Freiheit by Design in digitalen Infrastrukturen

Marit Hansen, Andreas Baur und Felix Bieker

Zusammenfassung
Digitale Infrastrukturen sind die Basis für die Digitalisierung. Von ihrer Gestaltung hängt der Grad der Freiheit von Individuen und Gesellschaft angesichts der technischen Evolution ab. Je größer eine Abhängigkeit von den Infrastrukturen ist, je größer die Abhängigkeiten und Ungleichgewichte innerhalb dieser sind und je weniger sich die Nutzenden ihnen entziehen können oder wollen, desto wichtiger ist ein faires Design, das insbesondere vor einem Machtmissbrauch schützt. In diesem Beitrag beschreiben wir die grundlegende Relevanz heutiger digitaler Infrastrukturen und erläutern, welche unerwünschten Effekte damit einhergehen. Im Mittelpunkt stehen Ansatzpunkte für die freiheitliche und demokratische Gestaltung digitaler Infrastrukturen.

1. Einleitung

„Freiheit in digitalen Infrastrukturen" – dieses Thema wählte die Plattform Privatheit für ihre Jahreskonferenz 2024. „Freiheit" wird in diesem Zusammenhang als Abwehr von ungerechtfertigter Machtausübung und Schutz vor Machtmissbrauch verstanden – eine Voraussetzung für individuelle Selbstentfaltung und kollektive Selbstbestimmung. Freiheit ist also zentral für die Grundrechte jeder Person und für unsere Demokratie.

Digitale Infrastrukturen sind das technische Rückgrat unserer Gesellschaft. Ohne das Vorhandensein von Infrastrukturen funktionieren weder Kommunikation noch Vernetzung in der digitalen Welt. Das betrifft nicht nur den individuellen elektronischen Austausch zwischen Menschen oder die Nutzung von Informations- oder Unterhaltungsangeboten, sondern Finanzwesen, Energieversorgung, Güteraustausch, Mobilität und der Gesundheitsbereich sind heute zu großen Teilen ohne digitale Infrastrukturen nicht denkbar.

Wie viel individuelle und kollektive Freiheit gelebt werden kann, hängt stark von der Gestaltung der digitalen Infrastrukturen ab. In diesem Beitrag zeigen wir, wie heutige digitale Infrastrukturen diese Freiheit gefährden, statt ihre Ausübung zu unterstützen. Analog zu den Prinzipien von „Datenschutz by Design" aus der Datenschutz-Grundverordnung (DSGVO) und „Security by Design" aus der Cyberresilienz-Verordnung schlagen wir vor, bei der Gestaltung von digitalen Infrastrukturen auch das Prinzip von „Freiheit by Design" als Richtschnur anzulegen.

Im Folgenden stellen wir digitale Infrastrukturen und ihre Problemfelder dar (2.), führen bestehende Ansätze aus dem Bereich der Infrastrukturstudien ein, die eine umfassende Analyse ermöglichen (3.), und zeigen Ansatzpunkte für die freiheitliche und demokratische Gestaltung digitaler Infrastrukturen auf (4.), bevor wir mit einem Ausblick aufzeigen, wie wir zu solchen Lösungen gelangen können (5.).

2. Digitale Infrastrukturen

Unter digitalen Infrastrukturen versteht man „netzartige sozio-technische Systeme, die verlässlich einen einheitlichen Satz von Leistungen anbieten, die von Interessierten als Grundlagen des menschlichen Zusammenlebens, als Eröffnung von Handlungsmöglichkeiten und als Schutz gegenüber Lebensrisiken genutzt werden können – wie für Kommunikation, Energieversorgung, Güteraustausch, Mobilität oder Unterhaltung".[1]

Larkin (2013, S. 329, eig. Übersetzung) hebt hervor, dass Infrastrukturen nicht nur Objekte oder Technologien sind, sondern „Objekte, die die Grundlage für das Funktionieren anderer Objekte bilden". Technologische Konzepte wie Interoperabilität und Standardisierung sind daher für das Funktionieren einer Infrastruktur zentral.

Die systemische und grundlegende Bedeutung von Infrastrukturen lässt sich nicht nur daran zeigen, dass sie andere Technologien ermöglichen, sondern auch, darin, dass sie darauf aufbauende Technologien und soziale Praktiken prägen und normieren. Ein besonderes Augenmerk auf die normsetzende und handlungsbeeinflussende Eigenschaft von Infrastrukturen haben DeNardis und Musiani (2016) mit dem Konzept der „*Governance by Infrastructure*" gelegt. Infrastrukturen werden dabei auch als Rohrleitungen unterhalb des Sozialen, oder, wie Star (1999) es ausdrückt, als „unsichtbare Arbeit" verstanden. Infrastrukturen entfalten eine ermöglichende, aber auch handlungseinschränkende Wirkung entlang den in ihr angelegten Normen und Werten (Values-in-Design-Ansatz).

Infrastruktur wirkt sich auf Praktiken und Nutzungen aus und kann so die bewusste Regulierung oder Steuerung durch vom Menschen geschaffene Technologie und deren Wirkungen über die Wirkung des Rechts hinaus verlängern. Infrastrukturen können deshalb auch als *frozen governance*

1 Aus dem Text der Plattform Privatheit zur Jahreskonferenz 2024, https://plattform-privatheit.de/p-prv/jahreskonferenzen/jahreskonferenz-2024.php.

verstanden werden, die sich in den Materialien, Technologien, Institutionen und Praktiken von Infrastrukturen niederschlagen und dadurch langfristig auf das Soziale wirken. Gleichzeitig geht das Verständnis von *frozen governance* nicht weit genug, da es davon ausgeht, dass es nur das intentionale oder klassische politische Regieren durch Technologie übersetzt oder verlängert wird, was unbeabsichtigte Wirkungen versteckt.

Diese Formen der Governance und Handlungsbeeinflussung lassen sich auch unter dem Schlagwort der infrastrukturellen Macht verstehen und analysieren. Macht wird hierbei nicht nur in einer direkten Weise verstanden, also im Sinne von *power to* und *power over. Power to* bezeichnet die eigenen Handlungsmöglichkeiten und *power over* die Möglichkeit, andere zu Handlungen zu zwingen oder an diesen zu hindern. Einem strukturellen, auf Foucaults Arbeiten aufbauenden Verständnis nach wird Macht auch dann ausgeübt, wenn bestimmte Handlungen, Wissen und Identitäten ermöglicht oder erschwert werden – also die Grundlagen dafür beeinflusst werden (Haugaard 2022).

Digitale Infrastrukturen wie Clouds ermöglichen nicht nur KI-Anwendungen, sondern sie bedingen und prägen die auf der Infrastruktur aufbauenden Technologien und legen fest, was überhaupt möglich ist (Rieder 2020). Es sind die Infrastrukturen selbst, die infrastrukturelle Macht ausüben, nicht nur die Unternehmen und Betreiber:innen dieser Technologien. Für van Dijck u. a. (2019) ist es vor allem die Möglichkeit, Standards zu setzen, Plattform- und Netzwerkeffekte sowie Zugriff auf die anfallenden Nutzungsdaten, die infrastrukturelle Macht ausmachen. Luitse (2024, eig. Übersetzung) betont den polit-ökonomischen Anteil von infrastruktureller Macht, da diese Infrastrukturen nicht nur die darauf aufbauenden Technologien und Gesellschaften beeinflussen, sondern durch „die Fähigkeit eine Einheit aus Rechen-Infrastrukturen, KI-Entwicklungspraxis, Diskursen und Governance-Prozessen zu formen, mit dem Ziel und Effekt die Marktmacht der Infrastruktur zu stärken."

Die vertikale Integration von Big-Tech-Unternehmen und vor allem großen Cloud-Anbieter:innen, die von Hardware über Rechenzentren, Cloud-Systemen, APIs und Software bis hin zu KI-Trainingsmöglichkeiten, Trainingsdaten und -modellen reicht, ist ein zentraler Faktor der infrastrukturellen Macht (Luitse 2024, 33).

Infrastrukturen und die Kontrolle über sie üben auch direkte Macht aus: zum Beispiel durch die Entscheidung darüber, wer die darüber angebotenen Leistungen erhält und wer dagegen das Angebot nicht oder nur

eingeschränkt nutzen kann. Dies kann explizit, aber auch durch implizite Hindernisse oder erschwerte Bedingungen geschehen.

Besonders relevant wird dies, wenn eine (digitale) Infrastruktur notwendig für die Teilhabe am (digitalen) Leben oder in der Gesellschaft ist. Nicht nur die unmittelbare Leistungserbringung (oder -versagung) spielt hier eine Rolle, sondern auch die Möglichkeit der Überwachung der Nutzenden in ihrem Verhalten. Als Grundregel kristallisiert sich heraus: Je weniger sich Nutzende der Infrastruktur entziehen können, desto mehr Daten können gesammelt und desto mehr Einfluss kann auf die Nutzenden ausgeübt werden.

Weil Infrastrukturen so grundlegend und systematisch bedeutsam sind, ist ihre Gestaltung und Ausprägung für demokratische und freiheitliche Gesellschaften von großer Bedeutung. Gerade aber diese Gestaltung ist wegen des grundlegenden Charakters sehr komplex: Sie können gestaltet und verändert werden; ein Re-Design von im Einsatz befindlichen Infrastrukturen ist jedoch aufwendig. Die Gestaltung von Infrastrukturen folgt ebenso wie ein etwaiges Re-Design erfahrungsgemäß nicht grundrechtlichen Erwägungen, sondern wird als von technischen Anforderungen geprägt konstruiert oder vor allem ökonomisch getrieben.[2]

Sicherheits- oder Datenschutzaspekte sind somit regelmäßig nachrangig bei der Gestaltung. Das zeigt sich beispielsweise in der Rückschau auf die Entwicklung des World Wide Web (WWW) in Bezug auf zahlreiche Sicherheitsprobleme: Berners-Lee als einer der wichtigsten Begründer des WWW verteidigte die Entscheidung, nicht gleich von Beginn mehr Sicherheit eingebaut zu haben, weil dies dem Ziel, eine für Entwickler:innen leicht bedienbare Plattform zu schaffen („eine Plattform zu schaffen, die Entwickler:innen vertraut ist und einfach zu nutzen"), entgegengestanden hätte (Leyden 2014, eig. Übersetzung). Demnach wurde in Kauf genommen, dass wichtige Eigenschaften und Funktionen wie Sicherheitsfeatures fehlten und so später ergänzt werden mussten, beispielsweise die Transportverschlüsselung in der Kommunikation zwischen Webbrowser und Webserver. Ein späteres Aufsatteln oder Nachrüsten von Eigenschaften oder Funktionen ist jedoch nicht immer einfach und in einigen Fällen schwierig, teuer oder sogar unmöglich.

2 So wurden Vorschläge zur vertrauenswürdigen Mobilkommunikation zwar in der wissenschaftlichen Diskussion aufgenommen, aber hatten keinen wirklichen Einfluss auf die Gestaltung der Mobilnetze (Federrath 1998).

Aktuell werden im KI-Bereich Infrastrukturen ausgebaut. KI basiert auf Cloud-Diensten, wird aber zunehmend selbst eine Infrastruktur für die Anwendungen unterschiedlicher Betreiber:innen. Diese Perspektive ist noch nicht ausreichend untersucht; dabei wäre es gerade zum jetzigen Zeitpunkt noch möglich und nach unserer Überzeugung auch erforderlich, bei KI-Infrastrukturen gestaltend einzugreifen.[3]

In der KI-Debatte wird häufig auf die Effizienz von KI oder durch diese zu erreichende Effizienzsteigerungen verwiesen. Dabei bleibt außer Acht, dass Effizienz kein Ziel an sich ist, und offen, was genau effizienter gestaltet wird und zu welchem Zweck. In den USA lässt sich aktuell verfolgen, wie unter dem Deckmantel von Effizienzsteigerungen demokratische und rechtsstaatliche Strukturen abgebaut werden. Demokratie und Rechtsstaatlichkeit sind jedoch nicht effizient. Sie sollen es auch nicht sein, sondern sie verteilen und kontrollieren Macht bewusst. Aushandlungen, Widerspruchsmöglichkeiten, Kontrolle und transparente demokratische Verfahren sind gerade nicht auf Effizienz ausgelegt, sondern wollen erreichen, dass nicht eine Gewalt oder eine Stelle unwidersprochen und ungeprüft ihre Ziele ohne Rücksicht auf andere Interessen und Normen durchsetzen kann.

Die Trump-Regierung setzt dabei auf den Abbau von Gewaltenteilung, Bürokratie, Verantwortlichkeit und Maßnahmen gegen strukturelle Diskriminierung (vgl. Teirstein 2025, Vought 2023). KI funktioniert als magische Effizienzmaschine, die zu besseren Ergebnissen gelangen und gleichzeitig Personal und Finanzmittel einsparen soll, wobei die gravierenden Umweltauswirkungen und durch sie verursachten wirtschaftlichen und sozialen Kosten ignoriert werden. Tatsächlich steht zu befürchten, dass Einsparungen und der Ersatz von öffentlichen Beschäftigten eher dazu führen, dass öffentliche Dienstleistungen aufgrund fehlenden Fachpersonals nicht mehr für darauf angewiesene Personen verfügbar sind (Hadgu/Gebru 2025).

Vor diesem Hintergrund stellt sich die Frage, wie (rechtliche und digitale) Infrastrukturen so gestaltet werden können, dass sie demokratische und freiheitliche Gesellschaften unterstützen und solchen Angriffen möglichst widerstehen können.

3 Die KI-Verordnung (KI-VO) enthält zahlreiche Regelungen für und Gestaltungsanforderungen an KI-Systeme. Damit greift die europäische Gesetzgebung gestaltend in den KI-Markt ein. Die KI-VO nimmt jedoch primär KI in Form von einzelnen Produkten in den Blick und adressiert die infrastrukturelle Perspektive allenfalls indirekt, beispielsweise in Bezug auf Risikobewertungen und Folgenabschätzungen.

Digitale Infrastrukturen formen die Bedingungen für das Leben in der digitalen Welt aus. Sie sind nicht naturgegeben, sondern werden von Akteur:innen aus Staat und Wirtschaft[4] entwickelt, aufgebaut und betrieben. Die Gestaltung ist daher auch keineswegs zufällig: Sie folgt überwiegend vorgegebenen, bewussten und unbewussten Design-Entscheidungen. Selbst wenn im Entwicklungsprozess nicht jede Design-Anforderung absichtsvoll unter Einbeziehen sämtlicher vorhersehbarer Folgen formuliert wird, werden von Entwicklungsteams ständig Entscheidungen zur Gestaltung getroffen. In diesem Sinne wird beispielsweise auch entschieden, ob und welche Voreinstellungen implementiert werden, ob etwas (und wenn ja, in welchem Rahmen) durch die Anwendenden oder die Endnutzenden konfigurierbar ist usw. Der Verzicht auf eine Implementierung einer Funktion oder einer Eigenschaft ist ebenfalls eine Gestaltungsentscheidung. Im Ergebnis bedeutet dies: Es gibt kein Nicht-Design.

Gleichzeitig sind Infrastrukturen im Alltag unsichtbar (s. auch Star 1999); erst durch eine Fehlfunktion, einen Glitch, werden sie sichtbar. Heutige digitale Infrastrukturen sind in den meisten Fällen funktionsfähig, jedoch, wie oben aufgezeigt, dysfunktional (s. auch Berlant 2016): Sie ermöglichen nämlich nicht eine gleichberechtigte Teilhabe aller Menschen, sondern sind verbunden mit Machterhalt und -erweiterung von Akteur:innen in Wirtschaft und Politik. Um die Infrastrukturen und ihre bereits in diesem Abschnitt benannten Dysfunktionalitäten sichtbar zu machen und sie zu analysieren, zeigen wir im folgenden Abschnitt bestehende Ansätze auf, die genau daran ansetzen.

3. Erste Analyseansätze

Für eine Untersuchung digitaler Infrastrukturen kann auf bestehende Ansätze der Infrastrukturstudien zurückgegriffen werden. Diese sind in Deutschland bisher noch nicht breit rezipiert worden, bieten aber zahlreiche Ansatzpunkte.

In den Infrastrukturstudien (z. B. Star 1999; Edwards u. a. 2009; Easterling 2014; Berlant 2016) wird mit den Perspektiven verschiedener Disziplinen die strukturelle Bedeutung von technischen Infrastrukturen untersucht.

4 Es können sich auch Projekte von einzelnen Personen, die keine kommerziellen Interessen haben, zu Infrastrukturen entwickeln. Üblicherweise lässt sich der zuverlässige Betrieb von Infrastrukturen jedoch nicht von Einzelpersonen gewährleisten.

Nach Berlant formt Infrastruktur die Gesellschaft; Easterling argumentiert, dass „einige der radikalsten Veränderungen in der globalisierten Welt nicht in der Sprache des Rechts oder Diplomatie geschrieben werden, sondern in […] infrastrukturellen Technologien" (2014, 15). Infrastrukturen sind in besonderem Maße handlungsnormierend, da sie durch Technologien und Praktiken, also ihre sozio-technische infrastrukturelle Form, soziale Handlungen, aber auch Wissen und Ressourcen steuern.

Oft werden wir uns Infrastrukturen erst dann bewusst, wenn sie nicht funktionieren (Star 1999). Aber wenn sie funktionieren, enthalten sie eine „systemische Logik und Logistik […]. Sie prägen die Art und Weise, wie wir leben und wie Gesellschaft organisiert wird" (van Dijck u. a. 2018, 9, eig. Übersetzung).

Science and Technology Studies erforschen das ko-konstitutive Verhältnis von Technik, im Speziellen auch Infrastrukturen, und Mensch/Gesellschaft: wie sie miteinander existieren und sich gegenseitig bedingen (z. B. Jasanoff 2004). Sie bauen auf Disziplinen wie der Techniksoziologie auf und ergänzen, z. B. durch Konzepte wie Latours *Akteur-Netzwerk-Theorie*, dass Technologien selbst als soziale Phänomene verstanden werden können (vgl. z. B. Bijker u. a. 1987; Felt u. a. 2017). Ansätze wie *Responsible Research and Innovation,* anwendungsbezogene Technikethik und *Constructive Technology Assessment* erforschen nicht nur, wie diese Zusammenwirkungen zu verstehen sind, sondern wie eine bessere und werteorientierte Gestaltung und Entwicklung von neuen Technologien aussehen kann (vgl. z. B. Rip u. a. 1995).

Die Fragen einer bewussten Gestaltung umfassender und ubiquitärer Infrastrukturen und vor allem KI-Infrastrukturen auf Systemebene sind bislang noch nicht beantwortet. Erste Ansätze finden sich zum Beispiel bei Musiani (2022), die die Prozesse der Einbettung von digitaler Souveränität in Infrastrukturen – *infrastructuring sovereignty* – untersucht. Infrastrukturen werden hierbei als prozessual und relational verstanden und nicht als fixe Artefakte, die außerhalb des Sozialen Handelns liegen. Dieses Verständnis von Infrastrukturen als Praktiken und Prozesse ermöglicht nicht nur, das Entstehen und Wirken von Infrastrukturen zu analysieren, zu verstehen und zu bewerten, sondern auch einzelne Ansatzpunkte für Einwirkungen und aktive Einbettung von Werten in die Prozesse, Praktiken und Technologien zu identifizieren und anzugehen.

Auch das Recht selbst kann auf verschiedene Arten als Infrastruktur betrachtet werden: Nach Byrne u. a. (2024, 1237f.) ko-konstituieren Rechtsnormen, -praxis und Institutionen *Legal Infrastructures* (rechtliche Infra-

strukturen). Diese *Legal Infrastructures* unterscheiden sich von anderen Arten von Infrastrukturen durch ihre normativen Eigenschaften: Recht konstruiert gesellschaftliche Infrastrukturen und hat dadurch eine inhärente Infrastrukturdynamik. Dabei kommt Recht auch eine soziale Ordnungsfunktion zu. Die *Legal Infrastructures* wirken konkret auf die Verteilung von *Affordances*, wie Macht, ein, da sie in anderen, materiellen, technischen oder sozialen Infrastrukturen eingebettet sind (Byrne u. a. 2024, 1241 u. 1243 f.).

In den bestehenden *Legal Infrastructures* wird also festgelegt, wie Macht innerhalb von Gesellschaften verteilt wird, welche Gruppen sie in welchem Maße ausüben und welche Gruppen ausgeschlossen werden. Dies ergänzt die vorwiegend individualistische Betrachtungsweise von Diskriminierungsdynamiken innerhalb des Rechts. Bei dieser von Individuen oder Gruppen ausgehenden Betrachtung wird oft von konkreten Fällen ausgegangen, in denen eine Diskriminierung bereits erfolgt ist. Aus den daraus ableitbaren strukturellen Gesellschaftsdynamiken, die bereits ausführlich untersucht wurden (vgl. Bieker/Hansen 2023b m. w. N.), lassen sich Schlussfolgerungen und Ansatzpunkte für die infrastrukturelle Ebene gewinnen.

Weiterhin können *Legal Infrastructures* als Praktiken betrachtet werden. Sie existieren nicht ohne soziale Auseinandersetzung mit ihnen. Recht konstituiert sich fortlaufend, Rechtsnormen müssen durch eine beständige Praxis aufrechterhalten werden, die ihr Legalität (Brunné/Tohope 2010) verleiht. Ein Ansatzpunkt hierzu ist auch die Frage, wie sich in Praktiken normative Strukturen und Anordnungen über Grenzen und Gemeinschaften hinweg (re-)produzieren. Aus infrastruktureller Sicht kommt dabei der Untersuchung, wie *Legal Infrastructures* das Teilen, Hinterfragen und Ausführen von Rechtsnormen ermöglichen, besondere Bedeutung zu, die sich nicht auf soziale Interaktionen beschränkt, sondern auch die verbundenen Ebenen rechtlich-technischer Integration betrachtet (Byrne u. a. 2024, 1242).

Für digitale Infrastrukturen bietet sich eine Betrachtung der Integration von Recht in Technik an. Problematisch ist hier in Hinblick auf By-Design-Ansätze, dass sie in der Praxis nicht (ausreichend) umgesetzt werden – trotz bestehender Rechtspflichten. Obwohl etwa Art. 25 DSGVO technikneutral formuliert ist, zusätzlich konkrete Hinweise auf Maßnahmen bietet und auf die unterschiedlichen Risiken individueller Datenverarbeitungen skaliert, ist die Vorschrift innerhalb der Wissenschaft und Praxis umstritten (vgl. Dewitte 2024). Ein Problem der Umsetzung liegt darin, dass Hersteller

von der DSGVO nicht adressiert werden und daher kein gesteigertes Eigeninteresse am Anbieten datenschutzfreundlicher Produkte haben. Während die datenschutzrechtlich Verantwortlichen im Prinzip die Möglichkeit haben, bei der Beschaffung von speziellen Produkten auf die Berücksichtigung des Art. 25 DSGVO zu drängen, unterbleibt zumeist ein Einfordern der Umsetzung des Datenschutzrechts, weil dies gar nicht innerhalb des eigenen Verantwortungsbereichs empfunden wird oder ohnehin unrealistisch erscheint.

Ein weiterer Ansatzpunkt für die rechtliche Analyse ist die Verknüpfung der Bereitstellung von physischer Infrastruktur mit Jurisdiktion. Dabei wird von verschiedenen Akteuren etwa der Bau von Straßen als Anlass zur Normsetzung genommen. Dies wurde in Hinblick auf (neo-)koloniale Kontexte untersucht (Cowan 2023, Rodiles 2022, Kwet 2022). Im Verhältnis zwischen den USA und der EU und anderen Regionen im Bereich von Cloud-Infrastrukturen, erfolgt ebenfalls eine Verknüpfung von Infrastrukturbereitstellung mit Jurisdiktion: Die USA haben mit dem US CLOUD Act umfassende Regelungen erlassen, die ihnen Zugriff auf die bei US-amerikanischen Unternehmen gespeicherte Daten einräumen, auch wenn dies durch den Zugriff auf die physische Infrastruktur regionaler Niederlassungen außerhalb der USA erfolgt.

4. Ansatzpunkte für demokratische und freiheitliche Infrastrukturen

Die europäische Gesetzgebung der letzten Jahre für den Digitalbereich ist durch einen risikobasierten Ansatz gekennzeichnet: Risiken sollen identifiziert, bewertet und ausreichend eingedämmt werden. Zum Eindämmen der Risiken wird der By-Design-Ansatz verfolgt. Dies zeigt sich beispielsweise in der DSGVO, die mit Art. 25 auf Datenschutz by Design und by Default setzt, aber auch in den jüngeren gesetzgeberischen Entwicklungen im Bereich der Cybersicherheit wie der NIS-2-Richtlinie (Richtlinie (EU) 2022/2555) und dem Cyber Resilience Act (CRA, Cyberresilienz-Verordnung, Verordnung (EU) 2024/2847), der das Paradigma „Security by Design" verfolgt. Doch wie geht „Freiheit by Design"? Oder – sinnvoll weitergedacht – „Grundrechte by Design"?

Um eine grundrechtskonforme Gestaltung von Infrastrukturen zu erreichen, bietet sich eine Kombination verschiedener Ansatzpunkte an, die sich an unterschiedliche Akteur:innen und die Ausgestaltung der Technologien selbst richten. Einige der Ansatzpunkte gehen von Anwender:innen

aus, die Alternativen zu Big-Tech-Infrastrukturen suchen oder ergänzende Maßnahmen treffen müssen, um das von den diesen Infrastrukturen ausgehende Risiko ausreichend zu beherrschen. Entscheidend ist, inwieweit technische Standards so gestaltet werden, dass sie (grund-)rechtliche Anforderungen umsetzen oder unterstützen.

Zu diskutieren sind zudem (weitere) Regulierungen des grundlegenden Infrastrukturbereichs auf gesetzlicher Ebene. Derartige Regulierungen müssen jedoch auch durchgesetzt werden; hier muss besser gewährleistet sein, dass sich Infrastrukturanbieter:innen an die rechtlichen Vorgaben halten. Einige interessante Ansatzpunkte werden im Folgenden erläutert.

4.1 Selbstbestimmung und Reduzierung von Abhängigkeiten

Der Freiheitsbegriff ist unmittelbar verbunden mit Selbstbestimmung; eine Fremdbestimmung soll vermieden oder zumindest eingeschränkt sein. Dieses Konzept ist verwandt mit der digitalen Souveränität. Unter diesem Schlagwort sowie überlappenden Konzepten wie der technologischen, operationalen und Daten-Souveränität werden aktuell vor allem in Europa Maßnahmen zur Reduktion der Abhängigkeit von Big Tech diskutiert (z. B. Glasze u. a. 2022, Baur 2024, Baur 2025). Eine häufig angewandte Definition versteht unter digitaler Souveränität „die Summe aller Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rollen in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können“ (Kompetenzzentrum Öffentliche IT 2017). Da der Begriff der digitalen Souveränität ein sehr schillernder ist, mit unterschiedlichen Definitionen und Anwendungen und in dem sich auch sehr widerstreitende Interessen wiederfinden, sind einige konzeptionelle Ergänzungen sinnvoll.

Der Begriff der Souveränität, an dem sich die digitale Souveränität bedient, stammt aus der politischen Theorie und kennt vor allem zwei Dimensionen: eine interne und eine externe. Die externe bezeichnet die Ordnung von Autoritäten und damit Abwehr ungerechtfertigter Einflussnahme meist mithilfe von staatlichen Territorien, während die interne die legitime Autorität innerhalb eines Staates definiert. Souveränität wurde erst durch Philosophen wie Rousseau auf demokratische Systeme und damit demokratisch legitimierte Machtausübung und Rechtstaatlichkeit erweitert.

Mit dem Argument der digitalen Souveränität können deswegen auch einer Abschottung und einer autoritären Organisation und Überwachung von Gesellschaften Vorschub geleistet werden, wie es zum Beispiel in

Russland unter dem Begriff des „souveränen Internets“ geschieht. Es ist deswegen wichtig, bei Initiativen zur Steigerung der digitalen Souveränität darauf zu achten, dass nicht nur staatliche Institutionen als Referenzpunkt genannt werden, sondern eben vor allem Gesellschaften und Individuen. Diese gilt es in ihrer Selbstbestimmung zu fördern und dabei nicht ihre Überwachung bzw. autoritäre Kontrollmechanismen und Abschottung voranzutreiben.

Digitale Souveränität im Sinne der Gesellschaft und der Individuen bedeutet, die Risiken ausreichend einzudämmen, die mit der Verarbeitung der Daten oder anderen Digitalisierungskomponenten verbunden sind. Dies betrifft insbesondere die Abhängigkeiten von der korrekten (und gewünschten) Funktionsweise von Hard- und Software und damit auch von Hersteller:innen, Zulieferer:innen oder Betreiber:innen. Es gilt, Klumpenrisiken zu vermeiden, beispielsweise Risikokonzentration aufgrund von zentralen singulären und nicht oder kaum auswechselbaren Komponenten. Zu den strategischen Zielen, die die öffentliche Verwaltung in Bezug auf digitale Souveränität verfolgt, gehören eine Wechselmöglichkeit, eine Gestaltungsfähigkeit und Einflussmöglichkeiten auf Anbieter:innen (IT-Planungsrat 2021).

4.2 Offene Standards und Transparenz

Offene Schnittstellen, Formate und Protokolle[5] unterstützen die Möglichkeit des Auswechselns von Komponenten auf der technischen Ebene. Dagegen erschweren proprietäre und nicht offengelegte Gestaltungen der Technik die für digitale Souveränität wünschenswerte oder gar erforderliche Interoperabilität und Interkonnektivität. Insoweit kommt auch den Open-Source-Entwicklungen eine große Bedeutung für digitale Souveränität zu. Dass Open Source das Potenzial für mehr Kontrolle, Einflussnahme und Beherrschbarkeit hat, ist keine neue Erkenntnis (Köhntopp u. a. 2000).

Da die Hauptverantwortung für Infrastrukturen im Allgemeinen und für digitale Infrastrukturen im Besonderen beim Staat liegt (vgl. Roßnagel 1997[6], Berlit 2011), kommt den Initiativen des Staats für digitale Souveräni-

5 Technische Schnittstellen, Formate und Protokolle sind mindestens ebenso relevant wie der eigentliche Code (Lessig 2001).

6 Roßnagel ging bereits 1997 davon aus, dass der Staat und das Recht nicht mehr in der Lage seien, im „immateriellen Sozialraum der Netze Gemeinwohlbelange durchzu-

tät der Verwaltung eine besondere Bedeutung zu. So hat beispielsweise das Land Schleswig-Holstein (2024) eine Open-Source-Strategie ausgearbeitet – das Land stellt allmählich seine Verarbeitung auf Open-Source-Komponenten um. Auf Bundesebene wirkt das Zentrum für Digitale Souveränität darauf hin, dass für die Verwaltung in Bund und Ländern Open-Source-Lösungen bereitgestellt werden (ZenDiS 2025). Dies geschieht unter anderem über die Plattform openCode.[7] Auch der IT-Planungsrat (2025) erkennt die Notwendigkeit von offenen Dokumentenstandards und offenen Kollaborationslösungen in der öffentlichen Verwaltung und fordert die Umsetzung in Deutschland bis 2027.

Das Konzept „Open Source" garantiert aus sich heraus noch nicht, dass es sich auch tatsächlich um einen korrekten Code ohne Schwachstellen handelt (Köhntopp u. a. 2000) – und schon gar nicht, dass der Code Werte-basiert ist. So hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden (2023) in ihrem Positionspapier zu Souveränen Clouds Open Source als Soll- und nicht als Muss-Kriterium aufgeführt; aus Sicht der Datenschutzkonferenz ist Open Source hilfreich für digitale Souveränität, aber keine notwendige Voraussetzung. Hinzu kommt, dass einerseits im Einsatz von Open-Source-Tools, andererseits im Entwicklungsprozess von Open Source heutzutage ebenfalls Abhängigkeiten bestehen, die Risiken mit sich bringen (instruktiv Seeger 2024). Besonders wichtig ist daher, in Anspruch genommene Produkte, Komponenten und Dienste durch (rechtskonforme) Alternativen ohne unverhältnismäßigen Aufwand auswechseln zu können.[8]

Generell spielt für die Produkt- und Systementwicklung und auch für die Wechselfähigkeit die technische Standardisierung eine wesentliche Rolle. Das Befolgen von technischen Standards ist in einigen Sektoren eine Pflicht, in anderen Bereichen zumindest angeraten. Für einen rechtssicheren Einsatz von Produkten und Systemen ist es hilfreich, wenn grund-

setzen und die Bürger zu schützen". Aufgrund der Schutzmöglichkeiten auf der Basis von Informationstechnik wandele sich die Erfüllungsverantwortung des Staates zu einer Strukturverantwortung. Der Staat werde seiner Schutzpflicht gerecht, wenn er Strukturen schaffe, „die seine Bürger befähigen, ihre Interessen in der Welt der Netze selbstbestimmt zu schützen". Es geht dabei weniger um einen Selbstdatenschutz, der die Last weitgehend auf die Schultern der Bürger:innen legt, sondern um die staatliche Rolle zur Befähigung der Betroffenen in Ergänzung zu einem Systemdatenschutz – auch und gerade im Sinne der digitalen Souveränität.

7 https://opencode.de/de.

8 Europäische Alternativen für digitale Produkte werden beispielsweise unter diesem Link gesammelt: https://european-alternatives.eu/ (Graf 2025).

rechtsrelevante Kriterien in technischen Standards berücksichtigt werden. Der Prozess der Erarbeitung technischer Standards ist üblicherweise von unternehmensübergreifenden ökonomischen Interessen getrieben. Jedoch müssen beispielsweise die von der Europäischen Kommission bei den Standardisierungsgremien CEN und CENELEC in Auftrag gegebenen Standards zur KI-VO auch die dort enthaltenen Anforderungen, die sich auf Grundrechte oder Energieverbrauch beziehen, berücksichtigen (Europäische Kommission 2023b).

Die Teilnehmenden in den Standardisierungsgremien stammen großenteils aus der Industrie. Auch wenn eine Teilnahme von Vertreter:innen aus der Zivilgesellschaft nicht ausgeschlossen ist, geschieht dies nur in geringem Umfang, schon weil der – üblicherweise unbezahlte – Zeitaufwand groß ist und internationale Reisen finanziert werden müssen. Aus denselben Gründen ist zurzeit auch die Beteiligung von Datenschutzaufsichtsbehörden an Standardisierungsinitiativen auf Einzelfälle begrenzt.

Weil technische Standards so einflussreich sein können, müssen sie und der Prozess der Erarbeitung gegen eine Manipulation geschützt werden. Die US-amerikanische Standardisierungsorganisation NIST (National Institute of Standards and Technology) hatte sich aufgrund einer zunächst unerkannten Einflussnahme des Geheimdiensts NSA (National Security Agency) im Bereich der Verschlüsselung gezwungen gesehen, eine bereits veröffentlichte Empfehlung für einen Krypto-Algorithmus zurückzuziehen (NIST 2014). Es ist generell wahrscheinlich, dass Geheimdienste versuchen, in vielen Standardisierungsgremien Einfluss zu nehmen (Rogers/Eden 2017). Abgesehen von möglichen Unterwanderungen der Standardisierungsprozesse sei betont, dass trotz des potenziell hohen Wirkungsgrads auf unsere Gesellschaft technische Normung nicht auf einer unmittelbaren demokratischen Legitimierung basiert – anders als bei parlamentarischen Entscheidungen über rechtliche Normen. Als Ansatzpunkte zur Verbesserung sollte diskutiert werden, wie gesellschaftliche Interessen, rechtliche Anforderungen und generell Risiken für die Grundrechte und Grundfreiheiten zuverlässig in den Standardisierungsprozessen behandelt und entsprechende Design-Entscheidungen dokumentiert werden können. Dass mehr Transparenz notwendig ist, zeigt sich auch daran, dass selbst die Ergebnisse der Standardisierung – also die technischen Standards, die umgesetzt werden sollen oder müssen – nicht generell frei und kostenlos zur Verfügung gestellt werden. Der EuGH hat mittlerweile in der Malamud-Entscheidung festgestellt, dass überwiegendes öffentliches Interesse

an der Verbreitung von harmonisierten europäischen Normen bestehen kann (EuGH-Urteil vom 05.03.2024 – C-588/21 P).[9]

Technische Standards für einzelne Komponenten in der Verarbeitung können in der Regel keinen rechtssicheren Einsatz garantieren; häufig kommt es auf den Einsatzkontext und die Einsatzumgebung an. Im Endeffekt muss der Verantwortliche sich selbst davon überzeugen, dass die rechtlichen Anforderungen eingehalten werden. Ein Faktor könnte dabei die Zertifizierung nach Art. 42f. DSGVO darstellen, auch wenn sie in der Praxis noch fast gar nicht vorkommt. Von den Datenschutzaufsichtsbehörden wird häufig eine Sofort-Bewertung der Datenschutzkonformität eines Produkts erwartet – am besten für alle möglichen Versionen und Konfigurationen. Dies ist unrealistisch, und Produktprüfungen gehören auch nicht zu den unmittelbaren Aufgaben der Datenschutzaufsicht, wofür sie zurzeit auch nicht ausgestattet sind. Diese Behörden unterstützen durchaus, in dem sie aufzeigen, welche Prüfpunkte Verantwortliche anlegen müssen, oder abstrakte Lösungen als Positivbeispiele skizzieren. Es ist aber so noch nicht gewährleistet, dass diejenigen Verantwortlichen, die sich an Recht und Gesetz halten wollen, ausreichende Hilfen erhalten. Nach Möglichkeit sollten die Verantwortlichen eine Situation vorfinden, in der es leicht ist, die rechtlichen Anforderungen zu erfüllen. Das gilt besonders für die Infrastrukturen, derer sie sich bedienen.

4.3 Moving Targets und Verantwortungsdiffusion angehen

Bisher schaffen es Big-Tech-Unternehmen, sich der Verantwortlichkeit durch Zeitverzögerung zu entziehen. Es werden Dienste angeboten, bevor Risiken identifiziert oder gar adressiert wurden, oft mit dem Hinweis bestehende Regelungen seien auf diese neuartige Technologie nicht anwendbar. Wenn sich Risiken in Schäden für betroffene Personen niederschlagen, werden diese zunächst abgestritten, bei wachsendem Druck kleine Änderungen umgesetzt, die die meist systemischen Ursachen nicht angehen. In etwaigen behördlichen oder gerichtlichen Verfahren werden Informationen nur langsam herausgegeben und im Anschluss auf ein ungünstiges Urteil nur minimale Änderungen vorgenommen oder argumentiert, dass diese be-

9 Die Standardisierungsorganisationen IEC und ISO wehren sich gegen den Informationszugang und haben beim EuGH Klage gegen die Europäische Kommission eingereicht (anhängige Rechtssache T-631/24, veröffentlicht am 17.02.2025, https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:C_202500919).

reits erfolgt seien und das Urteil damit nicht mehr auf die aktuelle Situation anwendbar sei (Bieker/Hansen 2023a).

Unter den aktuellen wirtschaftlichen Bedingungen wird diese Verzögerungstaktik belohnt. Auch hier funktioniert das Vorgehen nach der Maxime „Move fast and break things": In der gewonnenen Zeit können die Anbieter:innen bereits Gewinne erwirtschaften und sich eine starke Position auf dem Markt verschaffen. Sie haben damit einen großen ökonomischen Vorteil, insbesondere gegenüber gründlicheren und – was leider keine Selbstverständlichkeit ist – rechtstreu orientierten Anbieter:innen, die sich an bestehende Regelungen anpassen.

Dies zeigt sich auch im Bereich der KI, in dem es insbesondere Microsoft und Amazon als großen Cloud-Dienstleistern gelungen ist, mit dieser für große KI-Modelle notwendigen Infrastruktur infrastrukturelle Macht aufzubauen und maßgebliche Anbieter zu werden, die zum einen die technische Recheninfrastruktur bereitstellen, aber auch von der Datenerhebung, der Modellerstellung und dem Training sowie dem Endkund:innenkontakt wichtige Aspekte der KI-Dienste in sich vereinen (Luitse 2024). Selbst große Betreiber von eigenen KI-Anwendungen sind auf ihre Recheninfrastruktur angewiesen.

Aus informationstechnischer Perspektive benennen Balayn und Gürses (2024) agile Entwicklungsumgebungen als Teil dieses Problems: Aktuelle KI-Angebote beruhten auf einer Vielzahl von Diensten unterschiedlicher Anbieter:innen, die Betreiber:innen zusammenklicken, sodass kurzfristig Änderungen vorgenommen werden können, aber eben auch ein hochkomplexes Gefüge unterschiedlicher Akteur:innen entsteht. Dabei hätten die Betreiber:innen meist keine große Machtposition gegenüber ihren Diensteanbieter:innen, sodass sie auch nur begrenzten Einfluss auf die Gestaltung der Prozesse und ihnen zugrundeliegenden Infrastrukturen hätten. Sie fordern, dass diese Entwicklungsumgebungen reguliert werden müssen, anstatt sich auf einzelne Technologien zu beschränken, wie bei der KI-VO.

Zwar gibt es mit der DSGVO bereits eine technikneutrale Regulierung, die sich allgemein auf Datenverarbeitungen bezieht. Baylan und Gürses stellen jedoch fest, dass diese bisher nicht erfolgreich darin war, den genannten Verzögerungstaktiken und dieser Verantwortungsdiffusion effektiv entgegenzutreten.

Auf der zeitlichen Ebene wäre es denkbar, den gerichtlichen Rechtsweg, wie es bereits im Wettbewerbsrecht nach § 73 GWG geregelt ist, in bestimmten Fällen auf den BGH zu begrenzen, damit europarechtliche Fragen nicht erst, wie üblich, nach mehreren Instanzenzügen durch den EuGH

vorab entschieden werden können und so schneller Rechtssicherheit für alle Beteiligten hergestellt wird. Für die Klärung wichtiger Grundsatzfragen mit weitreichenden und teilweise faktisch irreversiblen Auswirkungen auf die Realität, wie dies bei der Gestaltung von digitalen Infrastrukturen nicht selten ist, wäre ein Fast Track beim EuGH denkbar.

Bezüglich der Verantwortungsdiffusion ist ein großes Problem der DSGVO, dass diese nur Verantwortliche und Auftragsverarbeiter:innen kennt. Hersteller:innen oder Anbieter:innen, die keine eigenen Zwecke mit der Datenverarbeitung verfolgen, sondern nur Dienste oder Infrastrukturen bereitstellen, fallen nicht in den Anwendungsbereich der DSGVO. Dies hat der EU-Gesetzgeber in der KI-VO explizit anders geregelt. Insofern können Verantwortliche etwa durch die Verpflichtung von Anbieter:innen nach Art. 9 KI-VO ein Risikomanagementsystem zu betreiben, voraussichtlich leichter Informationen für ihre eigenen Risikobeurteilungen (etwa nach Art. 27 KI-VO, Art. 35 und 24 DSGVO) erhalten. Allerdings ersetzt dies eigenständige Verpflichtungen der Anbieter:innen nach der DSGVO nicht ausreichend und birgt ebenfalls Gefahren der regulierten Selbstregulierung (Bieker 2025).

4.4 Inzentivierung korrigieren und Infrastrukturen regulieren

Das Digitale-Dienste-Verordnung (Verordnung (EU) 2022/2065) bezieht die infrastrukturelle Perspektive insoweit ein, dass sehr große Online-Plattformen und Suchmaschinen (Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs)) besonderen Pflichten unterworfen werden. Ziel der Digitale-Dienste-Verordnung ist es, illegale oder schädliche Online-Aktivitäten sowie die Verbreitung von Desinformation über die Plattformen und Suchmaschinen zu verhindern. VLOPs und VLSEs sind dadurch charakterisiert, dass sie mehr als 10% der 450 Mio. Verbraucher:innen in Europa erreichen. Nach der Definition betrifft dies eine kleine Anzahl (2023: 19 (Europäische Kommission 2023a), bis zum 1. Quartal 2025 wurde die Liste der VLOPS und VLOSEs auf 25 Angebote erweitert[10]); Anbieter:innen von LLMs gehören bisher nicht dazu.

Es ist noch unklar, ob die Regelungen zur Plattformkontrolle ausreichen und sie sich effektiv durchsetzen lassen. Schließlich basieren bisherige

10 Aktuelle Liste der VLOPs und VLOSEs: https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses (Abruf am 09.05.2025).

Geschäftsmodelle zahlreicher Anbieter:innen darauf, die Aufmerksamkeit der Internet-Nutzenden und vor allem deren Klicks auf sich zu lenken. Belohnt werden gerade nicht die sorgfältige Recherche und die korrekte Darstellung, sondern unseriöses Gebaren mit extremen Darstellungen, die verfälscht oder auch vollständig erfunden sein können. Hier müsste in die Geschäftsmodelle des Ausspielens von Werbung im Internet eingegriffen werden, wenn man wirklich eine Änderung erreichen möchte – z. B. indem nicht schnelle Klicks monetarisiert werden können, sondern etwa Klicks auf korrekte, ausgewogen dargestellte und vor allem qualitätsgesicherte Inhalte, die länger Bestand haben,

Zusätzlich wären Möglichkeiten zur Gewinnabschöpfung denkbar, wenn ein:e Akteur:in nicht nachweisen kann, dass diese Gewinne auf rechtmäßige Art und Weise entstanden sind. Es könnten Fonds eingerichtet werden, die abgeschöpfte Gewinne an Geschädigte weitergäben. Hierzu sind noch keine detaillierten Ausarbeitungen bekannt; wir finden es aber lohnend, dies weiterzuverfolgen.

Monopole und umfassende Marktmachtkonzentrationen sollten kartellrechtlich angegangen und entflochten werden. Hierbei ist es wichtig, nicht nur einzelne Dienstleistungen und Sektoren getrennt zu betrachten, sondern die Netzwerk- und Abhängigkeitseffekte integrierter Infrastrukturen zu berücksichtigen. Problematisch hierbei sind, dass trotz der interessanten und richtigen Ansatzpunkte in der EuroStack-Initiative auch hier Forderungen nach einem Abbau ‚lähmender Regulierung' und nach mehr Konsolidierung in Europa laut werden (Caffarra u.a. 2025, S. 6 f.). Eine sinnvolle Antwort auf die Nachteile fehlender Regulierung und großer Machtkonzentration in anderen Märkten kann jedoch nicht in der Kopie dieses Ansatzes liegen.

Während die Datenschutz-Grundverordnung den Fokus auf die Verarbeitung personenbezogener Daten legt und die Digitale-Dienste-Verordnung primär die Plattformen und Diensteanbieter:innen in den Blick nimmt, können bei Freiheit by Design weitere wesentliche Aspekte eine Rolle spielen. So wird der Klimawandel massive Auswirkungen auf die Freiheit haben, wo auf der Erde noch Lebensbedingungen herrschen, die sich für Menschen eignen. Für die Entwicklung des Klimas sind wiederum der Energieverbrauch und die Energieproduktion von großer Bedeutung. Besonders der Hype um KI führt aktuell und künftig zu einem erheblich gesteigerten Bedarf an Energie (IEA 2025). Dies führt dazu, dass Big-Tech-Unternehmen für ihre KI-Angebote eigene Kraftwerke bauen und betreiben.

Die Entscheidung darüber, welche Risiken und Nebenwirkungen von der Gesellschaft in Kauf genommen werden, was die Energieversorgung angeht, treffen diese Unternehmen großenteils in Eigenregie. Bisher ist jedenfalls nicht absehbar, dass der Betrieb von Atomkraftwerken damit verbunden ist, sowohl die Betriebsrisiken ausreichend abzusichern als auch die Langzeitlagerung und -versorgung für die Brennstäbe zu garantieren.

4.5 Öffentliche Infrastrukturen fördern und vor Vereinnahmung schützen

Forderungen nach öffentlichen Infrastrukturen treffen häufig auf die Erwiderung, dass diese durch Diskriminierung, Zensur und Überwachung leichter politisiert und auch missbraucht werden können. Gerade die Entwicklungen in den USA seit Beginn der zweiten Amtszeit von Präsident Donald Trump (Teirstein 2025[11]) zeigen jedoch, dass auch private Anbieter nicht per se Schutz vor Politisierung und Vereinnahmung garantieren.

Wir beobachten außerdem eine falsche Dichotomie zwischen komplett privaten Infrastrukturen auf der einen Seite und solchen, die direkt der Regierung und Exekutive eines Landes oder politischen Ordnung unterstellt sind. Gerade Beispiele des öffentlichen Rundfunks und anderer öffentlicher Institutionen zeigen, dass Ordnungsprinzipien denkbar sind, die sich dieser Dichotomie entziehen. Deswegen muss der Zivilgesellschaft eine stärkere Rolle zukommen.

Darüber hinaus sind die oben genannten Prinzipien der Werte-orientierten Infrastrukturgestaltung und der By-Design-Ansätze wichtige Anker innerhalb der vernetzten Technologien, die einen Missbrauch und Umwidmung erschweren und damit besonders marginalisierte Gruppen schützt.

5. Ausblick

Angesichts der aktuellen geopolitischen Entwicklungen und des rasanten technischen Fortschritts verdienen die Forschung zu digitalen Infrastrukturen und die Ausarbeitung von Lösungsstrategien gegen Machtkonzentration in und durch Infrastrukturen sowie Machtmissbrauch durch Staaten oder Wirtschaftsunternehmen deutlich mehr Aufmerksamkeit. Für den

11 Mit Verweisen auf zwei Websites, die als „Project 2025 Tracker" die Schritte der Verfassungskrise der USA und ihre Transformation dokumentieren.

Bereich der Cybersicherheit ist das Problembewusstsein zwar in jüngerer Zeit gestiegen, und der europäische Gesetzgeber hat in Rechtsnormen wie der NIS-2-Richtlinie und der Cyberresilienz-Verordnung Anforderungen für mehr Sicherheit und Risikobeherrschung über die gesamte Lieferkette für Hardware und Software formuliert. Weitere Digitalrechtsakte der EU, von der DSGVO aus dem Jahr 2016 bis zur KI-VO aus dem Jahr 2024 nehmen das Risiko für die Betroffenen und ihre Rechte und Freiheiten in den Blick. Während die DSGVO diesen Risikobegriff vor allem in Bezug auf die Pflichten der Verantwortlichen (und der Auftragsverarbeiter:innen) anwendet, hat das Konzept seitdem eine Ausweitung in DDVO und KI-VO erfahren. Ob diese Skalierung entlang von weitgefassten Risikobegriffen eine Verbesserung für den Grundrechteschutz darstellt, bleibt abzuwarten (vgl. Bieker 2025).

Die Durchschlagskraft der DSGVO im Sinne der europäischen Grundrechte war bisher jedoch, gelinde gesagt, beschränkt. Insbesondere gegenüber Anbieter:innen von Produkten und Dienstleistungen im Bereich der digitalen Infrastrukturen fehlt es an der nötigen Umgestaltung. Der Aufbau von (europäischen) Alternativen zu etablierten Infrastrukturen verläuft bisher zögerlich. Angebote, die von Anfang an konform zu den rechtlichen Anforderungen – im Sinne von „Grundrechte by Design" – gestaltet wurden, hatten in der Vergangenheit nicht unbedingt einen Marktvorteil.

Der aktuelle Prozess einer geopolitischen Disruption rechtfertigt einen Paradigmenwechsel: Es ist jetzt nötiger als je zuvor, dass die bisherigen digitalen Infrastrukturen samt den damit verbundenen Abhängigkeiten auf den Prüfstand kommen, und bei der Entwicklung neuer Infrastrukturen die grundrechtlichen Kriterien berücksichtigt werden. Europa muss sich faire Infrastrukturen leisten wollen. Im Fall von KI kann dies bedeuten, dass dezentralisierte, spezialisierte, aufwendiger trainierte Systeme ausgewählt werden, statt auf große allgemeine Modelle zu setzen, die mit fragwürdigen Methoden entwickelt wurden.

So wie Technologien nie die alleinige Lösung für soziale Probleme sein können, so sind auch Infrastrukturen nie ausreichend zum Schutz vor einer anti-demokratischen Übernahme geeignet. Technische Infrastrukturen werden Demokratien nicht schützen. Werte-orientierte öffentliche Infrastrukturen sind eine notwendige Bedingung für eine stabile, inklusive und freiheitliche Demokratie, aber keine hinreichende für ihre Existenzsicherung. Anti-demokratischen politischen Kräften muss in Gesellschaft und Politik begegnet und entgegengetreten werden, Demokratie dort gelebt und stabilisiert werden.

Infrastruktur-Design darf nicht zufällig passieren. Es bedarf eines systematischen, partizipativen und inklusiven Ansatzes unter Beteiligung aller gesellschaftlich relevanter Gruppen, um Risiken zu erkennen, Lösungen mit ihren Vor- und Nachteilen zu diskutieren und sich auf ein Vorgehen zu verständigen – kurzum: Es bedarf einer verlässlichen Infrastruktur zur fairen Gestaltung von Infrastrukturen.

Danksagung

Dieser Beitrag wurde teilweise gefördert durch das Ministerium für Wirtschaft, Arbeit und Tourismus Baden-Württemberg im Rahmen des Projekts Datenplattform der KI-Allianz BW und vom Bundesministerium für Forschung, Technologie und Raumfahrt im Rahmen des Projekts Neue Datenschutz-Governance – Technik, Regulierung und Transformation (DatenTRAFO)

Literatur

Balayn, Agathe und Gürses, Seda (2024): Misguided: AI regulation needs a shift in focus. *Internet Policy Review*, https://policyreview.info/articles/news/misguided-ai-regulation-needs-shift/1796.

Baur, Andreas (2024): European Dreams of the Cloud: Imagining Innovation and Political Control. *Geopolitics*, 29(3), S. 796–820. https://doi.org/10.1080/14650045.2022.2151902.

Baur, Andreas (2025): European ambitions captured by American clouds: digital sovereignty through Gaia-X?. *Information, Communication & Society*, S. 1–18. https://doi.org/10.1080/1369118X.2025.2516545.

Berlant, Lauren (2016): The commons: Infrastructures for troubling times. *Environment and Planning D: Society and Space,* 34(3), S. 393–419.

Berlit, Uwe (2011): Staatliche Infrastrukturverantwortung für rechtssichere Kommunikation im Netz – rechtliche Rahmenbedingungen und Probleme, *JurPC Web-Dok.* 39/2011, Abs. 1–45.

Bieker, Felix (2025): Risikobewertung im EU-Datenrecht: Effektiver Grundrechteschutz oder Feigenblatt?, *EuDIR (4)*, S. 190–197.

Bieker, Felix und Hansen, Marit (2023a): Daten-Fairness als Daten-Gerechtigkeit by Design. In: Friedewald, Michael u. a. (Hrsg.): *Daten-Fairness in einer globalisierten Welt.* Nomos, S. 29–56.

Bieker, Felix und Hansen, Marit (2023b): Data Protection in 2033: Playing Whac-A-Mole with Injustices? *European Data Protection Law Review (EDPL),* 9(4), S. 399–408. https://doi.org/10.21552/edpl/2023/4/6.

Bijker, Wiebe E.; Hughes, Thomas P. und Pinch, Trevor J. (Hrsg.) (1987): *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology*. Cambridge, MA.: MIT Press.

Brunnée, Jutta und Toope, Stephen J. (2010): Legitimacy and Liability in International: An Interactional Account. Cambridge University Press, https://doi.org/10.1017/CBO9780511781261.

Byrne, William Hamilton; Gammeltoft-Hansen, Thomas und Stappert, Nora (2024): Legal Infrastructures: Towards a Conceptual Framework. *German Law Journal,* 24, S. 1229–1246.

Caffarra, Cristina; Fermigier, Stefane; Hidalgo, Agata; Lechelle, Yann; Parsons, Clark; Styma, Felix und Yen, Andy (2025): 'Deploying the EuroStack: What's Needed Now', 19. Mai 2025. https://eurostack.eu/wp-content/uploads/2025/06/eurostack-white-paper-final-19-05-25-3.pdf.

Cowan, Deborah (2023): Law as Infrastructure of Colonial Space: Sketches from Turtle Island. *AJIL Unbound,* 117, S. 5–10.

DeNardis, Laura und Musiani, Francesca (2016): Governance by Infrastructure In: Musiani, Francesca; Cogburn, Derrick L.; DeNardis; Laura und Levinson, Nanette S. (Hrsg.): *The Turn to Infrastructure in Internet Governance.* Basingstoke: Palgrave Macmillan, S. 3–21.

Dewitte, Pierre (2024): The Many Shades of Impact Assessments. *Technology and Regulation,* S. 209–253. https://doi.org/10.26116/techreg.2024.018. https://doi.org/10.26116/techreg.2024.018.

Easterling, Keller (2014): *Extrastatecraft: The Power of Infrastructure Space*. London, New York: Verso.

Edwards, Paul N.; Bowker, Geoffrey C.; Jackson, Stefen J. und Williams, Robin (2009): Introduction: An Agenda for Infrastructure Studies. *Journal of the Association for Information Systems,* 10(5), S. 365–374.

Europäische Kommission (2023a): *More responsibility, less opacity: what it means to be a "Very Large Online Platform" – Statement by Commissioner Breton.* STATEMENT/23/2452, Brüssel, 25.04.2023. https://ec.europa.eu/commission/presscorner/detail/sk/STATEMENT_23_2452.

Europäische Kommission (2023b): *Durchführungsbeschluss der Kommission vom 22.5.2023 über einen Normungsauftrag an das Europäische Komitee für Normung und das Europäische Komitee für elektrotechnische Normung zur Unterstützung der Unionspolitik im Bereich der künstlichen Intelligenz*, C(2023) 3215 final, sowie Anhänge I und II, https://ec.europa.eu/growth/tools-databases/enorm/mandate/593_de.

Federrath, Hannes (1998): *Vertrauenswürdiges Mobilitätsmanagement in Telekommunikationsnetzen.* Dissertation, TU Dresden, Fakultät Informatik, Februar 1998.

Felt, Ulrike; Fouché, Rayvon; Miller, Clark A. und Smith-Doerr, Laurel (Hrsg.) (2017): *The Handbook of Science and Technology Studies*. 4. Aufl. Cambridge: MIT Press.Glasze, Georg u. a. (2022): Contested Spatialities of Digital Sovereignty. *Geopolitics*, 28(2), S. 919–958. https://doi.org/10.1080/14650045.2022.2050070.

Graf, Constantin (2025): *Europäische Alternativen für digitale Produkte.* https://european-alternatives.eu/de.

Hagdu, Asmelash Teka und Gebru, Timnit (2025): Replacing Federal Workers with Chatbots Would Be a Dystopian Nightmare. *Scientific American*. https://www.scientificamerican.com/article/replacing-federal-workers-with-chatbots-would-be-a-dystopian-nightmare/.

Haugaard, Mark (2022): Foucault and Power: A Critique and Retheorization. *Critical Review*, 34(3–4), S. 341–371. https://doi.org/10.1080/08913811.2022.2133803.

International Energy Agency (IEA) (2025): *Energy and AI*, IEA, Paris. https://www.iea.org/reports/energy-and-ai.

IT-Planungsrat (2021): *Strategie zur Stärkung der Digitalen Souveränität für die IT der Öffentlichen Verwaltung – Strategische Ziele, Lösungsansätze und Maßnahmen zur Umsetzung*, Version 1.0 Januar 2021. https://www.it-planungsrat.de/fileadmin/beschluesse/2021/Beschluss2021-09_Strategie_zur_Staerkung_der_digitalen_Souveraenitaet.pdf.

IT-Planungsrat (2025): *Offene Austauschformate*. Beschluss 2025/06 vom 26.03.2025. https://www.it-planungsrat.de/beschluss/beschluss-2025-06.

Jasanoff, Sheila (Hrsg.) (2004): *States of Knowledge: The Co-Production of Science and the Social Order*. London: Routledge.

Köhntopp, Kristian; Köhntopp, Marit und Pfitzmann, Andreas (2000): Sicherheit durch Open Source? – Chancen und Grenzen. *Datenschutz und Datensicherheit (DuD)* 24(9), S. 508–513.

Kompetenzzentrum Öffentliche IT (ÖFIT) (2017): *Digitale Souveränität,* November 2017. https://www.oeffentliche-it.de/publikationen?doc=71579&title=Digitale+Souveränität.

Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (2023): *Kriterien für Souveräne Clouds.* Positionspapier vom 11. Mai 2023. https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/2023-05-11_DSK-Positionspapier_Kriterien-Souv-Clouds.pdf.

Kwet, Michael (2022): Digital Colonialism and Infrastructure-as-Debt. *University of Bayreuth African Studies Online,* S. 65–77. https://ssrn.com/abstract=4004594.

Land Schleswig-Holstein (2024): *Die Open Innovation und Open Source Strategie des Landes Schleswig-Holstein.* https://www.schleswig-holstein.de/DE/landesregierung/themen/digitalisierung/linux-plus1/Downloads/_dateien/open-source-strategie.pdf.

Larkin, Brian (2013): The Politics and Poetics of Infrastructure. *Annual Review of Anthropology,* 42(1), S. 327–343. https://doi.org/10.1146/annurev-anthro-092412-155522.

Lessig, Lawrence (2001): *Code Version 2.0.* Basic Books, New York. https://commons.wikimedia.org/wiki/File:Code_v2.pdf.

Leyden, John (2014): *Sir Tim Berners-Lee defends decision not to bake security into www.* The Register, https://www.theregister.com/2014/10/08/sir_tim_bernerslee_defends_decision_not_to_bake_security_into_www/.

Luitse, Dieuwertje (2024): Platform Power in AI: The Evolution of Cloud Infrastructures in the Political Economy of Artificial Intelligence. *Internet Policy Review,* 13(2). https://doi.org/10.14763/2024.2.1768.

Musiani, Francesca (2022): Infrastructuring Digital Sovereignty: A Research Agenda for an Infrastructure-Based Sociology of Digital Self-Determination Practices. *Information, Communication & Society,* 25(6). S. 785–800. https://doi.org/10.1080/1369118X.2022.2049850.

National Institute of Standards and Technology (NIST) (2014): *NIST Removes Cryptography Algorithm from Random Number Generator Recommendations.* 21.04.2014, https://www.nist.gov/news-events/news/2014/04/nist-removes-cryptography-algorithm-random-number-generator-recommendations.

Rieder, Bernhard (2020): *Engines of Order: A Mechanology of Algorithmic Techniques.* Amsterdam University Press. https://doi.org/10.2307/j.ctv12sdvfl.

Rip, Arie; Misa, Thomas J. und Schot, Johan (Hrsg.) (1995*): Managing Technology in Society: The Approach of Constructive Technology Assessment*. London: Pinter Publishers.

Rodiles, Alejandro (2022): Infrastructural Developmentalism and Its Many Types of Global Law: A Comparative Look at the UN Sustainable Development Goals and China's Belt and Road Initiative. *London Review of International Law,* 10, S. 367–390.

Rogers, Michael und Grace Eden (2017): The Snowden Disclosures, Technical Standards, and the Making of Surveillance Infrastructures. *International Journal of Communication* 11, 802-823.

Roßnagel, Alexander (1997): Globale Datennetze: Ohnmacht des Staates – Selbstschutz der Bürger, *Zeitschrift für Rechtspolitik*, 26 ff.

Seeger, Martin (2024): Aktenzeichen XZ ungelöst – Haarscharf an einer Katastrophe vorbei? *Datenschutz und Datensicherheit (DuD),* 48(9), S. 589–594.

Star, Susan Leigh (1999): The Ethnography of Infrastructure. *American Behavioral Scientist,* 43(3), S. 377–391. https://doi.org/10.1177/00027649921955326.

Teirstein, Zoya (2025): Project 2025 was extreme. Trump's first 100 days have been even more radical. *Grist,* 30.04.2025. https://grist.org/accountability/project-2025-tracker-trump-environmental-policy-legal-constitutional-crisis/.

van Dijck, José; Poell, Thomas und Waal, Martijn (2018): *The Platform Society: Public Values in a Connective World*. New York: Oxford University Press.

van Dijck, José; Nieborg, David und Poell, Thomas (2019): Reframing Platform Power. *Internet Policy Review,* 8(2). https://doi.org/10.14763/2019.2.1414.

Vought, Ross (2023): Executive Office of the President of the United States of America, in: Dans, Paul und Groves, Steven (Hrsg.): A Mandate for Leadership – Project 2025, S. 43–67.

Zentrum Digitale Souveränität (ZenDiS) (2025): *Digitale Souveränität als Staatsaufgabe – Bausteine einer souveränen Digitalstrategie,* 02/2025. https://admin.zendis.de/wp-content/uploads/2025-02-Bausteine-souveraene-Digitalstrategie-LP21-Kurzfassung.pdf.