



# Digitalisierung nachhaltig und souverän gestalten

---

## Autor\*innen

Kerstin Fritzsche

Julia Pohle

Steffen Bauer

Fabio Haenel

Felix Eichbaum

## Kurz gesagt

Eine nachhaltige Gestaltung der Digitalisierung ist zentral für die sozial-ökologische Transformation. Welche Rolle die digitale Souveränität Deutschlands und Europas dafür spielt, wurde bislang jedoch noch nicht systematisch erforscht. Wie hängen digitale Souveränität und Nachhaltigkeit zusammen – und wo bestehen Potenziale für Synergien, aber auch Zielkonflikte?

## Inhaltsverzeichnis

1.	Die Digitalisierung nachhaltig und souverän gestalten .....	1
2.	Was ist digitale Souveränität? .....	4
2.1.	Diskurse in verschiedenen nationalen Kontexten .....	4
2.2.	Digitale Souveränität – eine Arbeitsdefinition .....	6
3.	Nexus aus digitaler Nachhaltigkeit, Souveränität und Resilienz.....	11
3.1.	Nachhaltige Digitalisierung.....	11
3.2.	Digitale Resilienz .....	13
3.3.	Zwischenfazit.....	15
4.	Digitale Souveränität und Nachhaltigkeit – Synergien und Zielkonflikte auf Ebene der EU.....	16
4.1.	Daten-Governance .....	18
4.2.	Plattformunternehmen.....	21
4.3.	Digitale Cloud-Infrastruktur.....	24
4.4.	Schlüsseltechnologien.....	26
4.4.1.	Halbleiter- und Mikrochip-Technik.....	27
4.4.2.	Künstliche Intelligenz .....	28
4.5.	IT- und Netzsicherheit .....	30
4.6.	Fazit.....	32
5.	Ausblick: Was sollte getan werden?.....	34
6.	Literatur.....	39
	Über die Autor*innen.....	45

## 1. Die Digitalisierung nachhaltig und souverän gestalten

Ohne eine klare Ausrichtung auf Nachhaltigkeit läuft die Digitalisierung Gefahr, zu einem „Brandbeschleuniger“ (WBGU 2019) nicht-nachhaltiger Wirtschafts- und Gesellschaftsmodelle zu werden. Gerade bei der digitalen Transformation bedeutet Nachhaltigkeit jedoch nicht allein die Berücksichtigung ökologischer Aspekte, wie z. B. den zunehmenden Energie- und Ressourcenverbrauch, die Nutzung von Rohstoffen, deren Abbau Umwelt- und Sozialstandards verletzt, oder wachsende Mengen an Elektroschrott. Auch gesellschaftliche Herausforderungen müssen für eine nachhaltige Gestaltung der Digitalisierung in den Blick genommen werden. Die Bandbreite reicht vom Beitrag sozialer Medien zu *Hate speech* und Desinformation im Netz, über die Abkopplung von Menschen, die mit dem digitalen Wandel nicht Schritt halten können, bis hin zu ethischen Fragestellungen bei der Nutzung Künstlicher Intelligenz (KI) und der Beeinflussung von Meinungen und Konsumverhalten durch die Dominanz globaler Plattformen. Die Rolle solcher marktbeherrschenden Plattformen für eine Transformation zu mehr Nachhaltigkeit ist bislang nicht einmal ansatzweise erschlossen (Ramesohl & Gunnemann 2021). Vor diesem Hintergrund gilt es im Hinblick auf eine wertebasierte Gestaltung der Digitalisierung beide Nachhaltigkeitsdimensionen – die ökologische wie die soziale – zu verschränken. Doch wie kann dies in einer globalisierten und hochgradig voneinander abhängigen Welt erfolgreich geschehen – insbesondere, solange die Digitalisierung von wenigen staatlichen und privatwirtschaftlichen Akteuren, vor allem internationalen Tech-Konzernen, vorangetrieben wird?

Seit einigen Jahren gewinnt der Begriff der „digitalen Souveränität“ in diesem Zusammenhang an Bedeutung. Spätestens seit dem Amtsantritt der europäischen Kommissionspräsidentin Ursula von der Leyen im Jahre 2019 ist die digitale bzw. technologische Selbstbestimmung zu einem Schlüsselthema der Europäischen Union (EU) avanciert und findet sich in zahlreichen offiziellen Dokumenten der Kommission und Reden ihrer Präsidentin wieder. Auch in Deutschland ist die digitale oder technologische Souveränität regelmäßig Gegenstand von Strategie- und Positionspapieren der Regierung wie auch wirtschaftlicher und gesellschaftlicher Akteure (Pohle 2020). Dabei wird auf nationaler wie europäischer Ebenen die Notwendigkeit der digitalen Selbstbestimmung vor allem mit der Abhängigkeit von Technologien anderer Länder, allen voran den USA und China, eine geringe Wettbewerbsfähigkeit

durch mangelnde Kapazitäten und Kompetenzen sowie eine damit verbundene hohe Verwundbarkeit der EU, ihrer Wirtschaft und ihrer Bürger\*innen begründet. Eine nur untergeordnete Rolle spielt dabei jedoch bislang die Frage, inwiefern eine souverän gestaltete Digitalisierung auch dazu beitragen kann, die Potenziale der Digitalisierung für den sozial-ökologischen Umbau von Wirtschaft und Gesellschaft zu heben und ihre negativen Konsequenzen für die Nachhaltigkeit zu begrenzen.<sup>1</sup>

Dies ist umso erstaunlicher, da sich die EU einerseits zum Ansatz einer *menschenzentrierten* und *wertebasierten*, das heißt an ethischen Normen und den Rechten des Individuums ausgerichteten Digitalisierung bekannt hat. Mit diesem Konzept positioniert sich die EU als Alternative zu dem US-amerikanischen marktliberalen und dem chinesischen regulativ-autoritären Modell der Digitalisierung. Zum anderen strebt die EU mit ihrem Green Deal die ökologische Ausrichtung der Wirtschaft der EU-Mitgliedsstaaten an und sieht dabei auch eine wesentliche Rolle für die Digitalisierung. Ergänzend dazu hat in Deutschland – nicht zuletzt durch die Umweltpolitische Digitalagenda des Bundesministeriums für Umwelt, Naturschutz und nukleare Sicherheit (BMU) aus dem Jahr 2020 – die Vorstellung einer umweltgerechten, ökologisch nachhaltigen Digitalisierung an Dynamik gewonnen.

In diesem Papier argumentieren wir, dass die beiden Transformationsdiskurse um Digitalisierung und Nachhaltigkeit auf nationaler wie europäischer Ebene inzwischen an verschiedenen Stellen zusammengeführt werden. Diese bleiben jedoch mit Fragen der digitalen Souveränität noch weitgehend unverbunden.<sup>2</sup> Forschung und Diskussion zu digitaler Nachhaltigkeit und digitaler Souveränität finden bislang zumeist losgelöst voneinander statt und haben thematisch wie personell nur wenige Überschneidungen.

---

<sup>1</sup> Lediglich die Fokusgruppe „Digitale Souveränität“ der Plattform „Innovative Digitalisierung der Wirtschaft“ beschäftigte sich in ihrem Papier „Digitale Souveränität und Resilienz: Voraussetzungen, Treiber und Maßnahmen für mehr Nachhaltigkeit“ (Bendig et al. 2020) mit dem Nexus aus digitaler Souveränität, Nachhaltigkeit und Resilienz.

<sup>2</sup> Selbst dort, wo das Konzept der digitalen Souveränität als Möglichkeit eines mobilisierenden politischen Narrativs verstanden wird, der fortschrittliche Digitalpolitik ermöglichen kann, werden Fragen der (insbes. ökologischen) Nachhaltigkeit wenig diskutiert (Falk & Schroeder 2022).

Allerdings ist eine nachhaltige Gestaltung der Digitalisierung ohne digitale Selbstbestimmung ebenso undenkbar, wie eine digitale Souveränität Europas, die sich nicht am Leitbild der Nachhaltigkeit orientiert. Die bestehende Lücke in Diskurs und Forschung zu digitaler Souveränität und Nachhaltigkeit soll das Verbundvorhaben „CO:DINA – Transformationsroadmap Digitalisierung und Nachhaltigkeit“ erkunden und mit einzelnen Forschungsbeiträgen adressieren.

Das vorliegende Papier nimmt als Grundlage dafür eine Positionsbestimmung vor und geht auf die folgenden Aspekte ein:

- **Begriffsklärung:** Wie kann digitale Souveränität – auch in Abgrenzung von ähnlichen Begrifflichkeiten – verstanden werden?
- **Exploration:** Wie hängen digitale Souveränität und die nachhaltige Gestaltung der Digitalisierung zusammen? Welcher Bezug besteht zu Fragen der digitalen Resilienz? Welche Vorhaben bestehen derzeit auf europäischer Ebene, um digitale Souveränität bzw. eine nachhaltige Digitalisierung voranzubringen?
- **Ausblick:** Welche Forschungsfragen können helfen, um den Zusammenhang zwischen digitaler Souveränität und Nachhaltigkeit noch besser zu verstehen?

Das Papier fokussiert sich überwiegend auf die Ebene der EU, da diese zentral für die Ausgestaltung der nationalen Digitalpolitiken ihrer Mitgliedsstaaten ist. Wo angebracht wird jedoch auch der deutsche Kontext eingehender betrachtet, da Deutschland ein zentraler Akteur in Bezug auf die nachhaltigkeitsorientierte Gestaltung der Digitalisierung auf europäischer Ebene ist.

## 2. Was ist digitale Souveränität?

### 2.1. Diskurse in verschiedenen nationalen Kontexten

Der Begriff der digitalen Souveränität hat in den letzten Jahren an Bedeutung gewonnen. Ursprünglich beriefen sich im Zusammenhang mit digitalen Technologien vor allem Länder wie China und Russland auf den Souveränitätsbegriff. Sie verbanden damit eine strenge Kontrolle des Cyberraums, was dazu beitrug, autokratische Strukturen auszubauen und freie Meinungsäußerung und etwaige demokratisierende Effekte durch das Internet zu unterdrücken. In den letzten Jahren wird das Konzept der digitalen Souveränität jedoch in den EU-Mitgliedsstaaten und anderen demokratischen Ländern zunehmend mit europäischen Werten und Zielen sowie universellen Grundrechten verbunden und ist damit Teil eines Gegenentwurfs zur amerikanischen und chinesischen Digitalökonomie (Pohle 2020).

Deutschland ist das Land in Europa, das den Diskurs derzeit am stärksten prägt, obwohl dieser dort erst seit den Snowden-Enthüllungen (2013) Form angenommen hat und damit später als in anderen Ländern. Durch die starke Betonung der digitalen Selbstbestimmungsfähigkeit von Individuen ist die aktuelle deutsche Debatte von der Abkehr von einem traditionellen Souveränitätsverständnis gekennzeichnet, wie es beispielsweise stärker noch in Frankreich herrscht, und unterliegt zudem einer stark normativ aufgeladenen Rechtfertigungslogik. Statt allein die Unabhängigkeit und Autorität des Staates im Digitalen zu betonen, wird digitale Souveränität als Voraussetzung dafür gesehen, den Prozess der digitalen Transformation mitzugestalten und im digitalen Raum selbstbestimmt handeln zu können, ohne dabei auf die Nutzung von ausländischer Technologie verzichten zu müssen. Dabei wird nicht nur die Souveränität des demokratischen Staates betont, sondern insbesondere auch die Autonomie und selbstbestimmte Handlungsfähigkeit des Bürgers in einer vernetzten Welt. Diese soll vor allem durch eine Stärkung von Digitalkompetenz und Nutzer\*innenrechten befördert werden.

Auf europäischer Ebene ist der Begriff der digitalen Souveränität eng mit einem sich wandelnden Selbstverständnis der EU verbunden. Mit ihrem Amtsantritt als Präsidentin der Europäischen Kommission formulierte Ursula von der Leyen eine geopolitische Agenda für die EU. Diese solle sich als normative Macht verstehen, welche ihre Souveränität durch eine erhöhte Außenwirkung in all ihren

Handlungsfeldern einfordern muss (Koenig 2019). Diese Ausrichtung ist als Reaktion auf die politischen Veränderungen des 21. Jahrhunderts zu verstehen, durch die die bisherige regelbasierte internationale Ordnung zunehmend in Frage gestellt wird. Zugleich verschiebt sich das internationale Machtgefüge von einer transatlantisch zu einer transpazifisch geprägten Ordnung. Die *geopolitische Wende* der EU-Kommission zeigt sich dabei insbesondere auch im Bereich der Digitalisierung und der Stärkung der europäischen digitalen Souveränität.

Ähnlich wie in Deutschland zeichnet sich die europäische Debatte durch eine stark normativ-aufgeladene Rechtfertigungslogik aus. Im Unterschied zur Debatte in Deutschland geht die Verwendung des Begriffs durch EU-Institutionen jedoch weniger in die Breite, da insbesondere die Handlungs- und Entscheidungsfähigkeit von Individuen weniger im Fokus steht. Stattdessen lässt sich mit Blick auf den europäischen Diskurs eine Vorliebe für alternative Begrifflichkeiten – bspw. *strategische Autonomie* und *technologische Souveränität* – und eine damit eng verknüpfte Fokussierung auf digitale Infrastrukturen und auf die Wettbewerbsfähigkeit der EU feststellen sowie eine sehr starke Kontinuität mit bestehenden Arbeitsprogrammen.

Edler et al. (2020) definieren technologische Souveränität als „die Fähigkeit eines Staates oder Staatenverbunds, die Technologien bereitzustellen, die er für sein Wohlergehen, seine Wettbewerbsfähigkeit und seine Handlungsfähigkeit als entscheidend erachtet, und die Fähigkeit, diese Technologien selbst zu entwickeln oder aus anderen Wirtschaftsräumen ohne einseitige strukturelle Abhängigkeiten zu beziehen“ (eigene Übersetzung). Technologische Souveränität ist damit nicht allein auf digitale Technologien beschränkt, wenngleich diese eine herausgehobene Rolle spielen, sondern umfasst auch andere als essenziell betrachtete Technologien. Als Mittel, um technologische Souveränität zu erreichen und Abhängigkeiten zu reduzieren, strebt die EU sowohl eine Förderung von Forschungskapazitäten und Wettbewerb an als auch den Aufbau von Infrastrukturen und die Stärkung von technologischen und wirtschaftlichen Schlüsselkompetenzen (EC 2020). Im Begriffsverständnis der EU ist dabei der Staat der entscheidende Akteur in der Herstellung und Sicherung technologischer Souveränität.

Das Verständnis von technologischer Souveränität ist auf EU-Ebene eng verbunden mit dem Konzept der strategischen Autonomie (Bauer & Erixon 2020). Dieses wurde 2016 in der „Globalen Strategie für die Außen- und Sicherheitspolitik“ (Bendiek 2016) der EU eingeführt und ähnelt dem oben

skizzierten Souveränitätsbegriff, betont jedoch deutlich stärker die Rolle von multilateralen Beziehungen und Partnerschaften (European External Action Service 2016, Lippert et al. 2019) wie auch sicherheits- und verteidigungspolitische Aspekte. Damit kann strategische Autonomie als eine Zutat für das Erreichen der technologischen Souveränität der EU und ihrer Mitgliedstaaten verstanden werden (Timmers 2019). Die Erfahrungen aus der Corona-Pandemie und der Wandel des geopolitischen Gefüges im Zusammenhang mit dem Krieg Russlands in der Ukraine haben der Diskussion um technologische Souveränität und strategische Souveränität in der EU neuen Schwung verliehen.

### **Box 1: Exkurs: Souveränität**

Der Begriff der Souveränität ist im allgemeinen Verständnis eng mit der Idee eines territorial begrenzten Nationalstaats verbunden. Demnach gilt ein Staat dann als souverän, wenn er – nach innen wie außen – politisch, wirtschaftlich und gesellschaftlich selbstbestimmt und unbeeinflusst von anderen Staaten agieren kann. Dabei ist der Begriff der Souveränität jedoch nicht mit Autarkie zu verwechseln, also der absoluten oder teilweisen Unabhängigkeit von anderen Staaten z. B. durch Selbstversorgung.

In einer engen Verflechtung mit anderen Staaten Souveränität zu bewahren, ist kein Widerspruch. Wichtig ist jedoch, dass diese Verflechtungen bewusst und nicht alternativlos eingegangen werden, sondern aus einem selbstbestimmten Abwägungs- und Entscheidungsprozess hervorgegangen sind und ein gewisses Maß an Handlungsfreiheit erlauben. Souveränität lässt sich damit allgemein als Selbstbestimmtheit verstehen.

## 2.2. Digitale Souveränität – eine Arbeitsdefinition

Diesem Positionspapier liegt ein breites und umfassendes Verständnis von digitaler Souveränität zu Grunde. Es versteht digitale Souveränität als „die Summe aller Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können“ (Goldacker 2017).

Wir sehen dabei drei Ebenen als zentral an: die staatliche Ebene, die Ebenen von Organisationen wie etwa öffentliche Einrichtungen oder Unternehmen sowie die Ebene des Individuums (siehe Abbildung 1).



Abbildung 1: Dimensionen digitaler Souveränität und Umsetzungsfelder (nach Pohle 2020)

Staatlichen Akteuren kommt bei der Gestaltung einer am Prinzip der digitalen Souveränität ausgerichteten Digitalpolitik eine besondere Rolle zu. So stellt der regulative Rahmen, der von Staaten oder einem Staatenverbund wie der EU für die Digitalisierung gesetzt wird, eine wichtige Voraussetzung für die Entwicklung und Ausübung digitaler Souveränität auf allen drei Ebenen dar. Dies hat vor allem mit drei globalen Trends und Dynamiken zu tun, die sich bis auf die individuelle Ebene der digitalen Souveränität auswirken:

- Zum einen hat **die technologische Hegemonie einiger weniger Staaten und Unternehmen** zu einem bislang nie gekannten Machtgefälle geführt:

Die materielle und immaterielle Macht über weite Teile der kritischen gesellschaftlichen und wirtschaftlichen Infrastruktur befindet sich heute in den Händen der Privatwirtschaft (Kapczynsk 2020). Diese entzieht sich – aufgrund rasanter Technologieentwicklung und der faktischen Exterritorialität multinationaler Tech-Konzerne – bislang weitgehend der staatlichen Regulierung. In den letzten Jahren hat jedoch die EU damit begonnen, diese Problematik durch eine Vielzahl von Regulierungsinitiativen im Bereich der Datennutzung, der KI sowie digitaler Plattformen und Dienstleistungen anzugehen. Jüngst hat zudem die Diskussion um die Produktion von Mikrochips in Europa an Dynamik gewonnen.

- Damit eng verbunden hat das Bewusstsein über **die Vulnerabilität digitaler, kritischer Infrastrukturen** gegenüber Eingriffen anderer Staaten zugenommen. Dazu beigetragen haben nicht zuletzt die Enthüllungen von Edward Snowden, der 2013 die weitreichende Überwachung der Internetkommunikation durch US-amerikanische Geheimdienste publik machte. Aber auch gezielte Cyberangriffe oder die Manipulation von sozialen Medien etwa in Wahlkampfzeiten sind inzwischen als drängende Herausforderungen erkannt. Auch hier fällt dem Staat eine besondere Rolle für den Schutz und die Sicherheit seiner digitalen Infrastrukturen zu.
- Schließlich zeigt sich, dass die Frage der Ausgestaltung der digitalen Wirtschaft und Gesellschaft hochgradig wertebezogen und damit kontrovers ist. Vor allem die USA und China ringen darum, die **normative Rahmensetzung** für die globale digitale Transformation zu dominieren. Die Bemühungen der EU, ihre technologische Souveränität zu stärken, sind daher untrennbar damit verbunden, mit einem **menschenzentrierten Ansatz** für die Digitalisierung eine Alternative zu den bisher dominierenden Modellen der USA und China zu etablieren. Gleichzeitig betont die EU zunehmend selbstbewusst ihren geopolitischen Gestaltungsanspruch in Fragen der digitalen Transformation auf globaler Ebene (Europäische Kommission 2020). Sie beruft sich dabei nicht zuletzt auf ihre umfassende Erfahrung aus zahlreichen Regulierungsvorhaben, etwa in Bezug auf Datenschutz, den Einsatz von KI, die Nutzung von Daten und die Ausgestaltung von Plattformen und digitalen Dienstleistungen.

Vor diesem Hintergrund bringt die Debatte um digitale bzw. technologische Souveränität in Deutschland und der EU sowohl den Wunsch nach als auch die Notwendigkeit von mehr Handlungs- und Gestaltungsfreiheit zum Ausdruck, um im digitalen Raum selbstbestimmt zu agieren, den digitalen Wandel nach eigenen Wertvorstellungen mitzugestalten sowie die eigene Vulnerabilität gegenüber vielfältigen Gefahren im Zusammenhang mit der Digitalisierung möglichst gering zu halten. Der Angriffskrieg Russlands auf die Ukraine hat hier insbesondere das Bewusstsein für Gefahr von Cyberangriffen erhöht. Zudem hat die COVID-19 Pandemie die Rolle der Digitalisierung für krisenresilientere Gesellschaften aufgezeigt und den Ruf nach mehr Selbstständigkeit und Entscheidungsmöglichkeiten im digitalen Raum gestärkt, aber auch Zielkonflikte – etwa zwischen Datennutzung und Datensouveränität – erkennen lassen.

**Box 2: Digitale Souveränität bewerten**

Digitale Souveränität ist ein normatives Konzept, das nicht gemessen, jedoch nach ausgewählten Kriterien bewertet werden kann. Eine solche Bewertung kann helfen, Zielbilder für die digitale Souveränität eines Staates zu entwickeln und die Einhaltung dieser Ziele zu überprüfen. Darüber hinaus ermöglicht sie, Länder hinsichtlich ihrer digitalen Souveränität zu vergleichen. Um die digitale Souveränität eines Landes zu bewerten, bedarf es jedoch einer eindeutigen Operationalisierung des Begriffs. Die Auswahl geeigneter Indikatoren hängt dabei vom zugrunde liegenden Begriffsverständnis der digitalen Souveränität ab (Cory & Dascoli 2021) und stellt – gemeinsam mit der Verfügbarkeit von Daten – eine wesentliche Herausforderung dar.

In einem der wenigen Versuche, einen modellhaften Index digitaler Souveränität zu erstellen, kombiniert Kaloudis (2021) mehrere Indizes, welche die digitalen Fähigkeiten und die politische Souveränität einzelner Länder abbilden. Er schlägt dabei eine Vielzahl weiterer möglicher Kriterien vor, die in einen kombinierten Index einfließen könnten, wie beispielsweise die Höhe der Investitionen in relevante Technologien, die Anzahl einschlägiger Patente oder das Import- bzw. Exportvolumen entsprechender Produkte und Grundstoffe. Jedoch wird dabei schnell deutlich, dass die Auswahl und Gewichtung der Indikatoren normativ geprägt sind und sogar zu widersprüchlichen oder nicht eindeutig zu interpretierenden Ergebnissen führen können. So zeichnet der von Kaloudis erstellte Index viele autokratische Staaten, wie beispielsweise China, als Länder mit lediglich geringer bis mittlerer digitaler Souveränität aus. Von den Staaten mit der höchsten digitalen Souveränitäts-Wertung werden 17 von 18 demokratisch regiert. Eine freiheitlich-demokratische Bevorzugung in der Bewertung könnte ein Grund dafür sein.

### 3. Nexus aus digitaler Nachhaltigkeit, Souveränität und Resilienz

#### 3.1. Nachhaltige Digitalisierung

Ähnlich wie bei dem Konzept der digitalen Souveränität gibt es auch in Bezug auf eine *nachhaltige Digitalisierung* unterschiedliche Begriffsverständnisse. Ein Grund dafür ist die Vielfalt an Definitionen für den Begriff der *Nachhaltigkeit* an sich (siehe Box 2). Des Weiteren kann der Bezug des Nachhaltigkeitsbegriffs zu Digitalisierung sehr unterschiedlich interpretiert werden. Debattiert werden vor allem drei Bedeutungsebenen für eine nachhaltige bzw. nachhaltigkeitsorientierte Digitalisierung:

- Nachhaltige Gestaltung *von* digitalen Technologien, Anwendungen und Märkten, also z. B. Reparierbarkeit von Smartphones, um Elektroschrott zu verringern, Barrierefreiheit digitaler Tools oder Regulierung digitaler Märkte, um Datenschutz für Nutzer\*innen zu gewährleisten.
- Erreichen von Nachhaltigkeitszielen *durch* den Einsatz digitaler Technologien, also z. B. digitales Arten-Monitoring, um einen Beitrag zum Erhalt der Biodiversität zu leisten, digital-gestütztes Ressourcenmanagement in der Industrie, um Materialien effizienter zu nutzen und Abfälle zu vermeiden oder Apps mit Informationsangeboten, um einen Beitrag zu gesellschaftlicher Inklusion zu leisten.
- Nachhaltige oder nachhaltigkeitsförderliche *systemische Veränderungen* vor allem durch soziale Innovationen in Folge der Digitalisierung, z. B. die Ermöglichung neuer nachhaltiger Geschäftsmodelle oder Verhaltensweisen durch Digitalisierung, wobei deren Effekte weit über die Wirkungen einzelner Technologien oder Anwendungen hinausgehen.

So ist zu beobachten, dass Innovationen wie die Sharing Economy in der Mobilität neue Verhaltensweisen für das Individuum ermöglichen und damit auch neue Entwicklungspfade für die Gesellschaft eröffnen. Dabei entscheidet die Art der Gestaltung und Nutzung von sozio-technischen Innovationen über deren Wirkung für eine nachhaltige Entwicklung.

Darüber hinaus wird ebenfalls betont, dass der Dreiklang der drei Nachhaltigkeitsstrategien Effizienz, Konsistenz und Suffizienz eine zentrale Rolle für eine nachhaltige Digitalisierung spielt (Reichel 2018). Effizienz steht dabei für

die ressourcen- und energiesparende Produktion und Nutzung digitaler Technologien. Konsistenz bedeutet, dass digitale Technologien möglichst so konstruiert sein sollten, dass sie in (möglichst) geschlossenen Ressourcenkreisläufen wiederverwertet werden können. Suffizienz hingegen zielt auf das Nutzungsverhalten ab und strebt einen sparsamen Einsatz der Digitalisierung und die Vermeidung unnötigen Konsums an.

### **Box 3: Exkurs: Nachhaltigkeit**

Der Begriff der Nachhaltigkeit stammt ursprünglich aus der Forstwirtschaft und steht dort für eine ausbalancierte wirtschaftliche Nutzung eines Waldes, ohne dessen Regenerationsfähigkeit zu beeinträchtigen. In den 1970er und 1980er Jahren gewann der Begriff der Nachhaltigkeit zunehmend politische Relevanz, etwa durch die Berichte des Club of Rome über die Grenzen des Wachstums (Meadows et al. 1974) und der sogenannten Brundtland Commission über „Unsere gemeinsame Zukunft“ (Brundtland 1985), die beide den bestehenden Konflikt zwischen wirtschaftlicher Entwicklung und dem Verbrauch und der Zerstörung natürlicher Lebensgrundlagen thematisierten. Mit steigendem Bewusstsein für den menschengemachten Klimawandel in den 1990er Jahren wurde der Begriff der Nachhaltigkeit zunehmend mit der Vermeidung von Treibhausgas-Emissionen verbunden.

Das Verständnis von nachhaltiger Entwicklung, das auch den 2015 lancierten Nachhaltigkeitszielen der Vereinten Nationen (UN SDGs) zugrunde liegt, geht jedoch weit über rein ökologische Aspekte hinaus. Es bezieht auch soziale Nachhaltigkeitsaspekte ein, etwa Zugang zu Bildung, Teilhabe, Geschlechtergerechtigkeit und Armutsbekämpfung. Die Diskussion um eine nachhaltige Digitalisierung, die vor allem in Deutschland in den letzten fünf bis zehn Jahren an Dynamik gewann, knüpft weitestgehend an dieses breite Verständnis von Nachhaltigkeit – das heißt seine sozial- wie ökologische Dimension – an. Hinzu kommen jedoch auch digitalspezifische Thematiken, die bisher in der Nachhaltigkeitsdebatte keine oder kaum eine Rolle spielten, wie z. B. Fragen des Umgangs mit und Schutzes von Daten oder die Beeinflussung von Nutzer\*innen sozialer Medien und damit potenziell negative Auswirkungen auf demokratische Prozesse und den gesellschaftlichen Zusammenhalt.

Den unterschiedlichen Konzepten und Verständnissen einer nachhaltigen Digitalisierung ist gemein, dass sie Nachhaltigkeit als normativen Rahmen, wenn nicht gar als Zielbild für die digitale Transformation betrachten.

### 3.2. Digitale Resilienz

Im Zuge der COVID-19 Pandemie werden die Wirkungen der Digitalisierung verstärkt mit dem Begriff der digitalen Resilienz in Verbindung gebracht. Dieser bezieht sich zumeist auf einzelne oder kollektive Akteure, für deren Funktionieren digitale Technologien eine wesentliche Rolle spielen. Für das Konzept der digitalen Resilienz besteht bisher keine allgemein gültige Definition. Es wird daher sehr unterschiedlich verwendet und beschreibt je nach Kontext und Begriffsverständnis die Fähigkeit,

- Krisen und Störereignisse von digital(isiert)en Systemen,
- Krisen und Störereignisse *mit Hilfe* digitaler Technologien, aber auch
- Krisen und Störereignisse, die *durch* digitale Technologien ausgelöst oder verstärkt werden,

zu überstehen und zu bewältigen. Ein Beispiel für die erste Dimension der digitalen Resilienz ist etwa der Einbau von Redundanzen in digitalen Infrastrukturen, damit mögliche physische Beschädigungen der Infrastruktur nicht sofort zu einem Totalausfall führen. Ein Beispiel für die zweite Ebene ist die Bewältigung der COVID-19 Pandemie unter Zuhilfenahme digitaler Tracking-Tools, um Infektionsketten besser nachvollziehen zu können. Für die dritte Dimension digitaler Resilienz kann beispielhaft die Verringerung der Anfälligkeit kritischer Infrastrukturen wie Krankenhäusern gegenüber Cyberangriffen, genannt werden. Resilienz im Sinne eines vorausschauenden Systemdesigns, um Risiken und ihre Folgewirkungen zu adressieren, kann somit als ein weiterer Aspekt eines holistischen Nachhaltigkeitsbegriffes betrachtet werden – es wird jedoch auch als eigenständiges, von Nachhaltigkeit unabhängiges Konzept genutzt.

Im CO:DINA-Vorhaben erkennen wir die enge Beziehung zwischen Resilienz und Nachhaltigkeit an und verstehen Resilienz vorrangig als Eigenschaft und Fähigkeit eines Akteurs oder eines Systems, Störereignisse zu bewältigen und

sich auf Basis der gemachten Erfahrungen weiterzuentwickeln. Damit sehen wir Resilienz als eine zentrale Bedingung für eine nachhaltige Entwicklung an.

#### **Box 4: Exkurs: Resilienz**

Der Begriff Resilienz zeichnet sich durch ein breites Bedeutungsspektrum aus. Originär wird er vor allem in der Psychologie verwendet und steht dort für die Widerstandsfähigkeit eines Individuums, sich durch Anpassungsleistungen trotz ungünstiger Lebensumstände und kritischer Lebensereignisse erfolgreich zu entwickeln. In den vergangenen Jahrzehnten wurde der Begriff verstärkt in sozialwissenschaftlichen Kontexten verwendet, um die Widerstandskraft eines gesellschaftlichen (Teil-)Systems gegenüber Störungen zu charakterisieren und dessen Fähigkeit zur Anpassung an veränderte Umweltbedingungen darzustellen.

Resilienz ist dabei an sich normativ neutral und kann mit unterschiedlichen Werten und Zielstellungen verbunden werden. Aus Nachhaltigkeitsperspektive sollte Resilienz in einer krisenhaften Welt als eine Grundvoraussetzung für den Erfolg von Nachhaltigkeitszielen angesehen werden (Beer & Rammler 2021).

Beer und Rammler definieren *transformative Resilienz* als die Fähigkeit einer Gesellschaft, neben der sozialökologischen Transformation auch gegenwärtigen wie zukünftigen Krisen gerecht zu werden. Der Grad der erreichten transformativen Resilienz entspricht dabei der Fähigkeit, unter wechselhaften und unsicheren Bedingungen eine nachhaltige Entwicklung der Gesellschaft erfolgreich voranzutreiben. Um dieses abstrakte Konzept im Sinne einer nachhaltigkeitspolitischen Anwendung zu konkretisieren, unterscheiden sie drei Dimensionen transformativer Resilienz:

- 1) *Widerstandsfähigkeit* als die Kapazität, mögliche Krisen zu antizipieren und relevante Gesellschaftssysteme zu stärken
- 2) *Anpassungsfähigkeit* als die Kapazität, auf Störungen zu reagieren und diese nachhaltig zu beheben; sowie
- 3) *Transformationsfähigkeit* als die Kapazität, den disruptiven Moment von Krisen als Katalysator für den sozioökologischen Umbau zu nutzen (Beer & Rammler 2021).

### 3.3. Zwischenfazit

Nachhaltige Digitalisierung und digitale Resilienz sind zwei weitere Schlüsselkonzepte, die eng mit Fragen der digitalen Souveränität verbunden sind. Digitale Souveränität kann als eine zentrale Voraussetzung zum Erreichen der normativen Zieldimensionen einer nachhaltigen Digitalisierung – also etwa ökologischer Unbedenklichkeit, sozialer Verträglichkeit und Generationengerechtigkeit – betrachtet werden. Nur eine weitreichende digitale Selbstbestimmungsfähigkeit kann es Gesellschaften ermöglichen, dass ihre Normen und Werte in der Ausgestaltung digitaler Technologien, Anwendungen und Märkte berücksichtigt werden.

Zudem ist digitale Souveränität ein zentraler Baustein für die digitale Resilienz von Gesellschaften, indem sie ihnen etwa erlaubt, kritische Infrastrukturen mit digitalen Komponenten auszustatten, die weniger anfällig gegenüber Angriffen durch staatliche wie nicht-staatliche Aggressoren sind (Rammler et al. 2021), sich unabhängiger von Technologieimporten zu machen oder Regeln für Teilsysteme, etwa digitale Märkte oder den Einsatz von KI, aufzustellen und durchzusetzen.

Allerdings sei erwähnt, dass sich das Verständnis von bzw. die Anforderungen an digitale Nachhaltigkeit, Resilienz und Souveränität über die Zeit hinweg wandeln und von zahlreichen Faktoren abhängig sind. Sie sollten daher immer vor ihrem gesellschaftlichen und politischen Kontext betrachtet werden (Beer & Rammler 2021).

#### 4. Digitale Souveränität und Nachhaltigkeit – Synergien und Zielkonflikte auf Ebene der EU

Mit dem digitalen Wandel und dem sozial-ökologischen Umbau von Wirtschaft und Gesellschaft steht die EU vor der Herausforderung, zwei umfassende Transformationsprozesse gleichzeitig bewältigen zu müssen. Neben dem Green Deal (siehe Box 5) wurden in den vergangenen Jahren auch zahlreiche digitalpolitische Regulierungsansätze lanciert. In Vorbereitung auf die von der EU zur „digitalen Dekade“ ausgerufenen 2020er-Jahre einigte sich die EU auf zahlreiche Gesetzesinitiativen (Europäische Kommission, 2021). Zu den geplanten und sich momentan im europäischen Gesetzgebungsprozess befindlichen Gesetzesinitiativen mit besonderer Relevanz für die digitale Souveränität gehören die KI-Verordnung (AI Act), die Verordnung über Daten-Governance (Data Governance Act), die Datenverordnung (Data Act), das Gesetz über digitale Märkte (Digital Markets Act, DMA), das Gesetz über digitale Dienste (Digital Services Act, DSA) sowie das Chip-Gesetz (European Chips Act).

##### **Box 5: Der European Green Deal und die digitale Transformation**

Mit ihrem *European Green Deal* will die EU bis 2050 der erste „klimaneutrale Kontinent“ werden. Neben den klima- und umweltpolitischen Zielsetzungen des Green Deals, soll das Vorhaben die EU auch international als Vorreiter in der Bekämpfung des Klimawandels positionieren sowie die EU durch die gezielte Förderung notwendiger Innovationen für die sozial-ökologische Wirtschaftstransformation rüsten.

Der Maßnahmenkatalog des European Green Deal wird inzwischen von einem klimafreundlichen Wiederaufbauprogramm ergänzt. Als Reaktion auf die wirtschaftlichen Folgen der COVID-19-Pandemie wurde 2020 der sogenannte Next Generation EU (NGEU) Fond mit einem Umfang von 750 Milliarden Euro als größtes Konjunkturpaket der EU-Geschichte beschlossen. Unter dem Schlagwort Green Recovery sollen dabei 37 Prozent der Mittel für den European Green Deal ausgegeben werden, weitere 20 Prozent sind für den Ausbau der Digitalisierung vorgesehen.

Darüber hinaus ist der 2020 beschlossene europäische „Aktionsplan für die Kreislaufwirtschaft“ ein wichtiger Baustein des European Green Deals. Dieser fokussiert sich auf die Gestaltung und Produktion von Produkten, damit verwendete Ressourcen künftig so lange wie möglich in der EU-Wirtschaft verbleiben. Neben den ökologischen Aspekten werden vor allem neue Geschäfts- und Beschäftigungsmöglichkeiten sowie die internationale Wettbewerbsfähigkeit als Gründe angeführt. Im Rahmen einer Kreislaufwirtschaft könnte Europa auch seine Abhängigkeit vom Import bestimmter Rohstoffe, wie z. B. seltene Erden, reduzieren.

Mit der 2021 in Kraft getretenen Ökodesign-Richtlinie werden des Weiteren Vorgaben für die Reparaturmöglichkeit von Elektrogeräten, einschließlich Elektronischer Displays gemacht. Entsprechender Regulierungsdruck der EU hat dabei in der Praxis bereits heute Auswirkungen über die Grenzen des EU-Markts hinaus. Beispielsweise gab Apple als Reaktion auf die EU-Richtlinie seine langjährige restriktive Ersatzteilpolitik auch auf dem amerikanischen Markt auf (Mearian 2021).

Erklärtes Ziel der EU ist es, mit solchen regulativen Maßnahmen, aber auch mit Förderprogrammen für Forschung und Entwicklung, zu einem Vorreiter von „weltweit kompetitiven, sozial verantwortlichen und nachhaltigen Hochtechnologien zu werden“ (EU 2021). Darüber hinaus soll der „Brüssel-Effekt“ (siehe Box 6) auch im Bereich Digitalisierung dabei helfen, Normen und Standards entsprechend europäischer Werte weltweit zu gestalten (Nestoras 2022).

Im Folgenden stellen wir anhand einzelner digitalpolitischer Themenfelder dar, inwiefern das Bestreben, die Digitalisierung selbstständig, selbstbestimmt und sicher auszuüben, dazu dienen könnte, sozial-ökologische Transformationspfade zu erschließen und zu beschreiten. Dabei betrachten wir insbesondere potenzielle Synergien sowie Zielkonflikte zwischen Souveränitäts- und Nachhaltigkeitszielen. Die Auswahl der relevanten Themenfelder orientiert sich an einer Studie des Oxford Internet Instituts, welche die Verwendungsweisen des Begriffs der digitalen Souveränität durch die zentralen EU-Akteure Kommission, Parlament und Rat empirisch untersuchte (Roberts et al. 2021). In der Studie wurden dazu alle Instanzen des Begriffs auf den Webseiten der genannten Akteure nach Themenkontexten gebündelt, wobei fünf wiederkehrende Handlungsfelder identifiziert werden konnten: Daten-

Governance, Plattformunternehmen, digitale Infrastruktur, aufkommende Technologien sowie IT-Sicherheit.

#### **Box 6: Der Brüssel-Effekt**

Der von der Handelsrechtsexpertin Anu Bradford vorgeschlagene Begriff „Brüssel-Effekt“ bezeichnet in Anlehnung an den Begriff „Kalifornien-Effekt“ die Übernahme strengere EU-Vorschriften durch andere Hoheitsbereiche und global agierende Firmen. Firmen orientieren sich dabei an den strengeren (europäischen) Standards, da mit diesen automatisch auch die schwächeren Standards anderer Staaten erfüllt werden und so ein Effizienzgewinn erzielt werden kann. Der Aufwand für Unternehmen, mehrere unterschiedliche Standards zu beachten ist in der Praxis häufig zu hoch. Es existieren also Marktanzreize für ein *race to the top* – das Gegenteil eines Unterbietungswettlaufs. In Bereichen wie Wettbewerbspolitik, Umweltschutz sowie der Verbrauchersicherheit ist die Europäische Union aufgrund ihrer Größe und Marktmacht sowie hohen Regulierungskapazitäten und der strengen Einhaltung von Standards bereits zu einer Art *regulatorischer Hegemon* avanciert (Bradford 2020).

#### 4.1. Daten-Governance

Daten-Governance – verstanden als das gesetzliche Rahmen- und Regelwerk für den Umgang mit Daten – ist das Feld, in dem das Bestreben, die europäische digitale Souveränität zu stärken, bislang am weitesten fortgeschritten ist. Mit dem Ziel, den Schutz persönlicher Daten europäischer Bürger\*innen zu verbessern, trat 2018 die europäische Datenschutzgrundverordnung (DSGVO) in Kraft. Mit der DSGVO wurden die Regeln zur Verarbeitung personenbezogener Daten EU-weit vereinheitlicht und teilweise ausgebaut. Sie gilt für inner- und außer-europäische Unternehmen, soweit deren Datenverarbeitung mit einem Angebot in Zusammenhang steht, das sich an Personen in der EU richtet. Der Bußgeldrahmen wurde dabei wesentlich erhöht, sodass die europäische Regulierung in diesem Fall als Katalysator für eine Fokusänderung des Ökosystems aus Softwaredesignern und Entwicklern wirkte. Außereuropäische Firmen haben ihr Produktportfolio inzwischen breit umgestellt, um weltweit der europäischen Datenschutzrichtlinie zu entsprechen. (Bluestone 2021). Damit hat

die DSGVO vermutlich auch außerhalb der EU eine Stärkung von Datenschutz-Prinzipien bewirkt (Greenleaf 2021).

Darüber hinaus stellt die europäische Datenstrategie eine der jüngsten Bemühungen dar, einen Ansatz für eine gemeinsame europäische Daten-Governance zu entwickeln. Zentrale Regulierungsbestandteile sind der sich noch in dem EU-Gesetzgebungsprozess befindlichen Data Governance Act<sup>3</sup> sowie der Data Act<sup>4</sup>. Ziel dieser Regulierungen ist es, einen funktionierenden Binnenmarkt für Daten bei gleichzeitig hohem Datenschutz zu schaffen und damit die Wertschöpfung aus Daten anzukurbeln.

Eine Balance zwischen einer privatwirtschaftlich-wachstumsorientierten und einer öffentlich-gemeinwohlorientierten Daten-Governance zu schaffen, ist eine zentrale Herausforderung europäischer Datenpolitik. Ein unzureichender Datenaustausch zwischen marktwirtschaftlichen Unternehmen oder staatlichen Organisationen kann als Innovationshemmer wirken, z. B. im Bereich der kommunalen Daseinsvorsorge. Um diese Herausforderungen zu bewältigen, schlägt die EU in ihrem Data Act einige Maßnahmen vor. So sollen die Bürger\*innen besseren Zugang zu den eigenen Daten erhalten, die von vernetzten Geräten erzeugt werden, sowie besser gegen den unrechtmäßigen Gebrauch dieser Daten geschützt werden. Darüber hinaus sollen kleine und mittlere Unternehmen (KMU) hinsichtlich der wirtschaftlichen Nutzung von Daten vor missbräuchlichen Vertragsklauseln geschützt werden, die von einer Vertragspartei mit einer deutlich stärkeren Verhandlungsposition vorgegeben werden. Behörden soll zudem im Fall einer definierten Notlage der Zugang zu spezifischen Daten des Privatsektors vereinfacht werden (Europäische Kommission, 2022b). Auch wenn die generelle Regulierung für das Teilen und Nutzen von Daten begrüßt wird, so wird vor allem von Expert\*innen aus der

---

<sup>3</sup> Hauptfokus des Data Governance Act sind bereits vorhandene, öffentliche Datenpools, die besser zugänglich gemacht werden sollen. Ein zentraler Ansatz sind dabei durch EU-Recht kontrollierte neutrale Vermittlungsstellen, sogenannten Datenintermediären, die mehr Transparenz und Vertrauen auf dem Datenmarkt garantieren könnten. Das vorgeschlagene Gesetz trifft aber auch Regelungen zur Datenspende von Privatpersonen, beispielsweise in Form von Datengenossenschaften.

<sup>4</sup> Der Data Act wird sich auf die Datennutzung im Kontext von Business-to-Business und Business-to-Government fokussieren und zugleich die bisherigen Regeln für Datenbanken überarbeiten.

Zivilgesellschaft Kritik am Datengesetz geäußert, da das Gemeinwohl hinter wirtschaftlichen Interessen weitgehend zurückbleibt (Dachwitz 2022).

### **Box 7: Gemeinwohlorientierte Daten-Governance – eine Case study**

In dem Versuch, eine starke Datenwirtschaft mit einer gemeinwohlorientierten Daten-Governance zu kombinieren, wurde im Rahmen des Projekts DECODE (*Decentralised Citizen-owned Data Ecosystems*) die Daten-Governance in Barcelona als Modellstadt grundlegend verändert. Die Daten der Bürger\*innen wurden im Sinne sog. *Data Commons* als öffentliche Infrastruktur interpretiert, über die gemeinwohlorientiert und unter Achtung des Datenschutzes verfügt werden kann. Auf diese Weise können die Bürger\*innen souverän über ihre Daten bestimmen und individuell festlegen, wer ihre Daten wann und zu welchem Zweck verwenden darf. Als europäische Alternative zum privatkapitalistischen Datenmodell des Silicon Valley oder gar Chinas digital-autoritärem Modell soll das DECODE-Projekt aufzeigen, wie Daten gemeinwohlorientiert und gleichzeitig ökonomisch sinnvoll verarbeitet werden und somit allen Beteiligten an der Daten-Wertschöpfungskette zum Vorteil gereichen können (Bria 2022).

Kritik am Modell der Data Commons kommt derweil aus volkswirtschaftlicher Richtung. So wird argumentiert, dass digitale Gemeingüter ihren Zweck nur dann erfüllen können, wenn sie auch in freien Marktsystemen außerhalb des Wertkreislaufes des Gemeinguts selbst gehandelt werden können. Dies birgt jedoch das Risiko eines übermäßigen Durchsickerns von Daten an rein gewinnorientierte Unternehmen, was die ursprüngliche Idee der Daten als Gemeingut unterminieren würde (Zygmuntowski et al. 2021).

Auch die Entwicklung des Datenökosystems rund um die Initiative Gaia-X betrifft Fragen der Daten-Governance. Bei dem paneuropäischen Projekt soll eine föderale und dezentrale Dateninfrastruktur entwickelt werden, die Unternehmen und Bürger\*innen gleichermaßen Zugriff und Kontrolle über ihre Daten ermöglicht. Dazu werden gemeinsame Standards entwickelt sowie eine passende Open Source Software-Gemeinschaft aufgebaut. Kritische Stimmen von Expert\*innen bescheinigen dem Projekt jedoch eine wachsende Abhängigkeit von internationalen Technologiekonzernen sowie mangelnde Transparenz und Kritikfähigkeit (Noyan 2021).

Daten-Governance spielt aus klima- und umweltpolitischer Sicht eine bedeutende Rolle, denn Akteure, die klimaschutzrelevante Softwareanwendungen entwickeln möchten, sind auf den Zugang zu relevanten und hochwertigen Daten angewiesen. Im kommunalen Kontext betrifft dies etwa die Bereiche Verkehrssteuerung, Energieversorgung oder die Gebäudetechnik (Öko-Institut & IZT 2021). Der Zugang zu geeigneten Datenbeständen ist zudem eine wichtige Voraussetzung für die Forschung zu klimapolitischen Problemstellungen wie auch für das Monitoring der 17 Ziele der Vereinten Nationen für nachhaltige Entwicklung (UN Sustainable Development Goals, SDGs). Die SDGs definieren politische Ziele, die global der Sicherung einer nachhaltigen Entwicklung auf ökonomischer, sozialer sowie ökologischer Ebene dienen sollen. Expert\*innen haben darauf hingewiesen, dass zur Erreichung dieser Ziele der Einsatz von digitalen Technologien notwendig ist, die die Datenrechte und die Privatsphäre der Bürger\*innen garantieren (Michael et al. 2019).

Zusammenfassend lässt sich sagen, dass die Aktivitäten der EU, ihre Souveränität im Bereich der Daten-Governance auf der Basis europäischer Grundwerte zu stärken, von zentraler Bedeutung für die soziale und ökologische Nachhaltigkeit Europas sind. Allerdings bedarf es noch weiterer Bemühungen, um besser zu verstehen, welche Ansätze der Daten-Governance geeignet sind, um gemeinwohl- und nachhaltigkeitsorientierte Ziele optimal zu unterstützen.

#### 4.2. Plattformunternehmen

Digitale Plattformunternehmen spielen eine immer größere Rolle für das Funktionieren einer modernen Gesellschaft und Wirtschaft und sind aus unserer Alltagswelt nicht mehr wegzudenken. Einzelne Unternehmen, wie etwa Google, Amazon und Meta, haben dabei eine dominierende Marktmacht erreicht. Hierbei spielen Konzentrationsprozesse auf Grund von Netzwerkeffekten eine entscheidende Rolle: Da große Plattformen, die bereits eine große Nutzerbasis haben, deutlich mehr Möglichkeiten in Bezug auf Vernetzung, Reichweite, Warenangebot oder Informationen bieten als kleine, werden sie auch häufiger und intensiver genutzt. Dadurch werden sie wiederum für neue Nutzer\*innen attraktiver, wodurch die Zahl der Nutzer\*innen weiter ansteigt. Nach einem solchen *Winner-takes-all*-Prinzip entstandene, besonders große Plattformunternehmen können den Marktzugang anderer Unternehmer

erschweren. Die entstandene Machtkonzentration wird dadurch konserviert oder sogar noch verstärkt (Stafford 2019).

Die Strukturen der derzeitigen Plattformwirtschaft können langfristig große Innovationshemmnisse darstellen (Campbell & Hulme 2001). Die bedeutende Marktmacht der sogenannten *Gatekeeper*, also Plattform-Unternehmen mit einer potenziell marktverzerrenden Macht, kann dabei neue nachhaltigkeitsorientierte Start-Ups und kleine und mittelständische Unternehmen in ihrer Entwicklung hemmen. Für die Transformation des bisherigen Wirtschaftssystems zu einer postfossilen Kreislaufwirtschaft spielen innovative privatwirtschaftliche Akteure jedoch eine entscheidende Rolle.

Social-Media-Plattformen als digitale Kommunikationsräume üben einen hohen Einfluss auf öffentliche Informationen und Willensbildungsprozesse aus. Ohne klare Rechtsvorgaben durch den Staat oblag es lange den Unternehmen selbst, Regeln für den Umgang mit kontroversen Inhalten oder Nutzer\*innen festzulegen. Doch die Verbreitung problematischer Inhalte in digitalen Öffentlichkeiten, wie Hasskommentare, Drohungen, bewusste Fehlinformationen und Verschwörungstheorien, beschädigen langfristig auch die Demokratie selbst, wie die Entwicklungen der letzten Jahre zeigen (Sternisko et al. 2020; Morgan 2018).

Mit dem Digital Markets Act (DMA) und dem Digital Services Act (DSA) befinden sich zwei zentrale digitale Regulierungsvorhaben im EU-Gesetzgebungsprozess, die die großen digitalen Plattformen dazu bringen sollen, ihrer gesellschaftlichen Verantwortung gerechter zu werden. Beide sollen noch im Laufe der französischen Ratspräsidentschaft 2022 verabschiedet werden. Auch wenn die Kommission in ihren offiziellen Verlautbarungen darauf achtet, die größten US-amerikanischen Technologie-Unternehmen nicht als explizite Ziele der Regulierungen zu erwähnen, so ist es offenkundig, dass der Anwendungsbereich insbesondere Google, Meta und Amazon betrifft (Holm-Hadulla et al. 2020). Für solche sogenannten Gatekeeper, sind im vorgeschlagenen Digital Markets Act neue Pflichten in Form von Geboten und Verboten vorgesehen.<sup>5</sup> Der DMA stellt dabei einen Wechsel von den bisherigen ex-post EU-Kartellverfahren hin zu einer

---

<sup>5</sup> Beispielsweise sieht der DMA vor, dass bei der Plattformnutzung generierte Daten mit gewerblichen Nutzer\*innen geteilt werden müssen. Eigene Produkte oder Dienstleistungen dürfen gegenüber denen Dritter auf der Plattform in der Reihung nicht mehr bevorzugt behandelt werden (Holm-Hadulla et al. 2020).

ex-ante Regulierung dar. Wieder gelten diese Regeln für Anbieter, unabhängig davon, wo sie residieren, solange diese ihre Dienstleistungen innerhalb der EU zur Verfügung stellen. Zur Durchsetzung sind neben hohen Geldbußen und Zwangsgeldern weitere mächtige Instrumente vorgesehen, etwa Ermittlungsbefugnisse der Europäischen Kommission und die Möglichkeit von einstweiligen Anordnungen. Zudem soll ein präventives Handeln gegenüber im Entstehen befindlichen Gatekeepern ermöglicht werden.

Ähnlich weitreichend sind die Regelungen für den vorgeschlagenen Digital Services Act, der dem besseren Schutz der Nutzer\*innen vor illegalen Dienstleistungen, Hassrede und Desinformation dienen soll. Dazu werden gestaffelte Verpflichtungen für Soziale Medien, Verkaufsplattformen sowie Vermittlungs- und Hosting-Dienste eingeführt.<sup>6</sup> Problematische Entwicklungen, die zum Teil schon jetzt demokratische Willensbildungsprozesse innerhalb der Europäischen Union schädigen, sollen damit unterbunden und die Souveränität der digitalen Kommunikationsräume der EU erhöht werden.

Skeptiker wenden allerdings ein, dass selbst wenn DMA und DSA ohne zu große Abschwächungen der derzeit vorgesehenen Regelungen beschlossen werden, diese Verordnungen an der wirtschaftlich-technologischen Macht der weltweit größten Plattformunternehmen wenig ändern würden. Als Beleg wird dafür auf das Beispiel der Kontaktverfolgungs-Apps während der COVID-19 Pandemie hingewiesen, bei der selbst souveräne europäischen Regierungen in der Umsetzung von einem kooperativen Verhalten von Google und Apple abhängig waren (Roberts et al. 2021).<sup>7</sup>

Ökologische Nachhaltigkeit ist kein Schwerpunkt der beiden EU-Vorhaben zur Plattform-Regulierung. Der Digital Services Act beinhaltet zwar auch Regeln für

---

<sup>6</sup> So werden Regelungen getroffen, die die Entfernung illegaler Inhalte auf Online-Plattformen besser und beschleunigt ermöglichen und gleichzeitig ein Over-Blocking, d. h. ein prophylaktisch ausgeführtes Löschen und damit Zensur, verhindern sollen (Bauer 2022).

<sup>7</sup> Mindestens 19 EU-Staaten hatten sich an Google und Apple gewandt, um das von diesen Firmen während der Pandemie entwickelte sog. Exposure Notification Framework (ENF) für staatliche Kontaktverfolgungs-Apps von infizierten Personen über Smartphones zu nutzen. Über die Programmierschnittstelle (API) kontrollierten diese Firmen allerdings weiterhin welche Smartphone-Modelle überhaupt mit der API zusammenarbeiteten und auch für wie lange diese zur Verfügung gestellt wurde. Auch die Gesetzesvorhaben des Digital Markets Act und des Digital Services Act würden daran nichts grundlegend ändern.

die personalisierte Werbung, doch spielt die für eine sozial-ökologische Transformation zentrale Änderung von Konsummustern keine Rolle (Bauer, 2022). Darüber hinaus verpassen es beide Vorhaben, verbindliche Bedingungen über die Nachhaltigkeitskriterien zu formulieren, die von Plattformunternehmen, die in der EU operieren, erfüllt werden müssen.

Zusammenfassend lässt sich daher sagen, dass die Datenmacht von Plattformunternehmen schon jetzt negative Auswirkungen hat und ein signifikantes Zukunftsrisiko darstellt. Eine Stärkung der digitalen Souveränität Europas gegenüber den marktbeherrschenden Tech-Konzernen würde die Nachhaltigkeitstransformationen unterstützen. Die angestrebten Ex-Ante-Regulierungen des Digital Markets Act und des Digital Services Act sind ein erster Schritt zu einer solchen verstärkten digitalen Souveränität. Dies könnte neuen KMUs mit Nachhaltigkeitsfokus der Marktzugang erleichtern und zudem den EU-Bürger\*innen mehr digitale Selbstbestimmung ermöglichen.

#### 4.3. Digitale Cloud-Infrastruktur

Eine leistungsstarke digitale Infrastruktur ist eine wichtige Bedingung für eine moderne, innovative und produktive Wirtschaft. Insbesondere der Einsatz von Cloud-Computing, bei dem über das Internet geteilte Computerressourcen, z. B. Server, Datenspeicher oder Anwendungen als Dienstleistung genutzt werden können, hat in den vergangenen Jahren zugenommen. Cloud-Lösungen vereinfachen das kollaborative Arbeiten über weite Entfernungen und bilden damit eine wichtige Basis der globalen digitalen Infrastruktur. Die größten Anbieter wie Google Cloud, Microsoft Azure und Amazon Web Services sind allerdings vollständig in US-amerikanischer Hand. Europäische Unternehmen spielen selbst in ihrem Heimatmarkt kaum eine Rolle (EIT Digital, 2020).

Die Bemühungen um den Aufbau europäischer Cloud-Kapazitäten befinden sich noch in der Planungsphase. In einer Absichtserklärung der EU-Staaten kündigten diese an, ein gemeinsames Regelwerk sowie eine föderale Cloud-Struktur zu entwickeln (EU 2020). Dazu fand Ende 2021 das erste Treffen der neu gegründeten *European Alliance for Industrial Data, Edge and Cloud* statt. Diese soll Unternehmen zusammenbringen, um gemeinsam mit der Europäischen Kommission eine langfristige Investitions-Roadmap für das europäische Cloud- und Edge Computing zu entwickeln (Europäische Kommission 2022). Teil der europäischen Bemühungen um eine Stärkung eigener Cloud-Infrastrukturen ist

die paneuropäische, öffentlich-private Initiative Gaia-X. In diesem Verbund sollen im Einklang mit den Klimaschutzzielen des Green Deals verbindliche technologische Standards auch hinsichtlich der Energieeffizienz für Cloud-Dienste festgelegt werden. Entsprechende Datenzentren sollen demnach höchsten Ansprüchen an Energieeffizienz und Ressourcenschonung genügen (Köhn et al. 2020).

Während die Cloud auf die Nutzung von häufig weit entfernten Datenzentren angewiesen ist, erfolgt beim Edge Computing die Datenverarbeitung möglichst dezentral in der Netzwerkperipherie. So hilft Edge Computing, die IT-Infrastruktur zu entlasten, und gewährleistet die für das Internet der Dinge so wichtigen schnellen Reaktionszeiten. Vor dem Hintergrund wachsender Datenströme und dem steigenden Bedarf an Rechenkapazitäten, soll Edge Computing dabei eine Erweiterung der bestehenden Netzarchitekturen darstellen und nicht deren Ablösung.

Die Nachhaltigkeitsbewertung digitaler Infrastrukturen, z. B. in Bezug auf Energieverbrauch und Treibhausgas-Emissionen, ist ein schwieriges Unterfangen. Eine besondere Herausforderung ist dabei die rasante technische Entwicklung, einschließlich der Verbesserungen der Energieeffizienz, genauso aber auch die Geschwindigkeit, mit der neue digitale Technologien und Geschäftsmodelle sich am Markt platzieren (Heyen et al. 2022).

Bei den Cloud-Datenzentren ist ein Konzentrationsprozess zu beobachten, der in Reaktion auf die energetischen Nachteile kleinerer Datenzentren stattfindet und in immer größeren, sogenannten *Hyperscale-Datenzentren* resultiert (Kaur 2021). Die verstärkte Internetnutzung während der Pandemie hat diesen Trend noch einmal verstärkt. Hyperscale-Datenzentren sind durch ihre Server-Infrastruktur mit Tausenden weitgehend identischen Rechnern auf höchste Skalierbarkeit ausgelegt, um so dynamisch und automatisiert die ständig schwankende Nachfrage der Kunden nach IT-Leistung erfüllen zu können. Solche Datenzentren, wie sie beispielsweise von Google und Amazon betrieben werden, sind äußerst energieeffizient. So erreichen die effizientesten Hyperscale-Rechenzentren eine sogenannte *Power usage effectiveness* (PUE)<sup>8</sup>

---

<sup>8</sup> Power Usage Effectiveness (PUE) ist eine technische Kennzahl, mit der sich die Energieeffizienz eines Rechenzentrums darstellen lässt. Der PUE-Wert setzt die insgesamt in einem Rechenzentrum verbrauchte Energie ins Verhältnis mit der

von 1,1 und sind damit bezogen auf die Energieaufnahme der Infrastruktur dieser Rechenzentren (gemeint sind damit Klimatisierung und unterbrechungsfreie Stromversorgung) schon nahe an einem praktisch überhaupt erreichbaren Optimum (Öko-Institut & IZT 2021).

Änderungen des Nutzungsverhaltens und systemische Veränderungen durch die Digitalisierung machen eine Vorhersage zukünftiger Energieverbräuche durch Dateninfrastrukturen nur schwer möglich. So kann eine verbreitete Implementierung von Edge Computing im Rahmen eines Rebound-Effektes beispielsweise auch gegenteilig zu einem höheren Energieverbrauch führen. Daher ist selbst die Definition eines Baseline-Szenarios für die Entwicklung des Energieverbrauchs bzw. der Treibhausgas-Emissionen von Cloud-Infrastrukturen sehr schwierig.

Welche Auswirkungen daraus letzten Endes für die ökologische Nachhaltigkeit erwachsen, lässt sich derzeit noch nicht abschätzen, jedoch birgt der Aufbau eigener europäischer Cloud-Infrastrukturen die Chance, ökologische Nachhaltigkeit von Beginn an mitzudenken und durch entsprechende Regulierungen auch umzusetzen. Dabei sollten mögliche Rebound-Effekte antizipiert sowie die bestehenden Unsicherheiten einer konkreten Nachhaltigkeitsbewertung neuartiger Technologien kritisch bedacht werden. Zudem kann der Aufbau eigener europäischer Cloud-Kapazitäten die Entwicklung und Umsetzung eines europäischen, menschenzentrierten Ansatzes der Daten-Governance unterstützen. So werden momentan noch viele Daten europäischer Bürger\*innen außerhalb Europas gespeichert. De facto ist damit kaum kontrollierbar, ob die entsprechenden Firmen alle europäische Datenschutzbestimmungen wirklich einhalten.

#### 4.4. Schlüsseltechnologien

Zu potenziell zukunftsprägenden digitalen Schlüsseltechnologien gehören Supercomputing (Exascale-Computing), Mobilfunktechnologien basierend auf dem 5G- und 6G-Standard, Quantentechnologien, Blockchain sowie Augmented und Virtual Reality. Die Künstliche Intelligenz, insbesondere in Form des Maschinellen Lernens, verändert jetzt schon tiefgreifend Wirtschaft und

---

Energieaufnahme der IT-Infrastruktur. In der Praxis werden Werte bis 1,2 als sehr effizient beurteilt. Konventionelle Rechenzentren weisen in der Regel einen PUE-Wert von 1,9 auf.

Gesellschaft. Weiterentwicklungen in der Halbleiter- und Mikrochip-Technik stellen die technische Basis für das Informationszeitalter. Im Folgenden wird auf Grund der besonderen Bedeutung der beiden Schlüsseltechnologien Mikrochip und Künstliche Intelligenz deren Zusammenhang mit einer nachhaltigen digitalen Souveränität diskutiert.

#### 4.4.1. Halbleiter- und Mikrochip-Technik

Spätestens seit der weltweiten Chip-Knappheit, die im Zuge der COVID-19 Pandemie zu massiven Liefer- und Produktionsengpässen etwa in der europäischen IT- und Automobilindustrie geführt hat, ist deutlich geworden, welchen Stellenwert die Halbleiter- und Mikrochipindustrie für die digitale Souveränität Europas einnimmt. Im Vergleich zu den Markführern USA, Taiwan, und Südkorea beträgt die europäische Halbleiterproduktion, einschließlich Prozessoren, aktuell lediglich zehn Prozent der weltweiten Gesamtproduktion (Europäische Kommission 2021). Die europäischen Bemühungen, diesen Wert bis zum Jahr 2030 zu verdoppeln, sollen in dem sogenannten *European Chips Act* festgelegt werden. Aktuell prüft sowohl der amerikanische Konzern Intel als auch der taiwanische Konzern TSMC, inwieweit europäische Regionen in naher Zukunft als Produktionsstandorte genutzt werden könnten (FAZ 2022).

Expert\*innen warnen jedoch davor, den Fokus zu sehr auf Produktionskapazitäten zu richten, denn die Wertschöpfungskette der Halbleiterindustrie ist komplex und End-to-End-Kapazitäten sind aktuell in keiner Region der Welt vorhanden (Kleinhans & Lee 2021). Es wäre demnach durchaus sinnvoll, die Potenziale beispielsweise im Bereich des Chipdesigns, der Grundlagenforschung oder in einschlägigen Zuliefererindustrien auszubauen, statt vorrangig auf heimische Endproduktion zu setzen; zumal der Investitionsvorsprung der asiatischen und amerikanischen Produzenten kaum noch einzuholen scheint (ebd.). Jedenfalls werden die für solche Vorhaben bereitgestellten Finanzmittel von Kritiker\*innen als unrealistisch betrachtet (Morozov 2021).

Neben geopolitischen und wirtschaftlichen Aspekten sollten in der Halbleiterproduktion auch Aspekte ökologischer Nachhaltigkeit im Vordergrund stehen. Während Mikrochips einerseits in vielen Technologien, die als Hoffnungsträger einer nachhaltigeren Zukunft gehandelt werden (z. B. im Bereich Elektromobilität oder Industrie 4.0), zur Anwendung kommen, ist ihre Produktion von einem besonders hohen CO<sub>2</sub>-Ausstoß gekennzeichnet (Gupta et

al. 2020). Vor allem der Wasser- und Stromverbrauch sowie die benötigte Fläche zum Bau von Fabrikanlagen schlägt sich negativ in der Ökobilanz von Mikrochips nieder.

Zusammenfassend lässt sich sagen, dass offen ist, ob Europa eine großflächige heimische Endproduktion für Mikrochips aufbauen kann oder sich nicht lieber auf die eigenen Stärken in der Halbleiterindustrie fokussieren sollte. Beide Optionen können einen wesentlichen Beitrag zur digitalen Souveränität der EU beitragen. Auch kann es sinnvoll sein, bewusst die Vorteile der internationalen Arbeitsteilung bei der Halbleitertechnik weiter zu nutzen. Allerdings ist darauf zu achten, dass keine einseitige Abhängigkeit von nicht-demokratischen und mit dem Westen in Konflikt befindlichen Staaten entsteht. Zudem sollten hohe Standards für Nachhaltigkeit und Klimaschutz in der Wertschöpfungskette von Mikrochips „made in Europe“ angewendet werden.

#### 4.4.2. Künstliche Intelligenz

Künstliche Intelligenz kann inzwischen immer komplexere Aufgaben bewältigen und wird großflächig in den unterschiedlichsten Bereichen von Wirtschaft und Gesellschaft eingesetzt. KI prägt dadurch zunehmend auch unseren (digitalen) Alltag. Europas noch immer großen Stärke in der akademischen Forschung im Bereich der Künstlichen Intelligenz spiegelt sich jedoch nicht in einem vergleichbaren Maße in der praktischen Anwendung oder entsprechend erfolgreiche KI-Unternehmen wider, sei es Start-Ups oder Tech-Konzerne. Im Vergleich zu den USA und China gelingt es den Mitgliedsstaaten der EU weniger gut, die eigene Stärke in der KI-Grundlagenforschung in entsprechende Produkte und wirtschaftliche Erfolge umsetzen (Zhang et al 2022). Damit werden die EU und ihre Mitgliedsstaaten zusehends abhängig von US-amerikanischer und chinesischer KI-Technologie.

Potenziell spielen KI-Anwendungen klima- und umweltpolitisch für alle drei Ebenen des Zusammenwirkens von Nachhaltigkeit und Digitalisierung (siehe Kapitel 3.1) eine wichtige Rolle. Die ökologisch-nachhaltige Gestaltung von KI-Systemen betrifft insbesondere den Stromverbrauch des Maschinellen Lernens bzw. die entsprechenden Treibhausgas-Äquivalente. Das Thema wird seit kurzem vermehrt diskutiert, da die für z. B. komplexe Sprachmodelle genutzten künstlichen neuronalen Netzwerke immer größer werden und für ihr Training auch einen wachsenden Stromverbrauch benötigen. Aus Untersuchungen

bekannt gewordene, besonders drastische Werte beruhen jedoch auf spekulative Berechnungen, die extreme, in der Praxis nicht vorkommende Fälle betrachten, und sind daher mit Vorsicht zu genießen (Strubell et al. 2019). Zudem kann ein aufwendig trainiertes künstliches neuronales Netz, z. B. ein Sprachmodell, gegebenenfalls vielfach und für einen längeren Zeitraum eingesetzt werden.

Für die Unterstützung von Nachhaltigkeitszielen durch den Einsatz von KI gibt es viele Beispiele. So kann beispielsweise der Produktionsablauf in der industriellen Fertigung mit datengetriebener Steuerung energie- und ressourceneffizienter gestaltet werden (Awasthi et al. 2021). KI könnte so eine wichtige Rolle zur Erreichung der Ziele des European Green Deal spielen. Politische Steuerung und Regulierung bedarf gerade im Hinblick auf die komplexen Probleme der Nachhaltigkeitstransformationen einer soliden informationellen Grundlage, um zielgerichtete Maßnahmen entwickeln zu können. Die Analyse großer Datensätze, die mittels KI-Technologien erst effektiv auswertbar werden, kann dabei eine wichtige Hilfe darstellen. Die Schaffung der regulativen Rahmenbedingungen, die einen besseren Austausch von und Zugang zu für die Nachhaltigkeit relevanten Daten ermöglichen, sollte daher innerhalb der EU eine hohe Priorität einnehmen.

Bezüglich sozialer Nachhaltigkeit bergen KI-Technologien deutliche Risiken. Viele konkrete Beispielfälle der letzten Jahre verdeutlichen, dass der unregulierte Einsatz von KI-Systemen die Grundrechte bedrohen kann. So weisen Systeme des Maschinellen Lernens auf Grund der verwendeten Trainingsdaten immer wieder strukturelle Verzerrungen auf, die Menschen beispielsweise auf Basis ihrer ethnischen Zugehörigkeit oder ihres Geschlechts benachteiligen (Hajian, Bonchi et al. 2016). Auch die Privatsphäre kann durch KI-basierte Überwachungssysteme wie z. B. die Gesichtserkennung bedroht werden (Smith & Miller 2022). KI-Technologien können für Manipulationen aller Art eingesetzt werden – von täuschend echt wirkenden simulierten Medien, sogenannten *Deep Fakes*, bis hin zur subtilen politischen Beeinflussung durch die gezielte Platzierung von Beiträgen in Sozialen Medien.

Mit dem KI-Gesetz (AI Act) strebt die EU die weltweit erstmalige Einrichtung eines Rechtsrahmens an, der die durch KI-Nutzung entstehende Risiken reguliert und damit eine breite gesellschaftliche Akzeptanz der KI-Nutzung garantieren soll. Das Gesetz soll den Risiken durch den Einsatz von KI frühzeitig begegnen und dabei die europäischen Werte in Form von Standards für eine „menschenzentrierte KI“ und eine „vertrauenswürdige KI“ untermauern

(Europäische Kommission, 2021). Es beansprucht Geltung für Anbieter, die außerhalb des Staatenverbundes residieren, solange sie entsprechende Anwendungen oder Ergebnisse innerhalb der EU anbieten. Nach der derzeitigen Fassung sind dabei sogar außereuropäische Nutzer von der Regulierung betroffen, falls eine auf deren Daten basierende Anwendung innerhalb des Binnenmarktes genutzt werden soll. Mit der weltweit ersten expliziten Regulierung von Künstlicher Intelligenz möchte die Europäische Union eine international prägende Vorreiterrolle einnehmen und ihre digitale Souveränität ausbauen.

Zusammenfassend lässt sich festhalten, dass bei entsprechender Nutzung und Gestaltung KI-Systeme einen wichtigen sozial-ökologischen Beitrag leisten können, im schlechtesten Fall aber auch als digitaler Brandbeschleuniger für Fehlentwicklungen dienen. Der Ansatz der vertrauenswürdigen und menschenzentrierten KI bietet Europa dabei die Chance, seine Werte in die Standards und Anwendungspraxis dieser wirkmächtigen Technologien einzuschreiben und gegebenenfalls auch weltweit zu prägen. Bei diesem Ansatz spielen bisher vor allem Aspekte der sozialen Nachhaltigkeit eine Rolle, während klima- und umweltpolitische Aspekte weitgehend außer Acht gelassen werden.

#### 4.5. IT- und Netzsicherheit

Die Zahl und Komplexität von Cyberangriffen nehmen in der EU zu und fügen der europäischen Wirtschaft und Gesellschaft jährlich großen Schaden zu. Zwar lassen sich die konkreten wirtschaftlichen Kosten bisher nicht exakt beziffern, Schätzungen belaufen sich jedoch für einige EU-Staaten auf bis zu 1,6 % des jährlichen BIP (Tofan et al. 2016). Selbst enge Verbündete spionieren europäische Ziele aus, wie spätestens durch die Enthüllungen von Edward Snowden im Jahr 2013 bekannt wurde.

Ein zentrales Element digitaler Souveränität ist daher eine möglichst hohe IT- und Netzsicherheit. Solche kann inzwischen als eine wichtige Rahmenbedingung des reibungslosen Funktionierens von Staat, Wirtschaft und Gesellschaft angesehen werden. Egal ob Behörden, Unternehmen oder grundlegende Infrastrukturen – bei mangelnder IT- und Netzsicherheit kann jederzeit eine Störung oder sogar ein grundlegender Ausfall und damit entsprechende Folgeschäden drohen. Auch Akteure, die für die Nachhaltigkeitstransformationen eine große Rolle spielen, können davon

betroffen sein. Denkbare Angriffsziele sind beispielsweise Netzinfrastrukturen und zentrale Speicher, die für ein Stromsystem, das auf erneuerbaren Energien basiert, zentral sind (Fischergoldack 2019). Durch die Digitalisierung entstehen hier potenziell neue Vulnerabilitäten. Eine möglichst hohe IT- und Netzsicherheit kann vor diesem Hintergrund als wichtiges Element für die Resilienz einer energetisch nachhaltigen Gesellschaft angesehen werden.

Mit dem 2019 in Kraft getretenen Rechtsakt zur Cybersicherheit wurde ein EU-weit einheitliches Zertifizierungssystem für Cybersicherheitsstandards von Produkten und -Dienstleistungen eingeführt, um die bisherige nationalstaatliche Fragmentierung zu überwinden (European Parliament and European Council, 2019). Damit wird der europäische Kapazitätsaufbau im Rahmen der Europäischen Cybersicherheits-Strategie bisher als relativ erfolgreich bewertet.

Zudem wurden gesamteuropäische Behörden und Netzwerke gestärkt oder neu etabliert. So erhielt die Agentur der EU für Cybersicherheit (ENISA) in Athen und Iraklio ein permanentes Mandat und eine deutliche Aufstockung der finanziellen und personellen Mittel. Im Mai 2021 wurde die Einrichtung des Europäischen Kompetenzzentrum für Cybersicherheit mit Sitz in Bukarest beschlossen. Dieses wird der Hauptknoten eines europäischen Netzwerkes von nationalen Koordinierungszentren bilden, die sich auf Innovations- und Industriepolitische Maßnahmen im Bereich der Cybersicherheit konzentrieren.

Auch wenn eine IT-Sicherheitskultur von zentraler Bedeutung ist, ersetzt diese nicht die Einschränkung der cyberkriminellen Aktivitäten durch Strafverfolgung. So lange bestimmte cyberkriminelle Gruppen den Schutz von Staaten (wie z. B. Russland und Nordkorea) genießen, sind zudem auch diplomatische Aktivitäten notwendig, die darauf hinarbeiten, diesen die Unterstützung zu entziehen (Caesar 2021).

Zusammenfassend lässt sich festhalten, dass IT- und Netzsicherheit eine elementare Grundvoraussetzung für die Resilienz und Nachhaltigkeit einer modernen digitalen Gesellschaft darstellt. Dies gilt etwa besonders mit Blick auf eine nachhaltige Energiewirtschaft, deren Infrastruktur sich durch spezifische Vulnerabilitäten auszeichnet, denen nur mit ausreichenden digitalen Sicherheitsvorkehrungen begegnet werden kann. Entsprechende europäische Behörden und Regulierungen sind dabei ein wichtiges Element digitaler Souveränität im Bereich IT- und Netzsicherheit – und damit auch ein Beitrag zu einer nachhaltigeren Entwicklung.

#### 4.6. Fazit

Die nachhaltige Gestaltung und Nutzung der Digitalisierung spielt eine zunehmend wichtigere Rolle für die europäische Transformationsziele, z. B. im Rahmen des European Green Deal. Parallel dazu sind in den letzten Jahren Fragestellungen bezüglich der digitalen Souveränität zunehmend in den Fokus gerückt. Es liegt daher eigentlich nahe, die Wechselwirkungen dieser beiden Felder systematisch zu untersuchen und in der europäischen Politikgestaltung zu berücksichtigen. Dies geschieht bisher jedoch nur geringfügig – stattdessen werden die beiden Diskurse um Nachhaltigkeit und digitale Souveränität weitgehend unverbunden nebeneinander geführt.

Diese Diskurse zusammenzuführen und daraus praxisrelevante und weitsichtige Handlungsoptionen für die Politik auf EU- und Bundesebene abzuleiten, ist jedoch ein herausforderndes Unterfangen. Dies liegt u. a. daran, dass die komplexe Thematik quer zu den etablierten ressortorientierten Politikagenden liegt und die Trennlinien der Fach-Communities überschreitet. Das Konzept der digitalen Souveränität unterliegt mit seinen vielen Bedeutungsebenen einer vielfältigen Verwendungsweise. Von der Fokussierung auf Wirtschaft und Sicherheit über die Handlungs- und Selbstbestimmungsfähigkeit jedes Einzelnen sowie des demokratischen Staates als Ganzes stehen die verschiedenen Dimensionen oft in einem Wettstreit miteinander. Bei dem vielseitigen und nicht weniger komplexen Themenfeld der Nachhaltigkeit verhält es sich ähnlich. Auch hier werden etwa soziale und ökologische Aspekte einer nachhaltigen Digitalisierung noch zu wenig mit Fragen der digitalen Souveränität verbunden. Zudem ist die „Nachhaltigkeits-Community“ sehr heterogen und fragmentiert. Dies ist zwar auch eine Stärke insoweit Akteure mit unterschiedlichsten Expertisen, Vorstellungen und Zielen für den Diskurs rund um eine nachhaltig-digitale Souveränität mobilisiert werden können, erfordert jedoch eine aktive Vernetzung und das Identifizieren von Fragestellungen, die gemeinsam adressiert werden können.

Europa hat dank seines großen Binnenmarktes, der hohen Regulierungskapazität, aber auch der eigenen wissenschaftlich-technologischen Basis und Innovationsfähigkeit die Chance, eine Führungsrolle bei einer nachhaltigen und zugleich souveränen Gestaltung der Digitalisierung zu übernehmen. Dazu müssen bestehende Potentiale für eine nachhaltige digitale Souveränität effektiver gehoben werden. Im folgenden Kapitel werden

Optionen skizziert, wie eine tiefere Beschäftigung mit den Schnittstellen zwischen digitaler Souveränität und digitaler Nachhaltigkeit unterstützt werden kann.

## 5. Ausblick: Was sollte getan werden?

Die Herausforderung ist klar umrissen: Eine Stärkung der digitalen Souveränität Europas muss von Anfang an eingebettet sein in den Rahmen der sozial-ökologischen Transformationen und soll den Pfadwechsel in Richtung der Erfüllung der Nachhaltigkeitszielen erleichtern. Eine digital-nachhaltige Souveränität ist dabei kein endgültig erzielbarer, statischer Endzustand, sondern ein dynamischer Prozess, der mit einem Risikomanagement von nicht vermeidbaren Abhängigkeiten verbunden bleiben wird.

Aus unserer Betrachtung der Diskussion lassen sich folgende vier zentralen Handlungsfelder ableiten, digitale Souveränität und digitale Nachhaltigkeit stärker miteinander zu verbinden:

- a) Entwicklung eines gemeinsamen Zielbildes der „digitalen Souveränität“ und deren Zusammenhang mit Nachhaltigkeit (Warum?)
- b) Analyse der Wirkungsweisen und Interdependenzen von Regulation, Investition und Intervention zur digitalen Nachhaltigkeit und Souveränität auf nationaler und europäischer Ebene (Wie wirken verschiedene Effekte und Instrumente?)
- c) Entwicklung einer EU-Strategie, um die nachhaltige und souveräne Gestaltung der Digitalisierung langfristig gestalten zu können (Wie kann Transformation gelingen?)
- d) Entwicklung eines integrierten Multi-Stakeholder-Ansatzes (Wer muss für ein Gelingen einbezogen werden?)

Im Folgenden werden für diese vier Handlungsfelder Ansätze skizziert, wie sie adressiert werden können. Die ersten beiden Handlungsfelder führen dabei zu entsprechenden Forschungsbedarfen, während bei den letzten beiden der Fokus auf Maßnahmen und der Gestaltung von Prozessen liegt.

### **a) Warum? Entwicklung eines gemeinsamen Zielbildes der „digitalen Souveränität“ und deren Zusammenhang mit Nachhaltigkeit**

Digitale Souveränität ist ein Konzept mit vielen Bedeutungsebenen und oftmals nur schwer differenzierbar von anderen Konzepten wie etwa „technologischer Souveränität“ und „strategischer Autonomie“. Diese Begriffe werden zu oft sehr breit interpretiert und unterschiedlich konnotiert, was eine zielgerichtete

Diskussion erschwert. Zudem fehlt bislang eine vertiefte Auseinandersetzung mit der Frage, wie digitale Souveränität – auf europäischer wie nationaler Ebene – mit nachhaltiger Entwicklung zusammengedacht werden kann.

Folgende Optionen schlagen wir vor:

- Kartierung der bereits bestehenden Diskurse um digitale Souveränität und nachhaltige Digitalisierung auf nationaler und europäischer Ebene
- Identifikation von Überschneidungen, Anknüpfungspunkte, gemeinsamen Zielen und Zielkonflikten in den Diskursen sowie relevanten Akteuren und Stakeholdern auf der Basis dieser Kartierung
- Zusammenführen der Expert\*innenkreise und Fachcommunities aus den Bereichen nachhaltige Digitalisierung und digitale Souveränität
- Entwicklung eines Zielbildes einer wünschenswerten digital-nachhaltigen Souveränität und Ansätze, dieses zu operationalisieren (etwa in einem *Index für digitale Souveränität und Nachhaltigkeit*)
- Förderung von Forschungsansätzen, die Zieldimensionen digitale Souveränität und Nachhaltigkeit weiter erkunden und Möglichkeiten entwickeln, diese zu adressieren.

**b) Wie wirken verschiedene Effekte und Instrumente? Analyse der Wirkungsweisen und Interdependenzen von Regulation, Investition und Intervention zur digitalen Nachhaltigkeit und Souveränität auf nationaler und europäischer Ebene**

Wie unsere Ausführungen gezeigt haben, besteht bereits eine Vielzahl an Ansätzen auf EU-Ebene, die Herausforderungen der digitalen Souveränität adressieren. Hier gilt es die Wirkungsweisen dieser Regularien in Bezug auf nachhaltige Digitalisierung zu prüfen und Ansätze zu definieren, wie Nachhaltigkeit gestärkt werden kann. Gleiches gilt für Investitionen in Branchen, die die digitale Souveränität Europas und Deutschlands stärken sollen. Wie können diese so gestaltet werden, dass sie gleichzeitig eine nachhaltige Digitalisierung befördern?

Folgende Optionen schlagen wir vor:

- Strukturierte Analyse der bestehenden und geplanten Regularien auf EU-Ebene (bspw. zu KI, Chipproduktion, Daten-Governance etc.) in Bezug auf potenzielle Wirkungen auf eine nachhaltige Entwicklung – und vice versa:

Untersuchung von Ansätzen zur nachhaltigen Gestaltung der Digitalisierung und inwiefern diese auf digitale Souveränität einzahlen können

- Mapping von Regulations- und Förderansätzen im Bereich digitale Souveränität und Nachhaltigkeit, um „blinde Flecken“ zu identifizieren
- Analyse privatwirtschaftlicher und staatlicher Investitionen auf die Entwicklung einer digital-nachhaltigen Souveränität
- Review der Erfolge und nicht erfüllter Erwartungen bestehender Cloud-Infrastruktur-Projekte Deutschlands und der EU, um daraus für künftige Planungs- und Umsetzungsprozesse zu lernen und Fehler zu vermeiden

### c) Wie kann Transformation gelingen? Entwicklung einer EU-Strategie, um die nachhaltige und souveräne Gestaltung der Digitalisierung langfristig gestalten und steuern zu können

Erkenntnisse aus den unter a) und b) skizzierten Forschungsmaßnahmen sollten zu einer gemeinsamen, langfristig verfolgbaren europäischen Strategie hin zu einer nachhaltigkeitsorientierten digitalen Souveränität beitragen. Dabei ist eine klare Priorisierung gefragt.

Wir schlagen daher eine Konzentration auf die folgenden Aspekte vor:

- **Standardisierung vorantreiben:** Verbreitung von europäischen Industriestandards und Regulierungsansätzen, wie beispielsweise die DSGVO (GDPR), als Erfahrungsgrundlage, um digital-nachhaltige Technologien im EU-Binnenmarkt und international zu fördern
- **Investitionsanreize setzen:** Verankerung von Mechanismen im europäischen Binnenmarkt, die ökologische Ziele und digitale Souveränität bei öffentlichen wie privaten Investitionsentscheidungen in digitale Technologien und Infrastrukturen stärken. Nachhaltigkeits- und Risikobewertungen hinsichtlich digitaler Souveränität sollten dazu bei Finanzdaten der Digitalwirtschaft eine viel größere Rolle spielen und in diesem Bereich aktive Nachhaltigkeits-Ratingagenturen etabliert oder aufgewertet werden.
- **Innovationen fördern:** Die europäische Digital- und Datenwirtschaft sollte zu einem wettbewerbsfähigen Exporteur von fairen, nachhaltigen digitalen Produkten und Dienstleistungen ausgebaut werden, während bestehende Ansätze für ein entsprechendes Innovationssystem

fortentwickelt werden. Lernräume für eine entsprechend ausgerichtete digitale Transformation wie Reallabore oder Innovationshubs sollten auf- und ausgebaut werden.

- **Gemeinwohlorientierung stärken:** Breite Diskussion und Förderung gemeinwohlorientierter Ansätze, wie beispielsweise im Bereich Daten-Governance, durch die eine nachhaltige und souveräne Digitalisierung gestärkt werden können
- **Internationale Kooperationen ausbauen:** Stärkung strategischer bi- und multilateraler Partnerschaften, etwa mit Indien und den Ländern Afrikas und Südostasiens, aber auch mit europäischen und transatlantischen Partnern. Neben der gemeinsamen Entwicklung von Standards für digitale Souveränität und Nachhaltigkeit sollte auch in der Forschungs- und Technologiepolitik und im Austausch von Best Practices zusammengearbeitet werden.
- **Langzeitorientierung stärken:** Bei politischen und administrativen Entscheidungen, die die Digitalisierung betreffen, sollten Expertisen für eine systematische, strategische Vorausschau ausgebaut und besser in institutionelle Entscheidungsprozesse eingebaut werden.

#### **d) Wer muss für ein Gelingen einbezogen werden? Entwicklung eines integrierten Multi-Stakeholder-Ansatzes**

Um eine hohe Wirkung zu entfalten, sollten Maßnahmen und Ansätze für eine nachhaltigkeitsorientierte digitale Souveränität in einem integrierten Multi-Stakeholder Ansatz entwickelt und umgesetzt werden. Nur so kann sichergestellt werden, dass die relevanten Fragestellungen adressiert und notwendigen Wissensbestände dafür eingebracht sowie tragfähige Lösungen entwickelt werden.

Folgende Optionen schlagen wir vor:

- Teilhabe und Partizipation der Gesellschaft am Diskurs um die Gestaltung einer nachhaltigen und digital-souveränen Zukunft von Anfang an einen zentralen Stellenwert einräumen
- Effektive Zusammenarbeit und Vernetzung einer Vielzahl an Akteuren (staatliche Institutionen und die öffentliche Verwaltung der EU-Mitgliedsländer, Unternehmen und Zivilgesellschaft sowie Medien, Nichtregierungsorganisationen und Think Tanks) zu Fragen der digitalen

Nachhaltigkeit und Souveränität voranbringen und entsprechende Formate etablieren bzw. ausbauen

- Ressort- und länderübergreifende Koordinationsstellen für Maßnahmen im Bereich digitaler Nachhaltigkeit und digitaler Souveränität stärken, um die Handlungskohärenz zu erhöhen. Die unterschiedlichen Ausgangslagen und Anforderungen relevanter Akteur\*innen erfordern einen hohen Koordinationsaufwand und verbesserte Schnittstellen.

Die hier aufgeführten Vorschläge haben keinen Anspruch auf Vollständigkeit. CO:DINA wird diese zusammen mit einer Vielzahl an Akteuren, die in der Debatte um digitale Souveränität und Nachhaltigkeit beteiligt sind, prüfen, hinterfragen und weiterentwickeln.

## 6. Literatur

- Awasthi, S., Travieso-González, C. M., Sanyal, G., & Kumar Singh, D. (Eds.). (2021). Artificial intelligence for a sustainable industry 4.0. Springer. <https://doi.org/10.1007/978-3-030-77070-9>
- Bauer, M., & Erixon, F. (2020). Europe's Quest for Technology Sovereignty: Opportunities and Pitfalls. European Centre for International Political Economy. [https://ecipe.org/wp-content/uploads/2020/05/ECI\\_20\\_OccPaper\\_02\\_2020\\_Technology\\_LY02.pdf](https://ecipe.org/wp-content/uploads/2020/05/ECI_20_OccPaper_02_2020_Technology_LY02.pdf)
- Bauer, S. (2022). Verbesserter Schutz in den Sozialen Netzwerken: Der EU Digital Services Act. Policy Spotlight Nr 2 (Verbundvorhaben CO:DINA, Hrsg.). IZT – Institut für Zukunftsstudien und Technologiebewertung; Wuppertal Institut für Klima, Umwelt, Energie.
- Beer, F., & Rammler, S. (2021). Zwischen den Zeitenwenden: Transformative Resilienz als Leitbild der Zukunftsgestaltung. In J. Radloff & A. Oxenfarth (Eds.), Politische Ökologie: 39. Jahrgang, 166 (September 2021). Resiliente Zukünfte: Mut zum Wandel (pp. 17–25). oekom verlag. [https://www.oekom.de/\\_files\\_media/zeitschriften/artikel/POE\\_2021\\_03\\_17.pdf](https://www.oekom.de/_files_media/zeitschriften/artikel/POE_2021_03_17.pdf)
- Bendiek, A. (2016). Die Globale Strategie für die Außen- und Sicherheitspolitik der EU. [https://www.swp-berlin.org/publications/products/aktuell/2016A44\\_bdk.pdf](https://www.swp-berlin.org/publications/products/aktuell/2016A44_bdk.pdf)
- Bendig, T., Ganten, P., Geese, E., Krosta-Hartl, P., Neuburger, R., & Schauf, T. (2020). Digitale Souveränität und Resilienz: Voraussetzungen, Treiber und Maßnahmen für mehr Nachhaltigkeit: Digital-Gipfel-Plattform 2 "Innovative Digitalisierung der Wirtschaft" – Fokusgruppe Digitale Souveränität. Berlin. [https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2020/digitale-souveraenitaet-und-resilienz.pdf?\\_\\_blob=publicationFile&v=8](https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2020/digitale-souveraenitaet-und-resilienz.pdf?__blob=publicationFile&v=8)
- Bluestone, D. (2021). State Of GDPR In 2021: Key Updates And What They Mean. <https://www.smashingmagazine.com/2021/02/state-gdpr-2021-key-updates/>
- Bradford, A. (2020). The Brussels Effect: How the European Union rules the world. Oxford University Press. <https://doi.org/10.1093/oso/9780190088583.001.0001>
- Bria, F. (2022). Digitalisierung: Big Democracy soll Big Tech und Big State überwinden. Friedrich-Ebert-Stiftung. <https://www.fes.de/abteilung-analyse-planung-und-beratung/artikelseite-apb/digitalisierung-big-democracy-soll-big-tech-und-big-state-ueberwinden>
- Brundtland, G. (1985). World Commission on environment and development. Environmental Policy and Law, 14(1), 26–30. [https://doi.org/10.1016/S0378-777X\(85\)80040-8](https://doi.org/10.1016/S0378-777X(85)80040-8)

- Caesar, E. (2021, April 19). The Incredible Rise of North Korea's Hacking Army. The New Yorker. <https://www.newyorker.com/magazine/2021/04/26/the-incredible-rise-of-north-koreas-hacking-armycaesar>
- Campbell, D., & Hulme, R. (2001). The winner-takes-all economy. The McKinsey Quarterly, 82. <https://link.gale.com/apps/doc/A72524620/AONE?u=anon~5735f3e5&sid=googleScholar&xid=c6b0a058>
- Cory, N., & Dascoli, L. (2021). How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them. Information Technology and Innovation Foundation. <https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost>
- Dachwitz, I. (2022). Data-Act-Verordnung: Neues Datengesetz der EU erntet massive Kritik aus der Zivilgesellschaft. <https://netzpolitik.org/2022/data-act-verordnung-neues-datengesetz-der-eu-erntet-massive-kritik-aus-der-zivilgesellschaft/#netzpolitik-pw>
- Eidler, J., Blind, K., Frietsch, R., Kimpeler, S., Kroll, H., Lerch, C., Reiss, T., Roth, F., Schubert, T., Schuler, J., & Walz, R. (2020). Technology sovereignty. From demand to concept. Karlsruhe. Fraunhofer Institute for Systems and Innovation Research. [https://www.isi.fraunhofer.de/content/dam/isi/dokumente/publikationen/technology\\_sovereignty.pdf](https://www.isi.fraunhofer.de/content/dam/isi/dokumente/publikationen/technology_sovereignty.pdf)
- Europäische Kommission (2020). Shaping Europe's digital future: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Brussels. European Commission. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0067>
- Europäische Kommission (2021). In-depth reviews of strategic areas for Europe's interests. [https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-industrial-strategy/depth-reviews-strategic-areas-europes-interests\\_en#hydrogen](https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-industrial-strategy/depth-reviews-strategic-areas-europes-interests_en#hydrogen)
- Europäische Kommission (2022). European Alliance for Industrial Data, Edge and Cloud. <https://digital-strategy.ec.europa.eu/en/policies/cloud-alliance>
- European External Action Service (2016). Shared Vision, Common Action: A Stronger Europe: A Global Strategy for the European Union's Foreign And Security Policy. [https://eeas.europa.eu/sites/default/files/eugs\\_review\\_web\\_0.pdf](https://eeas.europa.eu/sites/default/files/eugs_review_web_0.pdf)
- FAZ (2022, Januar 20). „Bis 2030 sollte ein Fünftel der Mikrochip-Produktion in Europa erfolgen“. Frankfurter Allgemeine Zeitung. <https://www.faz.net/aktuell/wirtschaft/digitec/eu-kommission-stellt-bald-entwurf-zur-mikrochip-produktion-in-europa-vor-17741924.html>
- Falk, S. & Schroeder, W. (2022). Digitale Souveränität - Ein Narrativ des Fortschritts. Discussion Paper (Das Progressive Zentrum, Hrsg.). Berlin. Zugriff am 30.05.2022. Verfügbar unter: <https://www.progressives-zentrum.org/wp->

content/uploads/2022/05/DigitaleSouveraenitaet\_Discussion-Paper\_Das-Progressive-Zentrum.pdf

- Fischer, L. (2019). IT security for functional resilience in energy systems: effect-centric IT security. In M. Ruth & S. Gössling-Reisemann (Eds.), Handbook on resilience of socio-technical systems (pp. 316–340). Edward Elgar Publishing. <https://doi.org/10.4337/9781786439376.00023>
- Goldacker, G. (2017). Digitale Souveränität. Berlin. <https://www.oeffentliche-it.de/documents/10181/14412/Digitale+Souver%C3%A4nit%C3%A4t>
- Greenleaf, G. (2021). Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance. Privacy Laws & Business International Report, 169(1). <https://doi.org/10.2139/ssrn.3836348>
- Gupta, U., Kim, Y. G., Lee, S., Tse, J., Lee, H.-H. S., Wei, G.-Y., Brooks, D., & Wu, C.-J. (2020, Oktober 28). Chasing Carbon: The Elusive Environmental Footprint of Computing. <http://arxiv.org/pdf/2011.02839v1>
- Hajian, S., Bonchi, F., & Castillo, C. (2016). Algorithmic Bias: From Discrimination Discovery to Fairness-aware Data Mining. In B. Krishnapuram, M. Shah, A. Smola, C. Aggarwal, D. Shen, & R. Rastogi (Eds.), Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (pp. 2125–2126). ACM. <https://doi.org/10.1145/2939672.2945386>
- Heyen, D. A., Gensch, C.-O., Gsell, M., Hacker, F., Minnich, L., Scherf, C.-S., Doll, C., Grimm, A., Marcheider-Weidemann, F., Ostertag, K., & Sartorius, C. (2022). Strukturwandel zu einer Green Economy: Analysen und Empfehlungen zur Gestaltung. Öko-Institut; Fraunhofer-Institut für System und Innovationsforschung. [https://www.umweltbundesamt.de/sites/default/files/medien/479/publikationen/uib\\_04-2022\\_strukturwandel\\_zu\\_einer\\_green\\_economy.pdf](https://www.umweltbundesamt.de/sites/default/files/medien/479/publikationen/uib_04-2022_strukturwandel_zu_einer_green_economy.pdf)
- Holm-Hadulla, M., Bug, H., & Winkelmann, K. (2020). Digital Markets Act und Digital Services Act: Die Europäische Kommission stellt zwei Verordnungsentwürfe zur Reform der Digital- und Wettbewerbsregeln vor.
- Kaloudis, M. (2021). Sovereignty in the Digital Age – How Can We Measure Digital Sovereignty and Support the EU’s Action Plan? New Global Studies. <https://doi.org/10.1515/ngs-2021-0015>
- Kaur, D. (TechHQ, Hrsg.). (2021). The era of hyperscale data centers is upon us. Zugriff am 30.05.2022. Verfügbar unter: <https://techhq.com/2021/03/the-era-of-hyperscale-data-centers-is-upon-us/>
- Kleinhans, J.-P., & Lee, J. (Dezember 2021). China's rise in semiconductors and Europe: Recommendations for policy makers. Berlin. [https://www.stiftung-nv.de/sites/default/files/chinas\\_rise\\_in\\_semiconductors\\_and\\_europe.pdf](https://www.stiftung-nv.de/sites/default/files/chinas_rise_in_semiconductors_and_europe.pdf)
- Koenig, N. (2019). The ‘geopolitical’ European Commission and its pitfalls. [https://www.hertie-school.org/fileadmin/user\\_upload/Policy\\_Brief\\_Nicole\\_geopolitical\\_commission.pdf](https://www.hertie-school.org/fileadmin/user_upload/Policy_Brief_Nicole_geopolitical_commission.pdf)

- Köhn, M., Gröger, J., & Stobbe, L. (2020). Energie- und Ressourceneffizienz digitaler Infrastrukturen. [https://doi.org/10.1007/978-3-658-06045-9\\_8](https://doi.org/10.1007/978-3-658-06045-9_8)
- Lippert, B., Ondarza, N. von, & Perthes, V. (2019). European Strategic Autonomy. Actors, Issues, Conflicts of Interest. Berlin.
- Meadows, D. H., Meadows, D. L., & Randers, J. (1974). The limits to growth: A report for the Club of Rome's Project on the Predicament of Mankind (2. ed.). Universe Books.
- Mearian, L. (2021). Apple gives in on right-to-repair. <https://www.computerworld.com/article/3641328/apple-gives-in-on-right-to-repair.html>
- Michael, K., Kobran, S., Abbas, R. & Hamdoun, S. (2019) Privacy, Data Rights and Cybersecurity: Technology for Good in the Achievement of Sustainable Development Goals. Tufts University, Medford, Massachusetts, USA: IEEE International Symposium on Technology and Society 14-16 November 2019.
- Morgan, S. (2018). Fake news, disinformation, manipulation and online tactics to undermine democracy. *Journal of Cyber Policy*, 3(1), 39-43. <https://doi.org/10.1080/23738871.2018.1462395>
- Morozov, E. (2021). Chips with everything. *Le Monde diplomatique*. <https://mondediplo.com/2021/08/03morozov>
- Nestoras, A. 2022. The 'Brussels Effect' in Digitalisation and the Future of Transatlantic Relations (European Liberal Forum, ed.). <https://doi.org/10.53121/ELFPB4>
- Noyan, O. (2021, November 19). Cracks appear as Gaia-X celebrates its progress. Euractiv. <https://www.euractiv.com/section/digital/news/cracks-appear-as-gaia-x-celebrates-its-progress/>
- Öko-Institut & Institut für Zukunftsstudien und Technologiebewertung (IZT) (2021). Deutschland auf dem Weg zur Klimaneutralität: Welche Chancen und Risiken ergeben sich durch die Digitalisierung? Freiburg, Berlin. [https://www.kfw.de/PDF/Download-Center/Konzernthemen/Research/PDF-Dokumente-Studien-und-Materialien/KfW\\_Digitalisierung\\_Klimaschutz.pdf](https://www.kfw.de/PDF/Download-Center/Konzernthemen/Research/PDF-Dokumente-Studien-und-Materialien/KfW_Digitalisierung_Klimaschutz.pdf)
- Pohle, J. (2020). Digital sovereignty: A new key concept of digital policy in Germany and Europe. Berlin. <https://www.kas.de/documents/252038/7995358/Digital+sovereignty.pdf/a8d0cb4b-c777-3e72-1bc7-b5fda656329a?version=1.0&t=1608034389334>
- Ramesohl, S., & Gunnemann, A. (2021). Plattformregulierung für die Nachhaltigkeitstransformation: Ansatzpunkte und Handlungsbedarfe für eine Plattformökonomie im Dienst des sozial-ökologischen Wandels (CODINA Positionspapier No. 5). [https://codina-transformation.de/wp-content/uploads/Positionspapier\\_Plattformregulierung-fu%CC%88r-die-Nachhaltigkeitstransformation.pdf](https://codina-transformation.de/wp-content/uploads/Positionspapier_Plattformregulierung-fu%CC%88r-die-Nachhaltigkeitstransformation.pdf)

- Rammler, S., Thomas, D., Uhl, A., Beer, F. (2021). Resiliente Mobilität. Ansätze für ein krisenfestes und soziales Verkehrssystem. Friedrich-Ebert-Stiftung, 10. <http://library.fes.de/pdf-files/a-p-b/18367.pdf>
- Reichel, A. (2018). Nachhaltige Digitalisierung, digitale Nachhaltigkeit? In H. Rogall, H. C. Binswanger, F. Ekardt, A. Grothe, W.-D. Hasenclever, I. Hauchler, M. Jänicke, K. Kollmann, N. V. Michaelis, H. G. Nutzinger, & G. Scherhorn (Eds.), *Jahrbuch Nachhaltige Ökonomie: 6 (2018/2019)*. Im Brennpunkt: Zukunft des nachhaltigen Wirtschaftens in der digitalen Welt. Metropolis Verlag.
- Roberts, H., Cows, J., Casolari, F., Morley, J., Taddeo, M., & Floridi, L. (2021). Safeguarding European values with digital sovereignty: an analysis of statements and policies. *Internet Policy Review*, 10(3). <https://doi.org/10.14763/2021.3.1575>
- Smith, M., & Miller, S. (2022). The ethical application of biometric facial recognition technology. *AI & Society*, 37(1), 167–175. <https://doi.org/10.1007/s00146-021-01199-9>
- Stafford, P. (2019). Winner-takes-all digital economy poses risk for capital markets. *Financial Times*. <https://www.ft.com/content/0b660446-1827-11ea-9ee4-11f260415385>
- Sternisko, A., Cichocka, A., & van Bavel, J. J. (2020). The dark side of social movements: Social identity, non-conformity, and the lure of conspiracy theories. *Current Opinion in Psychology*, 35, 1–6. <https://doi.org/10.1016/j.copsyc.2020.02.007>
- Strubell, E., Ganesh, A., & McCallum, A. (2019, June 5). Energy and Policy Considerations for Deep Learning in NLP (Proceedings of the 57th Annual Meeting of the Association for Computational Linguistics). Stroudsburg, PA, USA. Association for Computational Linguistics.
- Timmers, P. (2019). Strategic Autonomy and Cybersecurity. EU Cyber Direct. [https://euclid.s3.eu-central-1.amazonaws.com/euclid/assets/RfT\\_Rvvh/paul-timmers-strategic-autonomy-may-2019-eucyberdirect.pdf](https://euclid.s3.eu-central-1.amazonaws.com/euclid/assets/RfT_Rvvh/paul-timmers-strategic-autonomy-may-2019-eucyberdirect.pdf)  
<https://doi.org/10.1007/s13347-018-0328-0>
- Tofan, D., Nikolakopoulos, T., & Darra, E. (2016). The cost of incidents affecting CIIs: Systematic review of studies concerning the economic impact of cyber-security incidents on critical information infrastructures (CII). <https://www.enisa.europa.eu/publications/the-cost-of-incidents-affecting-ciis/@@download/fullReport>
- WBGU (2019). Unsere gemeinsame digitale Zukunft. Berlin. <https://www.wbgu.de/de/publikationen/publikation/unsere-gemeinsame-digitale-zukunft>
- Zhang, D., Mishra, S., Brynjolfsson, E., Etchemendy, J., Ganguli, D., Grosz, B., Lyons, T., Manyika, J., Niebles, J. C., Sellitto, M., Shoham, Y., Clark, J., & Perrault, R. (2021). The AI Index 2021 Annual Report. Human-Centered AI Institute. <https://arxiv.org/ftp/arxiv/papers/2103/2103.06312.pdf>

Zhang, D., Maslej, N., Brynjolfsson, E., Etchemendy, J., Lyons, T., Manyika, J., Ngo, H., Niebles, J.C., Sellitto, M., Sakhaee, E., Shoham, Y. (2022). The AI Index 2022 Annual Report. Stanford Institute for Human-Centered AI, Stanford University

Zygmuntowski, J. J., Zoboli, L., & Nemitz, P. F. (2021). Embedding European values in data governance: a case for public data commons. *Internet Policy Review*, 10(3). <https://doi.org/10.14763/2021.3.1572>

## Über die Autor\*innen

### **Kerstin Fritzsche**

Kerstin Fritzsche ist Politikwissenschaftlerin und arbeitet zu den Chancen und Herausforderungen digitaler Technologien für den sozial-ökologischen Wandel. Bis Oktober 2021 leitete sie das Forschungsfeld Digitalisierung am IZT – Institut für Zukunftsstudien und Technologiebewertung in Berlin und arbeitet nun im öffentlichen Dienst zu digitalpolitischen Themen.

### **Julia Pohle**

#### **WZB – Wissenschaftszentrum Berlin für Sozialforschung**

Dr. Julia Pohle ist Wissenschaftlerin am Wissenschaftszentrum Berlin für Sozialforschung (WZB) und assoziierte Forscherin an der Brussels School of Governance. Sie arbeitet und publiziert zu Themen der Globalen Kommunikationspolitik und der Internet Governance auf nationaler und globaler Ebene.

### **Steffen Bauer**

#### **IZT – Institut für Zukunftsstudien und Technologiebewertung**

Steffen Bauer ist wissenschaftlicher Mitarbeiter am IZT – Institut für Zukunftsstudien und Technologiebewertung. Er arbeitet zu den Chancen und Risiken neuer digitaler Technologien und deren Regulierung. Ein Fokus liegt dabei auf KI-Systemen. Steffen Bauer arbeitet unter anderem an Forschungsprojekten für das Bundesministerium für Umwelt, Naturschutz und nukleare Sicherheit und die Kreditanstalt für Wiederaufbau.

### **Fabio Haenel**

Fabio Haenel koordinierte von Oktober 2021 bis März 2022 zusammen mit Dr. Stephan Ramesohl das Projekt "CO:DINA – Transformationsroadmap Digitalisierung und Nachhaltigkeit". Er forscht zu den Chancen und Herausforderungen durch Innovation und neuartigen Technologieentwicklungen.

Felix Eichbaum

**IZT – Institut für Zukunftsstudien und Technologiebewertung**

Felix Eichbaum arbeitet als studentischer Mitarbeiter im Forschungsbereich Digitalisierung am IZT. Während seines Bachelorstudiums der Wissenschaftskommunikation beschäftigte er sich mit transdisziplinärer Forschung sowie dem Verhältnis von Wissenschaft und Öffentlichkeit. Gegenwärtig absolviert er ein Masterstudium mit dem Schwerpunkt Wissenschaftsphilosophie an der TU Berlin.

## 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 und nukleare Sicherheit (BMU) 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](mailto:info@izt.de)  
Internet: [www.izt.de](http://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](mailto:info@wupperinst.org)  
Internet:  
[www.wupperinst.org](http://www.wupperinst.org)



Weitere Veröffentlichungen  
unter.

[www.codina-  
transformation.de](http://www.codina-transformation.de)