar, dass menschliche Entscheidungen sogar vollständig durch solche Assistenten übernommen werden.

Die Bedingungen dafür, dass datengetriebene Assistenten – auch im sozial-ökologischen Sinne – ethische und auch ökologisch „verantwortungsvolle" Entscheidungen treffen, sind komplex und werden erst in jüngerer Zeit genauer untersucht. Schon heute kann aber mit guten Gründen angenommen werden, dass ein dominantes Verständnis von Datensouveränität in dieser Hinsicht wesentliche Auswirkungen haben wird. Denn die neuen Assistenten „lernen" und entwickeln ihre Vorhersagen, Vorschläge und Entscheidungen auf der Basis von digitalen Daten, die algorithmisch aggregiert und verarbeitet werden und

optimieren Zwecke und Präferenzen, die ihnen durch diese Datengrundlage – den „digitalen Zwilling" – vermittelt werden.

Auch unsere Konzeption des „Datensouveräns", als mit bestimmten Freiheiten und Ansprüchen ausgestatteter und nach bestimmten typischen Mustern sich verhaltender Akteur, fließt in die digitalen Umwelten ein, die wiederum die prägende „Lernumgebung" intelligenter Technologien bilden. Auch diesbezüglich wird die rechtlich und/oder technologisch regulierte Praxis im Kontext der Datensouveränität zu einer zentralen Stellschraube: es wird für die Funktionalitäten intelligenter Technologien einen großen Unterschied machen, ob unser „digitaler Zwilling" unsere Bedürfnisse und Prioritäten als Konsumenten oder Kosten-Nutzen-maximierende Marktteilnehmer widerspiegelt, oder die Datenspuren politisch deliberierender, am Gemeinwohl orientierter Bürger*innen. Dies bedeutet, dass ein Datensouveränitätsbegriff im Einklang mit den „twin challenges" Praktiken, Prozesse, Institutionen und Technologien fokussieren sollte, die partizipative, wertorientierte Entscheidungen unterstützen.

Die nachhaltigkeitspolitische Relevanz der Datensouveränität, das belegen die hier analysierten Regelungsvorschläge im Europäischen Data Act und dem Data Governance Act, wird politisch gesehen. Eine entschiedene Ausrichtung der vielbeschworenen, wertorientierten europäischen Datensouveränität an den Zielen der Grünen Transformation ist aber noch nicht erkennbar.

Literatur

Bauer, M. & Erixon, F. (2020). Europe's Quest for Technology Sovereignty: Opportunities and Pitfalls. Online verfügbar unter: https://ecipe.org/wp-content/uploads/2020/05/ECI_20_OccPaper_02_2020_Technology_LY02.pdf, zuletzt geprüft am 24.08.2022.

Beer, F., Räuchle, C., Schweitzer, E. & Piétron, D. (2021). Zukunftsfähige Daseinsvorsorge: Kommunen als Träger einer nachhaltig-digitalen Transformation. CO:DINA Positionspapier No. 8. Online verfügbar unter: https://codina-transformation.de/positionspapier-8-zukunftsfaehige_daseinsvorsorge/, zuletzt geprüft am 24.08.2022.

BMWi (2020). GAIA-X: Für ein digital souveränes Europa. Online verfügbar unter: https://www.bmwi.de/Redaktion/DE/Downloads/Monatsbericht/Monatsbericht-Themen/2020-09-im-fokus-gaia-x-fuer-ein-digital-souveraenes-europa.pdf?__blob=publicationFile&v=6, zuletzt geprüft am 24.08.2022.

Blair, G. S., (2021). Digital twins of the natural environment, Patterns 2 (10).

Clutton-Brock,P., Rolnick, D., Donti, P.L. & Kaack, L. (2021). Climate Change and AI. Recommendations for Government Action. Online verfügbar unter: https://www.gpai.ai/projects/climate-change-and-ai.pdf, zuletzt geprüft am 24.08.2022.

Bundesregierung (2021). Datenstrategie der Bundesregierung. Eine Innovationsstrategie für gesellschaftlichen Fortschritt und nachhaltiges Wachstum, Kabinettfassung, 27. Januar 2021. Online verfügbar unter: https://www.bundesregierung.de/breg-de/suche/datenstrategie-der-bundesregierung-1845632, zuletzt geprüft am 24.08.2022

Datenethikkommission, Gutachten der Datenethikkommission. Online verfügbar unter https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf?__blob=publicationFile&v=6, zuletzt geprüft am 31.08.2022.

Deutscher Ethikrat (2018), Stellungnahme Big Data und Gesundheit – Datensouveränität als informationelle Freiheitsgestaltung. Online verfügbar unter: https://www.ethikrat.org/fileadmin/Publikationen/Stellungnahmen/deutsch/stellungnahme-big-data-und-gesundheit.pdf, zuletzt geprüft am 31.08.2022.

Europäische Kommission (2020). Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen. Eine europäische Datenstrategie Eine Europäische Datenstrategie, COM(2020) 66 final. Online verfügbar unter: https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=COM:2020:0066:FIN, zuletzt geprüft am 24.08.2022.

ESA, Towards a European Artificial intelligence for Earth Observation (AI4EO) R&I Agenda, 2018. Online verfügbar unter: https://eo4society.esa.int/2018/09/19/towards-a-european-artificial-intelligence-for-earth-observation-ai4eo-ri-agenda/, zuletzt geprüft am 31.08.2022.

Fezer, K.-H. (2018). Repräsentatives Dateneigentum, Ein zivilgesellschaftliches Bürgerrecht, Stu-die im Auftrag der Konrad-Adenauer-Stiftung e. V. zum Thema „Einführung eines besonderen Rechts an Daten". Online verfügbar unter: https://www.kas.de/c/document_library/get_file?uuid=f828a351-a2f6-11c1-b720-1aa08eaccff9&groupId=252038, zuletzt geprüft am 31.8.2022.

Franke, J. (2021). Prinzipien der Datennutzung für ein sozial-ökologisches Berlin – Leitideen einer nachhaltigkeitsorientierten Datengovernance. Online verfügbar unter: https://ecornet.berlin/ergebnis/prinzipien-der-datennutzung-fuer-ein-sozial-oekologisches-berlin, zuletzt geprüft am 24.08.2022.

Franke, J. & Gailhofer, P. (2021). *Data Governance and Regulation for Sustainable Smart Cities.* In Frontiers in Sustainable Cities 3:763788. Online verfügbar unter: https://doi.org/10.3389/frsc.2021.763788, zuletzt geprüft am 24.08.2022.

Fritzsche, K., Pohle, J., Bauer, S., Haenel, F. & Eichbaum, F. (2022). Digitalisierung nachhaltig und souverän gestalten. CO:DINA Positionspapier No. 10. Online verfügbar unter: https://codina-transformation.de/wp-content/uploads/CODINA_Positionspapier_Digitale-Souvera%CC%88nita%CC%88t.pdf, zuletzt geprüft am 24.08.2022.

Gailhofer, P. (2021). Datenregulierung für ein nachhaltiges Berlin. Rechtspolitische Hintergründe für die szenarienbasierte Bewertung von Regulierungsansätzen (Wissen. Wandel. Berlin. Report Nr. 18). Berlin: Öko-Institut e.V., Forschungsverbund Ecornet Berlin

Gailhofer, P. & Scherf, C.-S. (2019). Regulierung der Datenökonomie. Ansätze einer ökologischen Positionierung, Öko-Institut Working Paper. Hg. v. Öko-Institut e.V. Online verfügbar unter https://www.oeko.de/fileadmin/oekodoc/WP-Datenregulierung.pdf, zuletzt geprüft am 31.08.2022.

Gailhofer, P. & Franke, J. (2021). Datenregulierung als sozial-ökologische Weichenstellung. Zeitschrift für Umweltrecht 32(10), 532–541.

Gailhofer, P., Franke, J., Gsell, M., Kollosche, I., Thomas, D., Stockhaus, H. & Best, A. (2022). Datengovernance und -regulierung für ein nachhaltiges Berlin – übergeordnete Erkenntnisse und Handlungsempfehlungen (Wissen. Wandel. Berlin. Report Nr.24). Berlin: Öko-Institut, UfU., IZT, Ecologic, Forschungsverbund Ecornet Berlin.

Galaz, V., Centeno, M.A., Callahan, P.W., Causevic, A., Patterson, T., Brass, I., Baum, S., Farber, D., Fischer, J., Garcia, D., McPhearson, T., Jimenez, D., King, B., Larcey, P. & Levy, K. (2022). Artificial intelligence, systemic risks, and sustainability, Technology in Society 67.

Grimm, D. (1994). Der Wandel der Staatsaufgaben und die Zukunft der Verfassung. In: Grimm, D. (Hrsg.), *Staatsaufgaben*, 1994, S. 613–646. Baden-Baden.

Hansjürgens, B (2015). Zur Neuen Ökonomie der Natur: Kritik und Gegenkritik, Wirtschaftsdienst 2015, 284–291.

Hoffmann-Riem, W. (2016). Innovation und Recht – Recht und Innovation. Mohr Siebeck.

Hummel, P., Braun, M. & Dabrock, P. (2019). Data Donations as Exercises of Sovereignty, in: Krutzinna, J. & Floridi, L. (eds.), The Ethics of Medical Data Donation, online verfügbar unter: https://link.springer.com/chapter/10.1007/978-3-030-04363-6_3, zuletzt geprüft am 31.8.2022.

König, P. D.,Wurster, S. & Sievert, M.D. (2022). Consumers are willing to pay a price for explainable, but not for green AI. Evidence from a choice-based conjoint analysis, Big Data & Society January 2022.

Morozov, E. & Bria, F. (2018). Rethinking the Smart City: Democratizing Urban Technology. Rosa-Luxemburg-Stiftung. Online verfügbar unter: https://www.rosalux.de/publikation/id/38134/die-smarte-stadt-neu-denken, zuletzt geprüft am 24.08.2022.

Nativi, S., Craglia, M. & Sciullo, L. (2022). MyDigitalTwin: Exploratory Research report, Publications Office of the European Union, Luxembourg, 2022, ISBN 978-92-76-53601-7, doi:10.2760/118634.

Palmetshofer, W., Semsrott, A. & Alberts, A. (2017). Der Wert persönlicher Daten. Ist Datenhandel der bessere Datenschutz? Studien und Gutachten im Auftrag des Sachverständigenrats für Verbraucherfragen Juni 2017.

Partnerschaft Deutschland (2020). Datensouveränität in der Smart City. Online verfügbar unter: https://www.pd-g.de/assets/Presse/Fachpresse/200213_PD-Impulse_Datensouveraenitaet_Smart_City.pdf, zuletzt geprüft am 24.08.2022.

Piétron, D., Gailhofer, P. & Sommer, F. (2022 [im Erscheinen]). Nachhaltige Daten-Governance in der Daseinsvorsorge.

Seidel, U. (2014). Das Grundrecht auf Datensouveränität, ZG 2014

Trute, H.-H. (1999). Verantwortungsteilung als Schlüsselbegriff eines sich verändernden Verhältnisses von öffentlichem und privatem Sektor. In G.F. Schuppert (Hrsg.), Jenseits von Privatisierung und „schlankem" Staat (S. 13–46). Nomos.

Viljoen, S. (2021). A Relational Theory for Data Governance. Yale Law Journal 131, 573–654.

von Grafenstein, M. (2022). Reconciling Conflicting Interests in Data through Data Governance. HIIG Discussion Paper 2022-02. Online verfügbar unter: https://www.hiig.de/publication/reconciling-conflicting-interests-in-data-through-data-governance-an-analytical-framework-and-a-brief-discussion-of-the-data-governance-act-draft-the-data-act-draft-the-ai-regulation-draft-as-wel/, zuletzt geprüft am 24.08.2022.

Voßkuhle, A. (2003). Beteiligung Privater an der Wahrnehmung öffentlicher Aufgaben und staatliche Verantwortung. Veröffentlichungen der Vereinigung der Deutschen Staatsrechtslehrer 62, 266–335.

Zuboff, S. (2019). The Age of Surveillance Capitalism: the fight for the future at the new frontier of power. Profile Books.

Über die Autor*innen

Dr. Johannes Franke

Unabhängiges Institut für Umweltfragen (UfU) e.V.

Dr. Johannes Franke ist Volljurist und ist am UfU im Fachbereich Umweltrecht & Partizipation tätig. Er arbeitet dort insbesondere zum Rechtsschutz in Umweltangelegenheiten sowie in verschiedenen Projekten an der Schnittstelle von Umweltrecht und Digitalisierung.

Dr. Peter Gailhofer

Öko-Institut e.V.

Dr. Peter Gailhofer ist Rechtsanwalt und berät für das Öko-Institut Akteure in Politik und Gesellschaft zu Fragen der umweltrechtlichen Regulierung und zur Stärkung und Durchsetzung ökologischer Menschenrechte, insbesondere im Kontext transnationalen Wirtschaftens. Seit längerem arbeitet er zudem zu ökologischen und umweltrechtlichen Implikationen von Künstlicher Intelligenz und Datenökonomie.

Über CO:DINA

Das Verbundvorhaben CO:DINA – Transformationsroadmap Digitalisierung und Nachhaltigkeit vernetzt Wissenschaft, Politik, Zivilgesellschaft und Wirtschaft, um neue strategische Stoßrichtungen für eine sozial-ökologische Digitalisierung zu identifizieren. Vielfalt in Denkweisen, Perspektiven und Erfahrungen ist die Voraussetzung, um die Komplexität der Digitalisierung besser zu verstehen und grundlegenden Fragen insbesondere zur Künstlichen Intelligenz mit tragfähigen Lösungsansätzen zu begegnen. Dabei entstehen Netzwerke zwischen Akteursgruppen, die bislang unzureichend verbunden waren. So wird die politische und gesellschaftliche Handlungsfähigkeit für einen sozial-ökologisch-digitalen Wandel gestärkt.

Das Vorhaben wird vom Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV) im Rahmen der KI-Leuchtturminitiative gefördert und gemeinsam vom IZT – Institut für Zukunftsstudien und Technologiebewertung und dem Wuppertal Institut für Klima, Umwelt, Energie umgesetzt.

Gefördert durch:

Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz

aufgrund eines Beschlusses des Deutschen Bundestages

Impressum

IZT – Institut für Zukunftsstudien und Technologiebewertung gemeinnützige GmbH
Schopenhauerstr. 26, 14129 Berlin
Tel.: +49 (0) 30 803088-0
Fax: +49 (0) 30 803088-88
E-Mail: info@izt.de
Internet: www.izt.de

Wuppertal Institut für Klima, Umwelt, Energie GmbH
Döppersberg 19, 42103 Wuppertal
Tel.: +49 (0) 202-2492-101
Fax: +49 (0) 202-2492-108
E-Mail: info@wupperinst.org
Internet: www.wupperinst.org

Weitere Veröffentlichungen unter:

www.codina-transformation.de