Fundamentals

Digitale Souveränität

Dr. Esther Görnemann

Wissenschaftliche Referentin Forschungssynthesen

https://www.weizenbaum-institut.de/portrait/p/esther-goernemann/

Veröffentlicht: 09.10.2026

Zitieren: Görnemann, E. (2024). Digitale Souveränität (Reihe Fundamentals). Berlin: Weizenbaum-Institut. https://doi.org/10.34669/wi.fund/2.de.web

Kompaktüberblick Digitale Souveränität

Klingt gut, bedeutet viel. Was ist digitale Souveränität jenseits politischer Rhetorik?

1.1 Objekte der digitalen Souveränität

1.2 Akteure der Souveränität

Was bedeutet Souveränität? Ein historischer Exkurs

Das große Erwachen. Warum will man digital souverän sein?

2.1 Cyberspace-Souveränität

2.2 Die eingemauerten Gärten des proprietären Internets

2.3 Die Macht der Plattformen

2.4 Massenüberwachung und Cyberspionage

Digitale Spionage - Die NSA Affäre

2.5 Abschottung und Isolation

2.6 Geoökonomische Abhängigkeit

Was sind Mikrochips?

2.7 Cyberangriffe und hybride Bedrohungen

Wege in die selbstbestimmte Zukunft. Wie werden wir digital souverän?

3.1 Gesetzgebung als wertorientiertes Gestaltungsinstrument

3.2 Rahmenbedingungen digitaler Souveränität

3.3 Digitale Souveränität auf Daten Ebene

3.4 Digitale Souveränität auf Code Ebene

3.5 Digitale Souveränität auf der physischen Ebene

Ausblick

Glossar

Referenzen

KOMPAKTÜBERBLICK DIGITALE SOUVERÄNITÄT

Der Begriff „digitale Souveränität“ ist aus dem politischen Diskurs nicht mehr wegzudenken. Man ist sich über Parteigrenzen hinweg einig: Digital souverän sein, das ist erstrebenswert und wichtig. Dabei bleibt aber unklar, was es eigentlich genau bedeutet, digital souverän zu sein und wie man diesen wünschenswerten Zustand erreicht. Fast jede digitalpolitische Maßnahme ließe sich heute mit dem Ziel der digitalen Souveränität rechtfertigen und rhetorisch aufpolieren. Trotzdem ist digitale Souveränität mehr als ein bedeutungsleeres Schmuckwort. Sie verdeutlicht die politischen Dimensionen digitaler Infrastrukturen und verweist auf Handlungsspielräume, in denen wir unsere digitale Zukunft selbstbestimmt mitgestalten können. Um digitale Souveränität in ihrer ganzen Bandbreite zu veranschaulichen, widmet sich dieser Kompaktüberblick **drei zentralen Fragen.**

Klingt gut, bedeutet viel. Was ist digitale Souveränität, jenseits von politischer Rhetorik?

Wir hinterfragen den politischen Diskurs um digitale Souveränität und finden Antworten auf die Frage, **wer** hier eigentlich **worüber** souverän werden soll. Im Anschluss stellen wir den geschichtlichen Bezug zur staatlichen Souveränität her, die zwar eine ähnlich bewegte Bedeutungsgeschichte hat, ansonsten aber mit digitaler Souveränität oft nicht mehr viel gemein hat.

Zum Kapitel springen

Das große Erwachen. Warum möchte man digital souverän werden?

Die letzten 30 Jahre Internetgeschichte lieferten viele berechtigte Anlässe, „das Digitale“ als Herausforderung für die Souveränität von öffentlichen Einrichtungen, Unternehmen, Individuen und kollektiven Bewegungen zu werten. Wir rekapitulieren **sieben wichtige Ereignisse** und Entwicklungen, die den Ruf nach digitaler Souveränität befeuerten und grundlegende Fragen der Machtverteilung und Gestaltungshoheit im digitalen Zeitalter aufwerfen.

Zum Kapitel springen

Die digitale Souveränität verschiedener Akteure kann durch unterschiedliche **staatliche Interventionen** gefördert werden. Dabei geht es in der EU und Deutschland unter anderem um die Förderung von Digitalkompetenz, Infrastrukturausbau, Datenpolitik, Plattformregulierung, die Entwicklung von Schlüsseltechnologien und Cybersicherheit. Die thematisierten Maßnahmen sollten im Idealfall wie Puzzleteile ineinandergreifen.

Zum Artikel springen

KLINGT GUT, BEDEUTET VIEL. WAS IST DIGITALE SOUVERÄNITÄT JENSEITS POLITISCHER RHETORIK?

„Wir müssen unsere digitale Souveränität stärken“, erklärte Bundeskanzler Olaf Scholz 2022 auf der Konferenz re:publica [1. *„Was wir jetzt in jedem Sektor, für jede Innovation brauchen, sind europäische Lösungen und europäische Souveränität“*, forderte zwei Jahre zuvor auch der französische Präsident Emmanuel Macron, für den das Streben nach digitaler Souveränität zu einem zentralen politischen Vorhaben seiner Präsidentschaft geworden ist [2].

> „Wir müssen unsere digitale Souveränität stärken“
>
> Olaf Scholz 2022

Wir begegnen Forderungen nach digitaler Souveränität auf vielen Ebenen der deutschen und europäischen Politik, in Parteiprogrammen, Strategiepapieren von Ministerien, in der EU-Kommission, dem Europarat, in Sicherheitsbehörden, unter Internetaktivist:innen und in Wirtschaftsverbänden. So allgegenwärtig der Begriff jedoch auch sein mag, seine eigentliche Bedeutung bleibt meist unscharf. Akteure aus Politik, Industrie und Zivilgesellschaft fordern unter dem Banner der digitalen Souveränität unterschiedliche, ja teils sogar widersprüchliche Maßnahmen. Offensichtlich haben wir es mit einem politischen *Hochwertwort* [3]zu tun. Digitale Souveränität ist eine unumstrittene Konsensvokabel. Gleich, welche Digitalpolitik man befürwortet, niemand kann sagen, dass ihm digitale Souveränität egal sei. Wer digitale Souveränität fordert, kann damit seine

politische Agenda rhetorisch aufwerten und mit höheren Idealen verknüpfen, ohne konkrete, überprüfbare Versprechen zu machen. Oft werden Hochwertwörter derart inflationär und in so vielen Kontexten verwendet, dass sie drohen, ihrer Bedeutung vollends beraubt zu werden und zu nichtssagenden Worthülsen zu werden.

Eine einheitliche Definition des Begriffs existiert auch in der Forschung bislang nicht [4][5][6]. Allgemein beinhaltet die Forderung nach digitaler Souveränität meist eine Vorstellung von mehr Autonomie, Entscheidungsfreiheit, Mitbestimmung und Kontrolle über „das Digitale“ [4][5]. Versuchen wir also, diese vage Vorstellung zu konkretisieren. Das kann gelingen, in dem man das Objekt der Souveränität („*Worüber* will man souverän werden?“) und den entsprechenden Akteur („*Wer* soll hier souverän werden?“) genauer bestimmt.

1.1 Objekte der digitalen Souveränität

Was genau „das Digitale“ ist, über das man sich mehr Souveränität erhofft, kann sehr verschieden sein, je nachdem, ob man zum Beispiel gerade über Ressourcenabhängigkeit, Fachkräftemangel, digitale Bildung oder Plattformregulierung spricht. Etwas vereinfacht lassen sich digitale Technologien und Infrastrukturen auf drei Ebenen darstellen, die zusammen das Technologiebündel abbilden: Die physische Ebene, die Code Ebene und die Daten Ebene [4][7][8]. Praktisch jede digitale Anwendung, die wir nutzen, basiert auf einer Kombination von IT-Komponenten auf diesen drei Ebenen.

Um eine E-Mail zu schreiben, benötigen wir mehrere Geräte (physische Ebene). Wir verfassen sie über eine Benutzeroberfläche, hinter der eine Reihe programmierter Software-Komponenten stehen (Code-Ebene) und versenden sie schließlich, indem die Nachricht mittels festgelegter Standards und Protokolle über verschiedene Server und Internetknotenpunkte zum Empfänger geleitet wird (Daten-Ebene).

Digitale Souveränität kann auf jeder dieser Ebenen gedacht werden, indem man sich die Frage stellt, zu welchem Grad sie *selbstbestimmt* oder zumindest *einigermaßen unabhängig* gestaltet werden können. Auf jeder Technologieebene erstreckt sich die angestrebte Wahl- und Gestaltungsfreiheit über die gesamte Leistungskette, also von der Forschung und Entwicklung über die Produktion, die Vermarktung und den Betrieb bis hin zur selbstbestimmten und sicheren Nutzung [9].

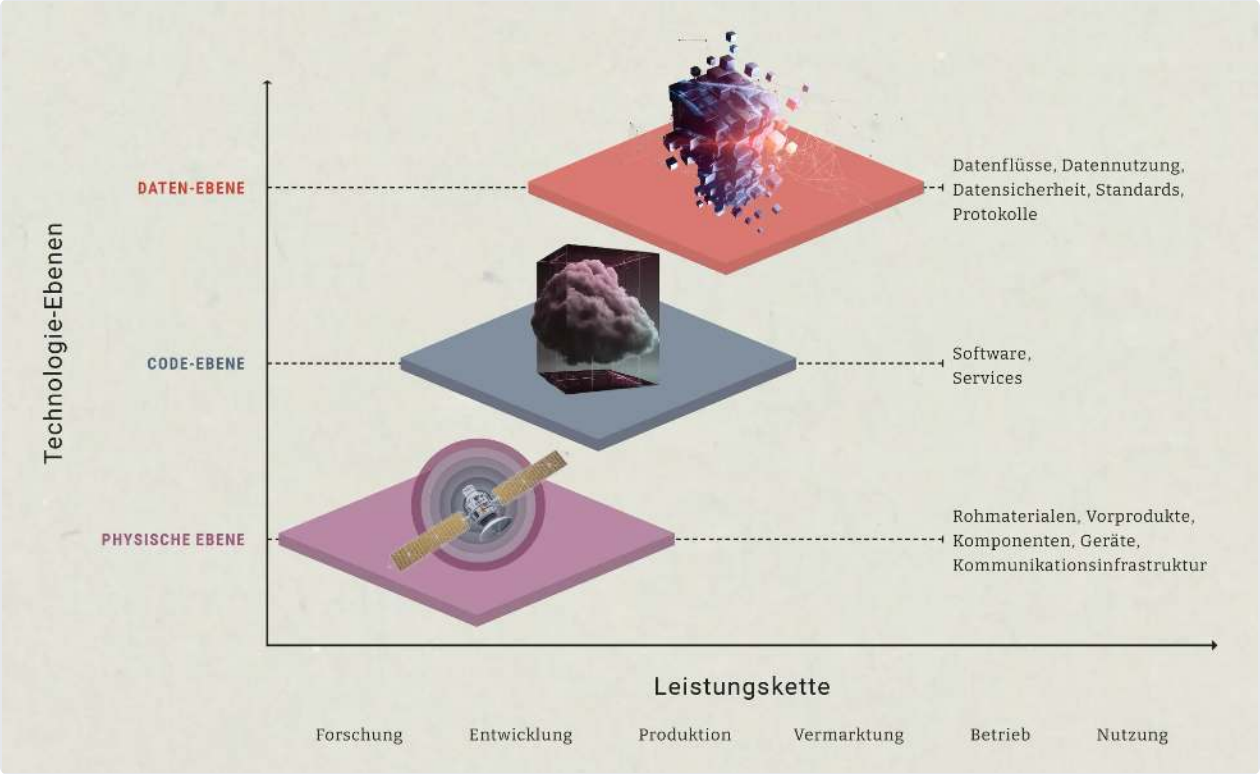


Diagramm der Technologie-Ebenen mit Daten-, Code- und physischer Ebene sowie der dazugehörigen Leistungs-kette

Es ist jedoch weder möglich noch sinnvoll, in all diesen Bereichen „autark“ (also komplett eigenständig) zu werden. Vielmehr kann es schon genügen, Entscheidungsräume zu schaffen, so dass es also Wahlmöglichkeiten zwischen mehreren Alternativen gibt. Gewisse Abhängigkeiten lassen sich ohnehin nicht vermeiden. In Europa existieren zum Beispiel keine nennenswerten Vorkommen seltener Erden, diese sind aber für die Produktion wichtiger technologischer Komponenten erforderlich. Die Abhängigkeit vom Import solcher Ressourcen ist also zwangsläufig. Es gibt auch Abhängigkeiten, die sich nicht zwangsläufig ergeben, sondern einfach über viele Jahre gewachsen sind, zum Beispiel die Dominanz US-amerikanischer Unternehmen in Sachen Cloud Computing. Bestrebungen, sich aus derartigen Abhängigkeiten zu befreien oder sie zu reduzieren, werden auch als „Akte der Resistenz“ [6] gegenüber digitalen Formen der Hegemonie bezeichnet. Denn im Ringen um digitale Souveränität offenbart sich auch die Fortsetzung eines Wettlaufs um ökonomische, politische und militärische Vorherrschaft in der Welt. Der digitale Raum ist neben physischen Territorien wie Land, Wasser, Luft und Weltraum, zum weiteren Schauplatz geostrategischer Machtkämpfe geworden [10].

1.2 Akteure der Souveränität

Unklarheit herrscht im Diskurs um digitale Souveränität insbesondere in der Frage, wessen Souveränität eigentlich gestärkt werden soll. Der Kreis „souveräner Akteure“ wird im politischen und wissenschaftlichen Diskurs oft sehr breit interpretiert. Es geht zum Beispiel um die digitale Souveränität einzelner Ländern oder Gruppen von Staaten – etwa Deutschland [9], die EU [11] oder der globale Süden [12]. Oft wird aber auch ein Fokus auf gesellschaftliche Teilbereiche oder Organisationen gelegt, sei es die öffentliche Verwaltung [13], die Wissenschaft [14], privatwirtschaftliche Unternehmen [15], die Zivilgesellschaft [16] oder Individuen [17]. Wir werden diese Akteursgruppen im dritten Kapitel wieder aufgreifen, weil sich politische Maßnahmen zur Steigerung der digitalen Souveränität meist an spezifische Akteursgruppen richten und jeder Gruppe selbst unterschiedliche Wege zur Verfügung stehen, ihre Gestaltungsspielräume im digitalen Raum auszubauen und zu nutzen.

Seit 1945 bauen die Vereinten Nationen auf das Versprechen, die Souveränität aller Staaten zu wahren.

Quelle anzeigen

Quelle öffnen ↗

Die breite Vielfalt an diskutierten Akteuren, der wir heute begegnen, ist aber erst mit der Zeit gewachsen. Als man vor rund 30 Jahren erstmals im Kontext des Digitalen von Souveränität sprach, lehnte sich deren Bedeutung noch recht stark an das staatstheoretische Verständnis an, das als souveränen Akteur klar den Staat im Blick hat. Dieses Verständnis findet in der Charta der Vereinten Nationen Ausdruck. Die mittlerweile 193 Mitgliedsländer erklären mit der Unterzeichnung der Charta, *die Souveränität anderer Staaten* zu wahren. Die UN-Charta behandelt dabei zwei wesentliche Konzepte von Souveränität, und zwar Souveränität nach innen und Souveränität nach außen.

Siehe Vertiefungstext Was bedeutet Souveränität? Ein historischer Exkurs

Souveränität nach außen

Souveränität nach außen bezieht sich auf das Gewaltverbot und die da

Souveränität nach innen

Souveränität nach innen bezieht sich auf die selbstbestimmte

garantierte *territoriale Unversehrtheit* der Staate UN-Mitgliedstaaten erkl ausdrücklich, auf jeglich Gewalt oder Androhung Gewalt gegen andere Sta zu verzichten. Angriffskr sind nicht mit der UN-Ch vereinbar, selbst Propaga für Angriffskriege ist exp unterlassen. Wird ein Sta angegriffen, hat er das R sich zu verteidigen. Die ä Souveränität eines Staat gegeben, wenn seine territoriale Unversehrthe gewahrt wird.

innerstaatliche Organisation: Jeder Staat hat in seinem Staatsgebiet „*das Recht, sein politisches, soziales, wirtschaftliches und kulturelles System frei zu wählen und zu entwickeln* [18]“. Souveräne Staaten dürfen also frei entscheiden, ob sie z.B. eine soziale Marktwirtschaft oder eine zentral gelenkte Planwirtschaft verfolgen, ob ein Einparteiensystem oder eine demokratische Republik regiert, oder auch ob sie der religiösen Führung weltliche Macht zusprechen. Die innere Souveränität eines Staates ist gegeben, wenn er über seine inneren Angelegenheiten selbstbestimmt und unabhängig entscheiden kann.

DAS GROSSE ERWACHEN. WARUM WILL MAN DIGITAL SOUVERÄN SEIN?

In den vergangenen 25 Jahren drang die Digitalisierung in weite Bereiche der Gesellschaft vor. Freizeitaktivitäten, zwischenmenschliche Kommunikation, Medienkonsum, Verwaltungsabläufe, ja, ganze Berufsgruppen verlagerten sich in den digitalen Raum. Es kam zu tiefgreifenden Umwälzungen, die neue Fragen der Autonomie,

Kontrolle und Machtverteilung zwischen verschiedenen Interessensgruppen aufwarfen. Im Laufe der Zeit gab es immer wieder Ereignisse, die dazu führten, dass man den Souveränitätsbegriff bemühte und ihn dabei neu interpretierte – bis digitale Souveränität schließlich zum politischen Hochwertwort wurde, das allgegenwärtig ist, aber eine enorme Bedeutungsbreite aufweist und nur selten definiert wird.

Wir rekapitulieren in diesem Kapitel *sieben zentrale Entwicklungen* der Internetgeschichte, in deren Zusammenhang von Souveränität gesprochen wurde. Sie erklären einerseits, warum der Begriff „digitale Souveränität" mit der Zeit so vieldeutig geworden ist. Sie zeigen aber auch, dass entlang der gesamten Leistungskette digitaler Infrastrukturen die Macht- und Gestaltungsinteressen verschiedener Gruppen aufeinandertreffen und auszuhandeln sind. Wie dies letzten Endes gelingen kann und wie an empfundenen Missständen gerüttelt wird, darauf gehen wir dann im dritten Teil des Kompaktüberblicks ein.

2.1 Cyberspace-Souveränität

Menschen sprechen seit vielen Jahrhunderten über Souveränität, und dabei ist eines stets erhalten geblieben: Sie ist an ein territoriales Konzept gebunden. Die Staatshoheit bezieht sich immer auf ein definiertes, physisch existentes Territorium, das die *Grenzen des Staatsgebiets* festlegt. Der digitale Raum – in den 90er Jahren gern „Cyberspace" genannt – ist jedoch kein physisches Territorium in diesem Sinne, denn ein fester geographisch-politischer Bezugsrahmen im Sinne eines Staatsgebietes ist schlicht nicht gegeben. Schon früh stand deshalb die Frage im Raum, in wessen Staatsgebiet der Cyberspace falle, wenn überhaupt in eines.

Mitte der 1990er Jahren sprach man in diesem Zusammenhang von „Cyberspace-Souveränität". In der technischen Community und der akademischen und journalistischen Debatte dominierte das Narrativ, der Cyberspace sei eine neue Sphäre menschlicher Aktivität, die sich in ihrer Natur fundamental von allem Dagewesenen unterscheide. Man war überzeugt, dass es schwierig bis unmöglich sein werde, sie mit dem existierenden rechtlichen Instrumentarium zu regulieren oder zu kontrollieren. Gesetze – so die gängige Annahme – galten schließlich nur innerhalb definierter territorialer Grenzen. Außerhalb dieser Grenzen seien sie weder durchsetzbar, noch besäßen sie Legitimität [23]. Eine der gewagtesten Forderungen lautete, dass der Cyberspace mit seiner grenzüberschreitenden, globalen Vernetzung und dezentralen Organisation so außergewöhnlich sei, dass er *seine eigene Souveränität brauche*, ähnlich wie ein eigener Nationalstaat. Diese Vision des Cyberspace wird verkörpert durch Internet-Pionier John Perry Barlow. 1996 verfasste er die „Unabhängigkeitserklärung des Cyberspace", die am eindrucksvollsten von ihm selbst vorgetragen wird.

John Perry Barlow, Internet-Pionier

Das Multi-Stakeholder-Governance-Ideal – Regieren mit der Weisheit der Vielen

Ursprünglich bedeutete „regieren“ im Internet hauptsächlich, technische Entscheidungen zu treffen, etwa in der Entwicklung von Standards und Datenprotokollen. Das Internet sollte eine quasi-neutrale Struktur werden, in der Informationen frei und offen von einem Ende der Welt zum anderen transportiert werden können und zu der alle Menschen gleichermaßen Zugang bekommen. Den Idealen der Freiheit und Offenheit entsprechend hatte sich für Entscheidungsfindungen das Multi-Stakeholder-Governance-Modell durchgesetzt. Möglichst alle, die sich im Internet aufhalten, sollten sich auch an seiner Entwicklung beteiligen können – neben Regierungen also auch die Privatwirtschaft, die technische Community und die Zivilgesellschaft [24]. Nach den Prinzipien der allgemeinen Teilhabe, transnationalen Zusammenarbeit und Konsensfindung wurden Entscheidungen, die die technische Weiterentwicklung des Internets betrafen also von vielen unterschiedlichen Interessensvertretern gemeinsam getroffen [25].

Gegen Ende der 1990er Jahre begann die rasante Kommerzialisierung des Internets, mit der ein rascher Anstieg der Nutzerzahlen, verfügbaren Anwendungen und abrufbaren Inhalte einherging. Das existierende „Regierungssystem“ des Internets – also Instandhaltung und Regulierung technischer Strukturen nach gemeinsamen Entscheidungen der Internetgemeinschaft – war nicht geeignet, um sicherzustellen, dass abrufbare Inhalte und Anwendungen lokalen Gesetzgebungen entsprachen. Staatliche Intervention und Regulierung wurde deshalb zunehmend als notwendig erachtet, um das Internet im Einklang mit nationalen Rechtsvorstellungen zu gestalten [26][27]. So setzten sich auf Ebene der Anwendungen und Inhalte im Internet zunehmend staatliche Regulierungsmaßnahmen durch, während auf Ebene der technischen Infrastrukturen, Standards und Protokolle bis heute nicht-Regierungsorganisationen nach Multistakeholder-Governance-Prozessen „regieren“.

2.2 Die eingemauerten Gärten des proprietären Internets

Die Kommerzialisierung des Internets führte also letztendlich zu mehr staatlicher Intervention im Internet. Aber genauso bedeutete sie zunehmende privatwirtschaftliche Intervention in die Gestaltung von Technologie. Gerade weil das Internet sich über viele Jahre frei und organisch entwickeln konnte und nicht auf Initiative kommerzieller Unternehmen entstanden war, erlaubte es radikal neue Formen der kooperativen Wertschöpfung [28]. Eine besondere Rolle spielten Open-Source-Methoden, bei denen international verstreute Gruppen von Menschen, oft unentgeltlich, gemeinsam Code und Software schrieben. Kollaborationsprojekte wie Wikipedia oder Linux waren nur machbar, weil das Internet eine offene Plattform war – und in vielerlei Hinsicht natürlich auch noch ist. Es war nicht für einen speziellen, kommerziellen Zweck gebaut worden, sondern als offener, kreativer Raum gedacht, der permanent durch seine Nutzer:innen verändert und weiterentwickelt wurde.

Die Kommerzialisierung des Internets führte also letztendlich zu mehr staatlicher Intervention im Internet. Aber genauso bedeutete sie zunehmende privatwirtschaftliche Intervention in die Gestaltung von Technologie. Gerade weil das Internet sich über viele Jahre frei und organisch entwickeln konnte und nicht auf Initiative kommerzieller Unternehmen entstanden war, erlaubte es radikal neue Formen der kooperativen Wertschöpfung [28]. Eine besondere Rolle spielten Open-Source-Methoden, bei denen international verstreute Gruppen von Menschen, oft unentgeltlich, gemeinsam Code und Software schrieben. Kollaborationsprojekte wie Wikipedia oder Linux waren nur machbar, weil das Internet eine offene Plattform war – und in vielerlei Hinsicht natürlich auch noch ist. Es war nicht für einen speziellen, kommerziellen Zweck gebaut worden, sondern als offener, kreativer Raum gedacht, der permanent durch seine Nutzer:innen verändert und weiterentwickelt wurde.

Apple II, 1977

Das iPhone hingegen symbolisiert den Vormarsch des Digitalen in Form von „sterilen“, vorprogrammierten Geräten und Services. Ein Einsehen oder gar Verändern des Programmcodes ist nicht mehr vorgesehen. Zu installierende Programme werden in App Stores vorselektiert oder direkt von Haus aus auf dem Smartphone

installiert. Sicherheitsupdates für ältere Geräte werden nach Belieben eingestellt. Wurde die Revolution der Computer und des Internets also einst von innovativen Gestaltungsspielräumen angetrieben, so ist die proprietäre Version des Digitalen heute eine ästhetische Welt der *„eingemauerten Gärten“* [29]. Diese Welt mag einfach zu nutzen, gut designt und komfortabel sein, aber sie ist eingewoben in ein Netzwerk aus kommerzieller Kontrolle und Restriktion. So geht diese Version des Digitalen mit einem schweren Verlust an digitaler Selbstbestimmung einher und schränkt kreative Gestaltungspielräume maßgeblich ein. Branchenverbände wie die Open Source Business Alliance (OSBA) argumentieren deshalb seit Jahren, dass der Weg in die digitale Souveränität maßgeblich durch einen verstärkten Einsatz und die Weiterentwicklung von quelloffener Software und offenen Standards gerade in der öffentlichen Verwaltung geebnet wird [30].

iPhone, 2007

2.3 Die Macht der Plattformen

Die zunehmende Kommerzialisierung des Internets seit den späten 1990er Jahren lieferte triftige Gründe dafür, das digitale Ökosystem als Herausforderung für die staatliche Souveränität zu sehen. Über viele Jahre konnten die Tech-Giganten der USA – allen voran Alphabet, Amazon, Meta, Apple und Microsoft – nahezu konkurrenzlose Macht aufbauen. Als Plattformunternehmen integrierten sie nach und nach immer mehr Anwendungen und Dienstleistungen in einer Kernplattform. Ihre Infrastrukturen wurden zu allgegenwärtigen Kommunikations- und Organisationsinstrumenten im privaten Alltag, wie auch in zahllosen Betrieben und in der öffentlichen Verwaltung [31]. Die Plattformen profitierten dabei häufig vom „Netzwerkeffekt“ [32], dem Prinzip, dass ein Netzwerk wertvoller wird, je mehr Mitglieder ihm angehören. Hat beispielsweise ein soziales Netzwerk eine kritische Masse an Mitgliedern einmal erreicht, steigt die Zahl der Nutzenden exponentiell an, bis Konkurrenten sich kaum noch durchsetzen können und sich fast zwangsläufig ein Monopol bildet.

Prof. Dr. Jeanette Hofmann

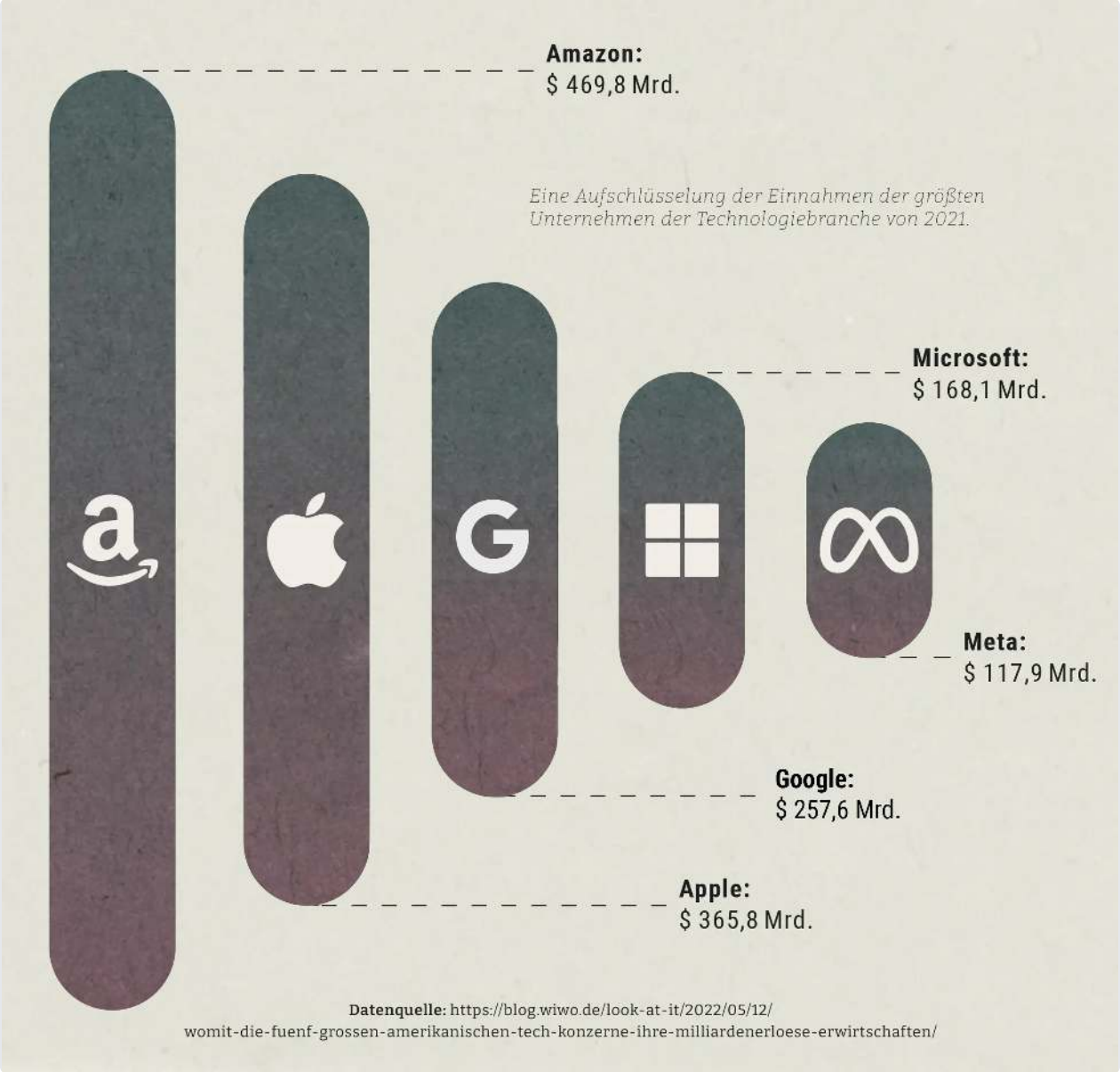
Principal Investigator der Forschungsgruppe „Technik, Macht und Herrschaft“ am Weizenbaum-Institut

„Die ökonomische Theorie der Netzwerkeffekte besagt, dass der Wert einer Infrastruktur wie etwa das Telefonnetz mit der Anzahl verbundener Menschen und Objekte steigt. Von expandierenden Infrastrukturen geht daher ein mehr oder minder **zwangloser Anschlusszwang** aus." (2020)

Go to Profile ↗

Plattformkonzerne bieten essentielle technische Infrastrukturen und Services des Internets, auf die Privatleute, Unternehmen und öffentliche Dienste angewiesen sind. Sie stellen Inhalte und Kommunikationswege bereit, gestalten öffentliche Räume und betreiben Marktplätze, über deren Wettbewerbsbedingungen sie maßgeblich mitbestimmen. Damit besitzen wenige (meist amerikanische) Großunternehmen weitreichende Gestaltungsspielräume und Regulierungskompetenzen – nicht nur über technische Infrastrukturen, sondern auch über die sozioökonomische Konditionen und Prozesse, die sich in ihnen abspielen [33]. Plattformkonzerne werden deshalb nicht selten als „quasi-Souveräne“ im digitalen Raum bezeichnet [18].

Die Dominanz der Plattformen stellt für Europa ein marktwirtschaftliches Risiko dar, weil sie droht, den Wettbewerb zu verzerren und die wirtschaftliche Stabilität und Innovationskraft gefährdet [31]. Plattformkonzerne haben mehr oder minder exklusiven Zugriff auf die enormen Datenmengen, die innerhalb ihrer Strukturen produziert werden. Diese Daten bieten ihnen unmittelbare Wettbewerbsvorteile gegenüber ihrer Konkurrenz. Große Datenmengen sind aber auch eine Voraussetzung dafür, Schlüsseltechnologien wie künstliche Intelligenz zu entwickeln [15]. Die Nachteile, die sich für europäische Unternehmen aufgrund Dominanz der Plattformkonzerne ergeben, werden gerade in wirtschaftsnahen Kreisen bisweilen als Einschränkung der wirtschaftlichen Handlungsspielräume und damit der digitalen Souveränität verstanden [7] [15].



Einnahmen der größten Unternehmen der Technologiebranche von 2021, Amazon, Apple, Google, Microsoft und Meta.

Die einseitige Abhängigkeit von ausländisch kontrollierten Unternehmen gilt aber auch als potenzielle Sicherheitsbedrohung. Regierungen können Plattformen als politische Hebel und Druckmittel gegen diejenigen einsetzen, die sich in Abhängigkeit befinden. Die US-Regierung hat dies zum Beispiel 2019 im Handelskonflikt mit China gezeigt, als das Handelsministerium Google per Dekret zwang, sämtliche Geschäfte mit Huawei einzustellen [35]. Auch aus diesem Grund wird die einseitige Abhängigkeit von Plattformunternehmen in der Politik als Herausforderung für die digitale Souveränität gesehen [30][31]. Schließlich äußert sich die Dominanz der Plattformkonzerne auch in ihrem Verhältnis zu ihren Nutzenden, deren Daten zum Rohstoff lukrativer digitaler Produkte geworden sind und deren individuelle digitale Souveränität dadurch deutlich geschwächt wurde [15][37].

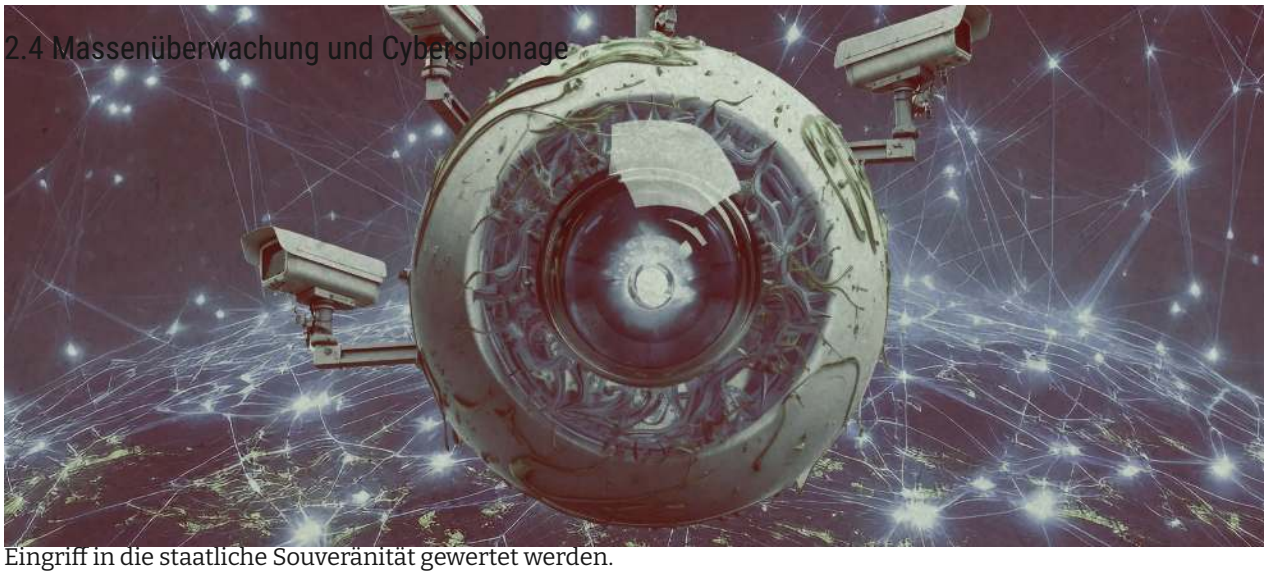
Überwachungskapitalismus – Das Geschäft mit den Daten

Große Plattformen greifen seit vielen Jahren verstärkt auf die lukrative Werbefinanzierung ihrer kostenlosen Services zurück. Früh zeigte sich, dass Werbung gerade im Internet besonders effektiv umgesetzt werden kann, da es hier möglich ist, sie zu personalisieren und gezielt auszuspielen. Hierfür werden im Hintergrund systematisch Nutzerdaten gesammelt, angereichert und analysiert. *Demographie, Konsumverhalten, soziale Kontakte, Interessen und Präferenzen, Persönlichkeit, Lebenssituation, Standort* – je detaillierter die Erkenntnisse, desto besser können individuell zugeschnittene Werbemaßnahmen zum richtigen Zeitpunkt, am richtigen Ort und im richtigen Kontext präsentiert werden. Der gigantische Marktwert der Plattformen beruht nicht zuletzt auf der Fähigkeit, zukünftiges (Konsum-) Verhalten vorhersagen und effektiv beeinflussen zu können. Während Nutzende im Rahmen dieser Geschäftsmodelle zunehmend transparenter wurden, blieb die Industrie dahinter

vergleichsweise undurchsichtig. Man spricht in diesem Zusammenhang von „Informationsasymmetrie“ – einem Zustand, in dem zwei Vertragsparteien nicht über dieselben Informationen verfügen. Wird auf Basis ungleicher Informationen gezielt zukünftiges Verhalten manipuliert, erwächst aus einer Informationsasymmetrie auch eine Machtasymmetrie [38]. Dass derartige Machtasymmetrien auch potentiell demokratiegefährdende Konsequenzen haben können, wurde 2018 im Zusammenhang mit dem Skandal um Cambridge Analytica [39] [40]intensiv diskutiert.

Die Harvard Ökonomin Shoshana Zuboff sieht die Systeme des Überwachungskapitalismus als *Angriff auf die individuelle digitale Souveränität*, weil sie die autonome Handlungs- und Entscheidungsfähigkeit Einzelner untergraben [37]. Gerade wenn im Kontext demokratischer Prozesse (wie Wahlen und Volksentscheide) die selbstbestimmte Handlungsfähigkeit der Bürger:innen unterwandert wird, kann man dies durchaus auch als Eingriff in die innere Souveränität des Staates verstehen, der durch Plattformen ermöglicht wird. Im November 2019 war Shoshana Zuboff am Humboldt Institut für Internet und Gesellschaft in Berlin, um über das Zeitalter des Überwachungskapitalismus zu sprechen.

2.4 Massenüberwachung und Cyberspionage



Eingriff in die staatliche Souveränität gewertet werden.

Nicht zuletzt geht es im Diskurs um digitale Souveränität neben staatlichen Belangen auch um die digitale Selbstbestimmung von Individuen und Zivilgesellschaft. Auch die individuelle Datensouveränität – also das *„gezielte, informierte Bereitstellen eigener Daten* [42]“ – wird durch die anlasslose Massenüberwachung von Kommunikationsdaten unmittelbar unterwandert.

Was die von Snowden geleakten Dokumente nachweisen, sind tiefgehende, globale Überwachungsanstrengungen durch die Geheimdienste westlicher Staaten, insbesondere der USA. Zweifel an ihrer Glaubhaftigkeit räumte der Europäische Gerichtshof in gleich zwei Urteilen unmissverständlich aus. So bestätigten die höchsten Richter 2015, dass *„die NSA und andere amerikanische Sicherheitsbehörden*“ auf personenbezogene Daten *„im Rahmen einer massenhaften und undifferenzierten Überwachung und Erfassung zugreifen* [43]“.

Die NSA-Affäre

Siehe VertiefungstextDigitale Spionage - Die NSA Affäre

Politische Spionage und Wirtschaftsspionage

Die NSA-Affäre zeigte zudem, dass die Aufgabe der Geheimdienste auch darin bestand, *Konkurrenzspionage* zu betreiben. Dies wurde schon 2001 bekannt, als sich ein Ausschuss des Europäischen Parlaments mit „Echelon“ beschäftigte, einem globalen Abhörsystem der Five Eyes, das die globale Satellitenkommunikation abhörte [54].

Der Bericht des Ausschusses legt nahe, dass der Geheimdienstverbund gezielt die Kombun munikation von Unternehmen abhörte. Ausländische Unternehmen wurden ausspioniert, um inländischen Unternehmen Wettbewerbsvorteile zu verschaffen. Mit den erlangten Informationen konnten US-Unternehmen zum Beispiel ihren europäischen Konkurrenten bei Patentanmeldungen zuvorkommen [55][56], oder sie in Verhandlungen ausstechen [57][58]. Den Snowden Leaks lässt sich entnehmen, dass Industriespionage auch zwölf Jahre später noch zu den strategischen Missionen der NSA gehörte [59]. Neben Russland und China gehörten auch Deutschland und Frankreich zu den Zielländern der NSA. Die Mission sah vor, jeglichen Vorsprung in kritischen Technologien zu unterbinden, der diesen Ländern militärische, ökonomische oder politische Vorteile verschaffen würde.

weapons.
c. Threats posed by foreign space and counter-space systems: China and Russia
Accepted Risks:
a. Weapons and force developments in: Saudi Arabia, and India
b. Threats posed by foreign space and counter-space systems: India and France.

(S//SI) **J. MISSION: Emerging Strategic Technologies: Preventing Technological Surprise.**
Focus Areas: Critical technologies that could provide a strategic military, economic, or political advantage: high energy lasers, low energy lasers, advances in computing and information technology, directed energy weapons, **stealth and counter-stealth**, electronic warfare technologies, space and remote sensing, electro-optics, nanotechnologies, energetic materials. The emerging strategic technology threat is expected to come mainly from Russia, China, India, Japan, Germany, France, Korea, Israel, Singapore, and Sweden.
Accepted Risks: Technological advances and/or basic S&T development on a global basis elsewhere.

(S//SI) **K. MISSION: Foreign Policy ((includes Intention of Nations and Multinational Orgs)): Ensuring Diplomatic Advantage for the U.S.**
Focus Areas: Positions, objectives, programs, and actions on the part of governments or multilateral organizations that could significantly impact U.S. national security interests: China, Russia, France

Geleakte NSA-Unterlagen: Auch unter Freunden dient Konkurrenzspionage dem Zweck, sich militärische, ökonomische und politische Vorteile zu verschaffen

Quelle: New York Times

Quelle öffnen ↗

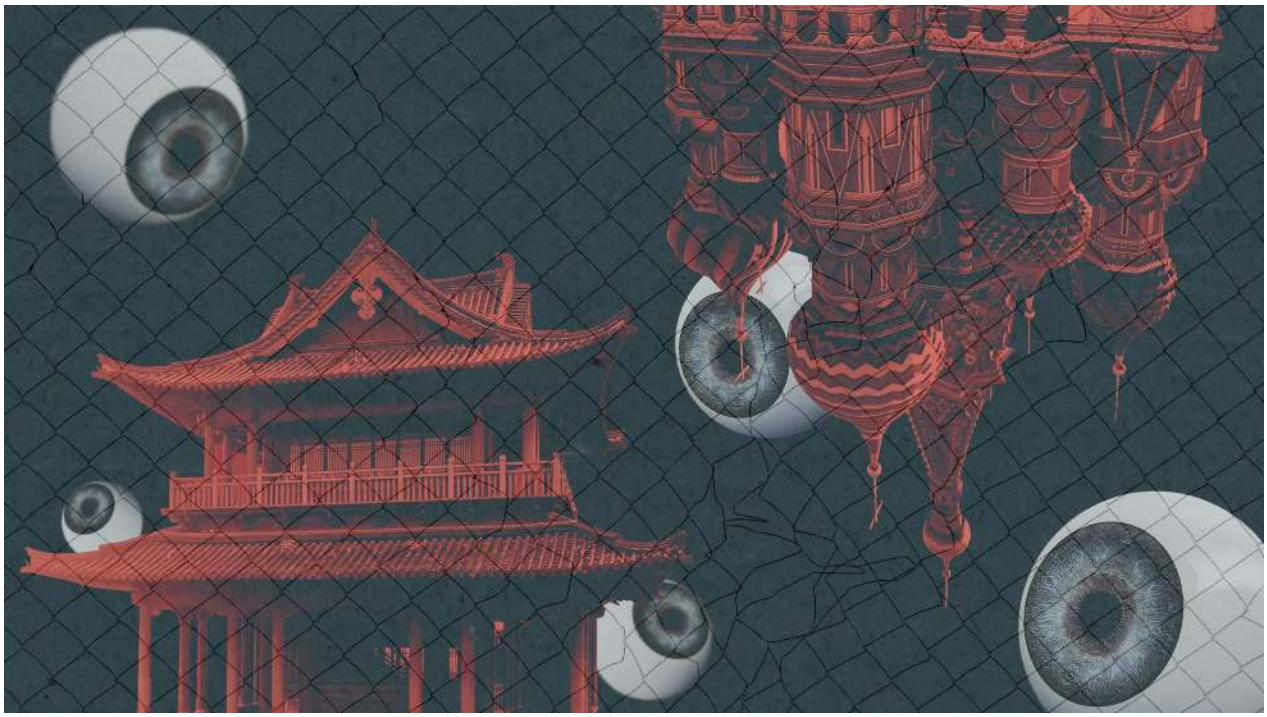
Dokumente der NSA beschreiben zudem das jahrelange, systematische und gezielte Abhören von Spitzenpolitiker:innen – darunter auch Angela Merkel [60] – und politischen Einrichtungen. Unter den politischen Zielen befand sich Berichten zufolge die Zentrale der Vereinten Nationen [61], die Internationale Atomenergie-Organisation [62] und mittels Cyberangriff auf den belgischen Konzern Belgacom mutmaßlich auch die Europäische Kommission, der Europäische Rat, das Europäische Parlament und die NATO [63].

2.5 Abschottung und Isolation

In autoritären Staaten wie China oder Russland wurde der Vormarsch vernetzter Kommunikation als Bedrohung der bestehenden politischen Ordnung wahrgenommen [5]. Als eines der ersten Länder reagierte China mit einer Strategie der maximalen technischen Isolation und Kontrolle. Russland folgte diesem Beispiel wenige Jahre später. Die chinesische Regierung stützte sich dabei auf eine für sie typische Interpretation der nationalen Souveränität als Nicht-Einmischungsgebot. Im Kern habe sich kein anderes Land in chinesische Angelegenheiten einzumischen, dafür würde sich auch China nicht in die Angelegenheiten anderer Staaten (etwa in bewaffnete Konflikte) einmischen. Diese Souveränitätsrhetorik wurde seitens China schon in den frühen 2000er Jahren verwendet. Nach der NSA-Affäre 2013 fand sie mehr Anwendung auf den digitalen Kontext und wurde zu einer weiteren Interpretation digitaler Souveränität, die in ihrer radikalen Umsetzung jedoch weit vom europäischen Verständnis entfernt ist. Digitale Souveränität (hier meist „Cybersouveränität“ genannt) bedeutet in diesem

Zusammenhang, Datenströme und digitale Infrastrukturen möglichst vollständig der nationalen Kontrolle zu unterwerfen.

Das Splinternet – Autoritäre Staaten schotten sich ab



In Reaktion auf die NSA-Affäre erklärte China 2015 als eines der ersten Länder der Welt „Cybersouveränität" zu Ziel und Grundsatz seiner digitalpolitischen Maßnahmen. In seiner Eröffnungsrede der Global Internet Conference erklärte Chinas Präsident Xi Jinping 2015, dass im Sinne der staatlichen Souveränität jedes Land seine eigenen Regulierungsansätze im Internet verfolgen dürfen sollte [64]. Niemand solle in die Cybersouveränität eines anderen Landes eingreifen, sich mittels digitaler Kanäle in die inneren Angelegenheiten anderer Staaten einmischen oder Cyberaktivitäten unterstützen, die die nationale Sicherheit eines anderen Landes untergraben [65]. China sieht Cybersouveränität primär als einen Weg, die nationale Sicherheit zu wahren, das Land vor äußerer Einflussnahmen und wirtschaftlicher Spionage zu schützen [5], aber auch, um die lokale Wirtschaft zu unterstützen, indem chinesischen Firmen bevorzugte Behandlung zuteilwird [65]. Ähnlich verhält es sich in Russland, wo digitale Souveränität mit stärkerer staatlicher Kontrolle über den digitalen Raum und insbesondere über den Datenverkehr auf russischem Staatsgebiet gleichgesetzt wird [65].

Eine wichtige Rolle in dieser Strategie spielt die *Datenlokalisierung* [66], die vorsieht, dass Daten möglichst nur noch innerhalb nationaler Grenzen und rechtlicher Zuständigkeiten gespeichert, übertragen und verarbeitet werden. Hierfür ist es erforderlich, Kontrolle über die wesentlichen technischen Infrastrukturen des Internets zu erlangen bzw. diese auf dem eigenen Staatsgebiet zu lokalisieren. Technisch umgesetzt wird dies zum Beispiel mit nationalen Dateninfrastrukturen, lokalen Datenzentren, nationalem Routing, nationalen E-Mail Services und nationaler Grundnetz-Infrastruktur [67].

Die geschaffenen Strukturen bieten jedoch auch neue Möglichkeiten für die systematische Überwachung und Zensur der Bevölkerung. In Russland beispielsweise sind Internetanbieter seit 2019 durch das „Sovereign Internet Law" verpflichtet, Netzwerktechnik zu installieren, die eine effektivere Überwachung des Datenverkehrs und die Sperrung unerwünschter Inhalte ermöglichen. In China sorgen die „Internet Domain Name Regulations" seit 2019 dafür, dass jeglicher grenzüberschreitender Datenverkehr geblockt wird, der zuvor nicht ausdrücklich von den Zensurbehörden genehmigt wurde. Will beispielsweise ein ausländisch registriertes Nachrichtenportal in China abrufbar sein, wird es sich selbst zensieren müssen [68].

Abschottungstendenzen in der EU

Argumente für stärkere technische Abschottung wurden nach der NSA-Affäre auch in westlichen Ländern laut, beispielsweise in der Diskussion um das Schengen-Routing [69]. Das erklärte Ziel dabei war es, den Schutz vor Spionageaktivitäten ausländischer Geheimdienste im Schengenraum zu stärken. Das Schengen-Routing wäre nicht zuletzt mit dem willkommenen Nebeneffekt verbunden gewesen, dass europäische Firmen, insbesondere die Deutsche Telekom, von dieser Umsetzung hätten profitieren können [70]. Die Idee wurde jedoch zunächst wieder verworfen. Zu gering sei der tatsächliche Nutzen, zu global vernetzt der Datenverkehr, zu groß die Gefahr eines „*Splinternets*" – eines anhand geographischer und kommerzieller Grenzen in viele voneinander isolierte Bereiche zerfaserten Internets [71][72]. Doch auch rund 10 Jahre nach der NSA-Affäre werden in der Debatte um digitale Souveränität immer wieder ähnliche Argumente für die Lokalisierung essentieller technischer Infrastrukturen innerhalb der EU gemacht, zum Beispiel im Rahmen des europäischen Dateninfrastrukturprojekts Gaia-X [73] (siehe Kapitel 3.3).

Prof. Dr. Thorsten Thiel

Assoziierter Forscher am Weizenbaum-Institut

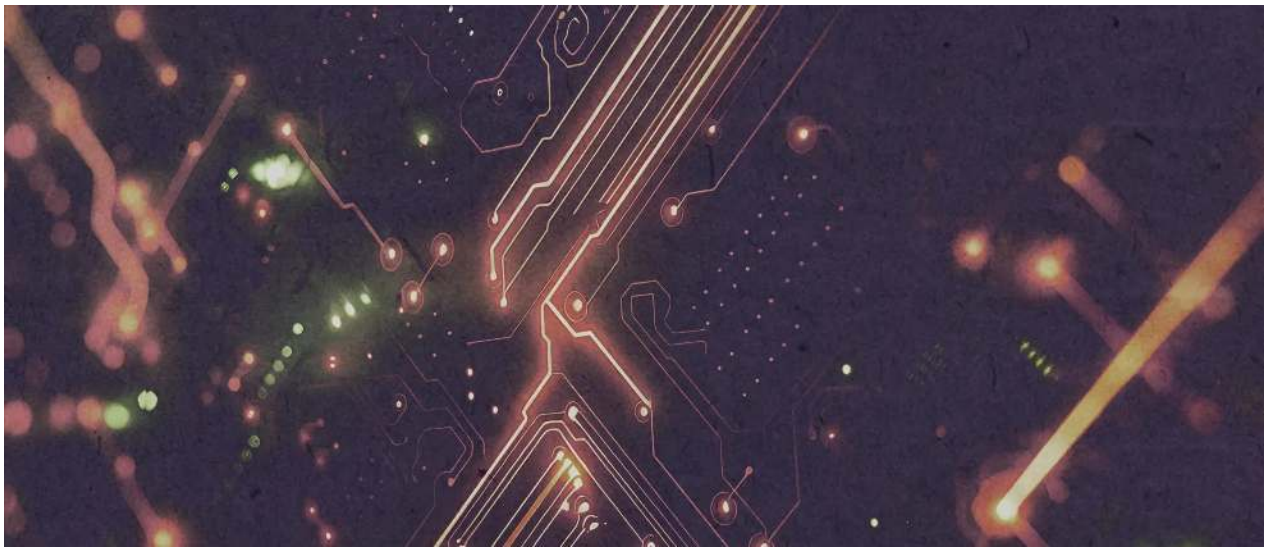
„Das Schengen-Routing war ein im Anschluss an die Snowden-Enthüllungen diskutierter politischer Vorstoß, Datenverkehr stärker zu nationalisieren bzw. zu regionalisieren, um zu verhindern, dass US-amerikanische Dienste Zugriffsmöglichkeiten auf solche Kommunikation erhalten, die ausschließlich zwischen Angehörigen einer Region – in diesem Fall der Region jener europäischen Länder, die dem Schengener Abkommen beigetreten sind – stattfindet." (2014)

Go to Profile ↗

2.6 Geoökonomische Abhängigkeit

In der Debatte um digitale Souveränität geht es gerade auf EU-Ebene häufig darum, sich aus wirtschaftlichen Abhängigkeitsverhältnissen zu befreien. Die Digitalindustrie ist wie kaum ein anderer Industriezweig von Abhängigkeiten geprägt. Wer essentielle Komponenten oder Dienste beherrscht, ist in der Lage, andere Staaten unter Druck zu setzen, wer von einzelnen Zulieferern oder Ländern abhängig ist, macht sich erpressbar. Derartige wirtschaftliche Abhängigkeitsverhältnisse werden im Diskurs um digitale Souveränität sehr prominent thematisiert, denn sie schmälern die Möglichkeit – gerade der europäischen Industrie – unabhängig und selbstbestimmt agieren zu können. Digitale Souveränität (in diesem Zusammenhang wird häufig von „*strategischer Autonomie*" gesprochen [74]) bedeutet hier, die strukturelle Abhängigkeit von digitalen Technologien und geistigem Eigentum aus dem Ausland zu reduzieren, um Verfügbarkeiten zu sichern, Wahlmöglichkeiten zu schaffen und die eigene wirtschaftliche Wettbewerbsfähigkeit zu stärken [31].

Die Halbleiterindustrie



Eine besonders essentielle Komponente digitaler Infrastrukturen bilden Mikrochips – elektronische, auf Halbleitern basierende Bauteile. Sie liefern die Basis für eine Vielzahl moderner Geräte von Smartphones über Computer, Fernseher, Autos, Industrieroboter, Waffensysteme bis hin zu medizinischen Geräten.

Gerade die Halbleiterindustrie ist von außergewöhnlichen Abhängigkeiten geprägt. Denn die erstaunlichen Fortschritte der Mikroelektronik sind nur möglich gewesen, weil sich Unternehmen mit der Zeit extrem spezialisierten. Anstatt alle Schritte vom Schaltungsdesign bis hin zu Test und Montage aus einer Hand anzubieten, wurde es ökonomisch immer sinnvoller, sich auf ein Kerngeschäft zu spezialisieren, das dann entsprechend skaliert wurde. Im Silicon Valley konzentrierten sich Firmen wie AMD, Broadcomm oder Qualcomm zunehmend auf margenträchtige Arbeitsschritte wie das Design von Bauplänen und Schaltungsentwürfen. In Taiwan entstanden große Auftragsfertiger, wie TSMC, der Weltmarktführer in der Produktion von Logik- und Hochleistungschips, die etwa in der künstlichen Intelligenz zum Einsatz kommen [79]. Mikrochips basieren auf global verteilten, kleinteiligen Lieferketten und hochkomplexen Produktionsprozessen. Tausende von Arbeitsschritten greifen minutiös ineinander, wurden über Jahrzehnte verfeinert und spezialisiert. Kein Land der Welt wäre derzeit in der Lage, eine ausreichende Menge Mikrochips im Alleingang zu entwickeln und herzustellen.

Siehe VertiefungstextWas sind Mikrochips?

Jahrzehnte der technologiegetriebenen Globalisierung haben so komplexe Risikokaskaden geschaffen [31]. Fällt die Verfügbarkeit auch nur einer essentiellen Komponente aus, drohen ganze Industriezweige einzubrechen. Entsprechende Produktionskapazitäten im eigenen Land neu aufzubauen würde – ganz ungeachtet der beträchtlichen erforderlichen Investitionen – Jahrzehnte dauern. Dies wäre rein marktwirtschaftlich betrachtet unlogisch und ineffizient. In der Halbleiterindustrie herrscht jedoch schon lang keine marktwirtschaftliche Logik mehr, denn die Handlungsbeziehungen haben sich über Jahre politisiert.

Politisierung und Handelskrieg

Regierungen haben erkannt, dass gerade die Abhängigkeit von ausländisch bezogenen Mikrochips sie verwundbar macht. Halbleiterprodukte sind für viele Branchen und Produkte von essentieller Bedeutung und ihre Verfügbarkeit ist aufgrund fragiler Lieferketten ohne Ausfalloptionen ohnehin unsicher. Darüber hinaus kam es in den letzten Jahren bereits mehrfach zu Lieferausfällen mit teils dramatischen Konsequenzen, zum Beispiel

als während der Coronapandemie ein unerwartet hoher Bedarf nach Computern mit Grenzschließungen und Lock-Downs kollidierte. Bestrebungen, sich aus diesen Abhängigkeiten zu befreien gelten als Weg in die digitale Souveränität [7].

Die globale Halbleiterindustrie wurde zum Schauplatz internationaler Geopolitik und zum Instrument, um gezielt Einfluss auf andere Staaten auszuüben [9]. Zwischen den USA und China herrscht schon länger ein Machtkampf um politische, wirtschaftliche und militärische Vormachtstellung in der Welt, der die beiden Nationen in einen offenen Handelskrieg stürzte. Die USA und China konkurrieren in Schlüsseltechnologien wie künstlicher Intelligenz, autonomen Waffensystemen und Quantencomputern miteinander – alles Technologiefelder, in denen Hochleistungschips eingesetzt werden. Natürlich gibt es vergleichbare Bestrebungen auch in Europa, nur waren diese bislang nicht sonderlich erfolgreich. In der Chipindustrie entwickelte sich ein Wettkampf um Patente, Fertigungsanlagen und Fachkräfte. Beide Länder subventionieren ihre heimische Halbleiterindustrie massiv. Gleichzeitig belegten sie einander in eskalierender Weise mit Importzöllen und Ausfuhrbeschränkungen, um sich wirtschaftliche Vorteile zu verschaffen und Wissenstransfer zu verhindern. Nichtsdestotrotz lässt sich die Halbleiterindustrie nicht so schnell umsiedeln. Amerikanische Hochleistungschips werden noch immer überwiegend in Taiwan gefertigt, weshalb sich die USA vor allem durch Chinas Ambitionen bedroht sehen, die taiwanesische Halbinsel einzunehmen. Dies könnte China nicht nur Einblick in Produktionsprozesse geben, sondern darüber hinaus Kontrolle über die Ausfuhr von Mikrochips in die USA.

2.7 Cyberangriffe und hybride Bedrohungen

Auch das Thema Cybersicherheit hat Einzug in die Debatte um digitale Souveränität gehalten, denn gerade von Sicherheitsbehörden wird ein hohes Cybersicherheitsniveau als Voraussetzung für die digitale Souveränität von Zivilgesellschaft, Wirtschaft, Wissenschaft und Staat gesehen [80]. Sie alle können demnach ihre Rolle in der digitalen Welt nur dann selbstständig, selbstbestimmt und sicher ausüben, wenn sie sich auf sichere Technologien und entsprechende Fähigkeiten für den sicheren Umgang mit Technologie stützen können.

Digitale Infrastrukturen laden aber zu Sabotage ein und werden von Hackern mit Profitabsichten, zum Teil auch von staatsnahen Hackerkollektiven mit politischen Absichten angegriffen. Cyberangriffe häufen sich - gerade auf staatliche Einrichtungen und auf kleine und mittlere Unternehmen, die oft weniger wehrhaft sind als Großunternehmen. Die Bedrohungslage wird seitens deutscher Behörden als *„so hoch wie nie zuvor“* eingeschätzt, wobei der Schwerpunkt aktueller Angriffswellen auf Ransomware Attacken liegt [81]. Ein Ransomware-Angriff ist eine Art digitale Erpressung. Angreifer nutzen dabei Sicherheitslücken gezielt aus, um in Systeme einzudringen und sie zu verschlüsseln. Der oft einzige Weg, die Daten wiederzuerlangen ist, ein Lösegeld zu zahlen. Ransomware-Angriffe zielen auch immer wieder auf kritische staatliche Infrastrukturen ab, wie beispielsweise Gesundheitssysteme oder auch Versorgungsinfrastruktur (zum Beispiel die Colonial Pipelines).

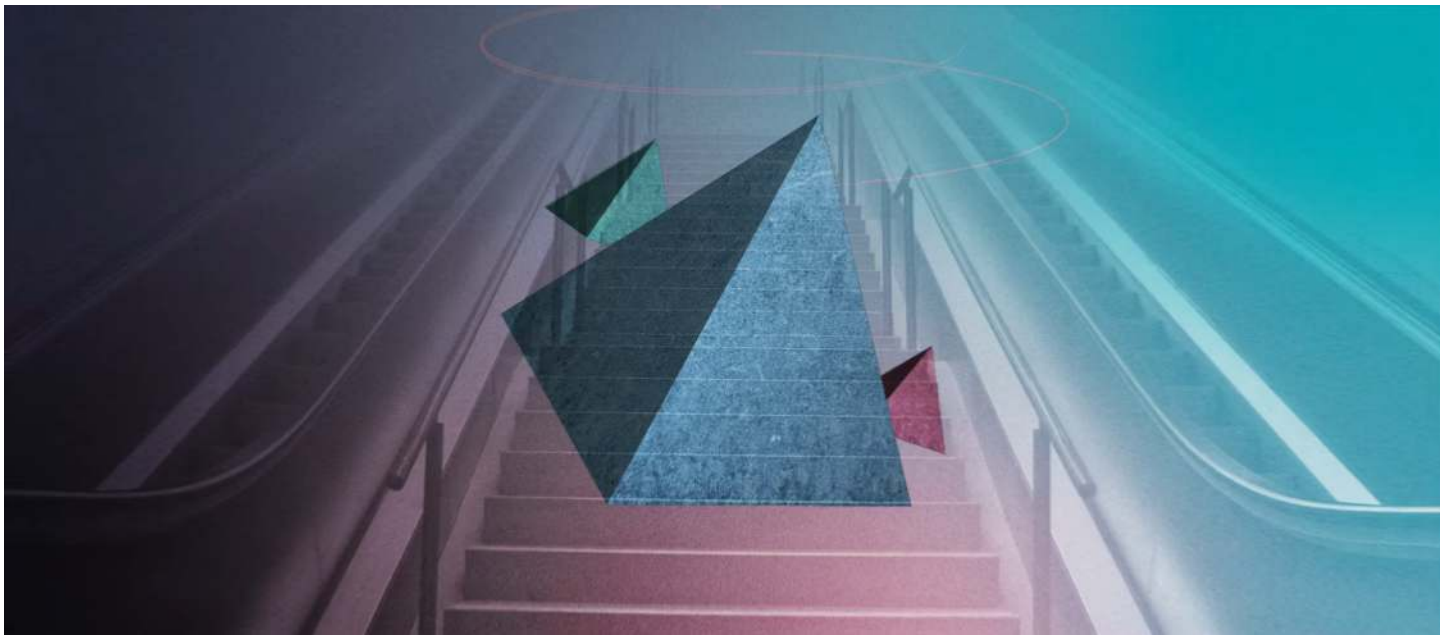
Globale Cyberangriffe in Echtzeit

Quelle: Kaspersky, 2024

Quelle öffnen ↗

Neben Cyberangriffen wird auch die Gefahr hybrider Bedrohungen im Diskurs um digitale Souveränität immer wieder thematisiert. Dabei handelt es sich um die gezielte Verbreitung von Desinformation und Propaganda, die zur Unterwanderung von demokratischen Prozessen und zu Unruhen führen können. In einer Studie erläuterte die EU-Kommission die akute Gefahr, die von Desinformation und gezielt gestreuter Propaganda ausgeht: Hybride Bedrohungen gefährden „*Menschenrechte, Rechtsstaatlichkeit, demokratische Prozesse, nationale Souveränität und geopolitische Stabilität* [82]“. Die digitale Einflussnahme durch Desinformation führt demnach zu einem wachsenden Mobilisierungspotential europäischer Bürger:innen, gerade in dafür empfänglichen Milieus wie unter Rechtsextremen, Verschwörungsgläubigen und Personen, die den Staat delegitimieren.

Die EU sieht es als Teilaspekt digitaler Souveränität, dass EU Bürger:innen im digitalen Raum frei von absichtsvoller äußerer Einflussnahme sind und selbstbestimmt Entscheidungen treffen können [83]. Diesem Aspekt sind wir in etwas anderer Form auch schon im Kontext der Datenökonomie begegnet (siehe Kapitel 2.3.), denn ob nun Konzerne mit Profitinteresse das Kaufverhalten manipulieren oder ausländische Akteure Desinformation verbreiten um für öffentliche Unruhe zu sorgen – in beiden Fällen werden digitale Strukturen verwendet, um gezielt Einfluss auf die (individuelle oder öffentliche) Meinung und das (individuelle oder kollektive) Verhalten auszuüben. Digitale Souveränität kann hier als Fähigkeit interpretiert werden, im digitalen Raum frei von äußerer Einflussnahme selbstbestimmte Entscheidungen treffen zu können [83].



WEGE IN DIE SELBSTBESTIMMTE ZUKUNFT. WIE WERDEN WIR DIGITAL SOUVERÄN?

Die politischen Diskussionen in der EU drehen sich um verschiedene Politikbereiche, die als Bausteine gesehen werden können, um die digitale Souveränität zu stärken [84]. Im Folgenden gehen wir die Handlungsoptionen verschiedener Akteure durch. Die Zivilgesellschaft, die Wirtschaft, die Wissenschaft und die öffentliche Verwaltung besitzen selbst Möglichkeiten, ihre Handlungs- und Gestaltungsrahmen zu erweitern. Zusätzlich kann der Gesetzgeber sie dabei gezielt mit politischen Maßnahmen unterstützen. Der EU kommt dabei die wichtige Rolle zu, die teilweise in Konflikt stehenden Interessen aller Akteursgruppen im Blick zu haben und miteinander abzuwägen. Aber welche Prioritäten setzt die EU in ihrer Digitalpolitik und woran orientiert sie sich dabei?

3.1 Gesetzgebung als wertorientiertes Gestaltungsinstrument

Die Digitalisierung sollte im besten Fall den Bedürfnissen der Gesellschaft über alle Akteursgruppen hinweg gerecht werden [85]. Strategisch versucht die EU deshalb, sich in ihrer Digitalpolitik an „europäischen Werten“ zu orientieren und technologische und regulatorische Strukturen zu schaffen, die diesen Werten auch gerecht werden. Margrethe Vestager, die schon als EU-Kommissarin für Handel zahlreiche Verfahren gegen US-Tech-Konzerne einleitete, betont hier die Ziele der europäischen Digitalstrategie [86].

Dabei werden drei Dinge deutlich. Erstens ist die Wettbewerbsfähigkeit der EU ein wichtiges Anliegen und sie verfolgt mit Ihrer Digitalpolitik auch ganz klar eigene ökonomische Interessen. Zweitens nennt Vestager die Sicherheit und die Grundrechte der EU-Bürger als Leitwerte der europäischen digitalen Agenda, betont aber auch, dass Regulierungen nur eingesetzt werden, wo diese Werte bedroht werden. Dies kann man als Abgrenzung

von den Souveränitätsambitionen autoritärer Staaten verstehen, die häufig versuchen, eine stärkere Kontrolle der eigenen Gesellschaft im digitalen Raum durchzusetzen (siehe Kapitel 2.5).

> „Indem wir die Standards setzen, können wir den Weg zu ethischen Technologien weltweit ebnen und sicherstellen, dass die EU auf diesem Weg wettbewerbsfähig bleibt. Unsere [...] Vorschriften werden dort eingreifen, wo [...] die Sicherheit und die Grundrechte der EU-Bürger auf dem Spiel stehen."
>
> Margrethe Vestager, Vizepräsidentin und Kommissarin für Digitales in der EU-Kommission, 2021

Dabei werden drei Dinge deutlich. Erstens ist die Wettbewerbsfähigkeit der EU ein wichtiges Anliegen und sie verfolgt mit Ihrer Digitalpolitik auch ganz klar eigene ökonomische Interessen. Zweitens nennt Vestager die Sicherheit und die Grundrechte der EU-Bürger als Leitwerte der europäischen digitalen Agenda, betont aber auch, dass Regulierungen nur eingesetzt werden, wo diese Werte bedroht werden. Dies kann man als Abgrenzung von den Souveränitätsambitionen autoritärer Staaten verstehen, die häufig versuchen, eine stärkere Kontrolle der eigenen Gesellschaft im digitalen Raum durchzusetzen (siehe Kapitel 2.5).

Drittens spricht Frau Vestager an, dass europäische Standards weltweite Auswirkungen haben. Sie deutet damit auf den „*Brussel's Effect*" hin. Angesichts der beträchtlichen Größe und Attraktivität des europäischen Marktes haben Regulierungsmaßnahmen der EU häufig einen starken Effekt auf Unternehmen und Regierungen außerhalb der EU. Diese haben einen Anreiz, den europäischen Regulierungsansätzen zu folgen, wenn sie in der EU Geschäfte machen wollen. Es wird durchaus auch argumentiert, dass die EU in ihrer Rolle als „*globaler, regulatorischer Hegemon* [87]" in die Souveränität anderer Länder eingreift.

Simon Schrör

Leiter der Forschungsgruppe „Normsetzung und Entscheidungsverfahren" am Weizenbaum-Institut

„Unter dem Brussels Effect versteht man, dass die EU über den europäischen Binnenmarkt hinaus ökonomische Anreize zur Übernahme ihrer Regulierungsansätze schafft. Sie wird praktisch zum *Regulierungsexporteur* und kann indirekt Kontrolle über Unternehmen und die Gesetze anderer Regierungen ausüben. Kritisch gewendet kann der Brussels Effekt somit aber auch für mittelbare Eingriffe in die Souveränität anderer, meist kleinerer Staaten stehen." (2024)

Go to Profile ↗

Doch welche Steuerungsoptionen nutzen die EU und die deutsche Bundesregierung tatsächlich, um die digitale Souveränität zu stärken? Welche Hebel haben Zivilgesellschaft, Organisationen und Institutionen selbst in der Hand, um ihre jeweiligen Handlungsspielräume zu erweitern? Wir beginnen mit einigen Grundvoraussetzungen digitaler Souveränität, die über alle Akteure und Technologieebenen hinweg systemisch relevant sind: Eine hinreichende Bildung und Teilhabe der Zivilgesellschaft, umfassende Cybersicherheit und die Entwicklung von Schlüsseltechnologien. Die wichtigsten Handlungsoptionen betrachten wir im Anschluss entlang der drei Technologieebenen – Daten Ebene, Code Ebene und physische Ebene.

3.2 Rahmenbedingungen digitaler Souveränität

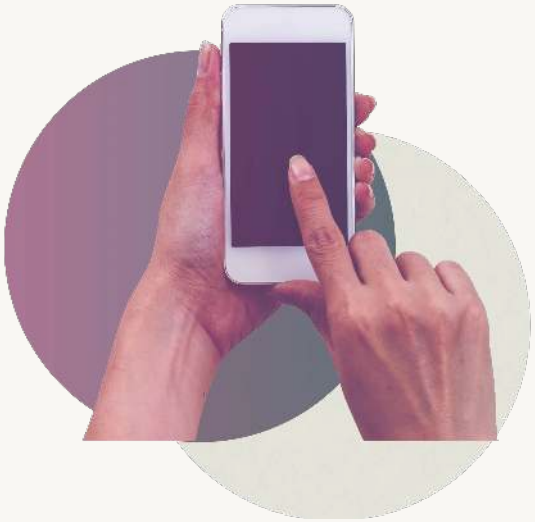
Digitale Souveränität kann nur auf einer souveränen Zivilgesellschaft aufbauen. *„Nur digital befähigte und kompetente Bürgerinnen und Bürger [...] können ihr Schicksal selbst in die Hand nehmen und mit Zuversicht und Selbstbewusstsein auf ihre Mittel, Werte und Entscheidungen blicken“* das unterstreicht auch die EU-Kommission [88]. Was in der wissenschaftlichen Literatur häufig „individuelle digitale Souveränität“ genannt wird, umfasst Digitalkompetenz und Partizipation. Digitale Bildung und Kompetenzen befähigen die Zivilgesellschaft, *„im digitalen Raum bewusste, absichtsvolle und unabhängige Entscheidungen treffen zu können* [65]“, während sie durch Möglichkeiten der Teilhabe ermächtigt wird, sich an Diskursen und Entscheidungen, aber auch unmittelbar an der Gestaltung von Technologie zu beteiligen [16].

Individuelle Selbstbestimmung durch Digitalkompetenz

Beginnen wir mit der Frage, welche Kompetenzen man den eigentlich braucht, um absichtsvolle und unabhängige Entscheidungen im digitalen Raum treffen zu können und damit ein Stück weit digital souverän zu werden. Digitalkompetenz umfasst Wissen und Fertigkeiten auf allen Technologieebenen.

Techniknutzungskompetenz

Zunächst einmal gilt es, Technik überhaupt benutzen zu können. Eine digital kompetente Person wird also diverse IT-Komponenten – Endgeräte, wichtige Anwendungen und Internetdienste – handhaben können und wissen, wie und wofür man sie einsetzt [42][89]. Sie wird ebenfalls genug Vorwissen zu besitzen, um „über die Herausgabe, Erfassung, Speicherung, Nutzung und Verarbeitung eigener Daten umfassend und qualifiziert entscheiden“ zu können [42].

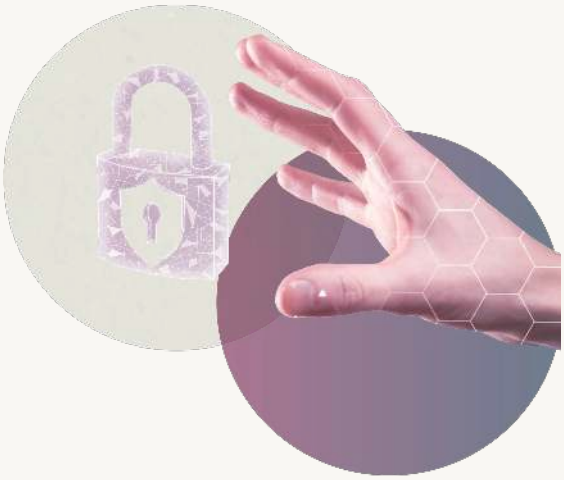


Mediennutzungskompetenz

Kann man Technik einmal bedienen, so wird darüber hinaus erforderlich, auch die Medien, auf die man im digitalen Raum zugreift, nutzen und einschätzen zu können. Das bedeutet zum Beispiel, dass man effektiv nach Informationen suchen kann [89][42] oder dass man die Qualität und Glaubwürdigkeit von Informationen und Kommunikationspartnern einschätzen kann und diese kritisch hinterfragt [90][16][42].

IT Sicherheit

Zu den essentiellen Kompetenzen digital souveräner Personen wird regelmäßig auch die Fähigkeit gezählt, Sicherheitsrisiken minimieren zu können [80] – nicht zuletzt, weil effektiver Selbstschutz immer auch andere Nutzende schützt [42]. Das beinhaltet zum Beispiel, in der Lage zu sein, sich effektiv vor Datenverlust, Identitätsdiebstahl, Malware und Phishing schützen zu können.



Rechtssicherheit

Nicht selten wird als Teil der Digitalkompetenz auch eine zumindest grundlegend vorhandene Rechtssicherheit genannt [42]. Dazu gehört, dass man seine eigenen Rechte (z.B. in Bezug auf Datenschutz) kennt, und fähig ist, sie einzufordern. Rechtssicherheit bedeutet aber auch, die Rechte anderer im digitalen Raum zu kennen und sich entsprechend rechtskonform verhalten zu können. Hier werden insbesondere Urheberrecht und Strafrecht (etwa in Bezug auf digitales Mobbing, Verleumdung und Stalking) genannt [42].

Folgenabschätzung

Digitalkompetenz umfasst auch das Wissen über mögliche Folgen der Nutzung für sich selbst und für andere. Das können zum Beispiel Kenntnisse über gesundheitliche Folgen der IT-Nutzung sein – etwa Schlafmangel oder Konzentrationsstörungen [42] – oder auch ein tiefergehendes Verständnis der gesellschaftlichen, wirtschaftlichen und staatlichen Interessen im digitalen Raum [6].

Die EU-Kommission zählt digitale Bildung und Kompetenzentwicklung zu den obersten Zielen der europäischen Digitalpolitik bis 2030 [89]. Sie ist die Grundlage dafür, dass die Zivilbevölkerung sich kritisch und bewusst mit Technologien auseinandersetzen und den Einfluss der digitalen Transformation auf Gesellschaft und Umwelt einschätzen kann [90]. Ein Mangel an digitalen Kompetenzen kann für Personen mit sozialer Ausgrenzung und erheblichen Nachteilen in der Gesellschaft, auf dem Arbeitsmarkt und im Ausbildungssystem einhergehen [91]. Im Umkehrschluss sind Unternehmen und die öffentliche Verwaltung auf digital kompetente Arbeitskräfte angewiesen, um langfristig wettbewerbsfähig zu sein, was verdeutlicht, wie wichtig die Kompetenzentwicklung in der Zivilgesellschaft auch für andere Akteursgruppen ist.

Staatliche Bildungsangebote bilden das Rahmenwerk für Kompetenzerwerb auf individueller Ebene und können helfen die Kompetenzentwicklung den zukünftigen Bedürfnissen (zum Beispiel des Arbeitsmarktes) anzupassen [16]. Das Bundesministerium für Bildung und Forschung (BMBF) startete deshalb 2021 eine digitale „Bildungsoffensive“. Diese sieht unter anderem vor, Schulen besser technisch auszustatten, digitale Lernwerkzeuge zu entwickeln und pädagogische Fachkräfte zu qualifizieren. Für den Bereich Aus- und Weiterbildung werden digitale Weiterbildungsmaßnahmen entwickelt und frei verfügbare Bildungsmaterialien verbreitet [92]. Im Bundesministerium für Familie, Soziales, Frauen und Jugend (BMFSFJ) steht auch die Teilhabe und Autonomie älterer Menschen im Fokus, entwickelt werden hier zum Beispiel niedrigschwellige, altersspezifische Bildungsangebote für Senior:innen [17]. Das Bundesministerium des Innern und für Heimat rief 2023 den Digitalführerschein ins Leben: Ein umfangreiches Bildungsangebot, verbunden mit der Möglichkeit, die eigenen Digitalkompetenzen in verschiedenen Schwierigkeitsgraden zu testen und sich bei erfolgreicher Prüfung ein Zertifikat ausstellen zu lassen [93].

Demokratische Selbstbestimmung durch Partizipation und Teilhabe

Digitalkompetenzen helfen dabei, sich individuell selbstbestimmt im digitalen Raum bewegen zu können. Sie sind aber auch eine hilfreiche, wenn nicht sogar notwendige Voraussetzung dafür, sich aktiv in politische und technische Gestaltungsprozesse der digitalen Welt einbringen zu können [16]. Partizipation bedeutet, demokratisch selbstbestimmt zu werden, also politische Entscheidungen im Interesse der Gesellschaft zu beeinflussen und Technologien mitzugestalten. Die demokratische Handlungsfähigkeit der Zivilgesellschaft im digitalen Raum kann durch den Staat aktiv gefördert werden.

Dr. Bianca Herlo

Leiterin der Forschungsgruppe „Design, Diversität und New Commons“ am Weizenbaum-Institut

„Menschen müssen zu *individueller und demokratischer Selbstbestimmung* ermächtigt werden. Mit Digitalkompetenz können sie Kulturen, Praktiken und Visionen positiv beeinflussen, denen sie in Organisationen, Regierungen und in der Zivilgesellschaft begegnen, und so zu mehr digitaler Souveränität beitragen.“ (2023)

Go to Profile ↗

Dafür ist es zunächst erforderlich, dass Transparenz über wichtige politische und wirtschaftliche Entscheidungsprozesse herrscht, etwa in der Regulierung oder Entwicklung technischer Standards. Nur so können Bürger diese Prozesse nachvollziehen und sich einbringen. Repräsentant:innen der Zivilgesellschaft

können (und sollten) diese Normungsprozesse aktiv begleiten [94][95], oder sogar bereits in die Entwicklung staatlicher Strategien – etwa zum Aufbau digitaler Souveränität – einbezogen werden [85]. Dies sind zielführende Ansätze, damit Gemeinwohlinteressen frühzeitig und wirksam vertreten werden.

Der Staat kann die demokratische Beteiligung der Zivilgesellschaft aktiv fördern [19], indem er Ausschusssitzungen öffentlich abhält, Abläufe vorab kommuniziert, ausreichende Fristen festlegt und Bürger:innen einlädt, sich in Beratungsgremien oder in die Ausarbeitung von Gesetzesvorschlägen einzubringen. Beteiligungsformate können auch digital und niedrigschwellig gestaltet werden – zahlreiche zivilgesellschaftliche NGOs fordern zum Beispiel die Einrichtung einer zentralen Veröffentlichungs- und Beteiligungsplattform [96].

Umfassende Cybersicherheit

Als zweite Rahmenbedingung der digitalen Souveränität wird mit Nachdruck auf die Sicherheit und Resilienz digitaler Infrastrukturen hingewiesen [15][97]. Cybersicherheit gilt als Grundvoraussetzung für das gesellschaftliche Leben, wirtschaftliche Abläufe und den Schutz kritischer Infrastrukturen [99]. Strategien und Maßnahmen zur Erhöhung der IT-Sicherheit werden angesichts einer hohen Bedrohungslage auf europäischer und auf Bundesebene formuliert. Ende 2020 stellte die EU-Kommission die neue Cybersicherheitsstrategie der EU vor [100]. Zentral hierin ist der Plan, Cyberbedrohungen länderübergreifend, koordiniert, und in enger Zusammenarbeit zu begegnen. Die Maßnahmenpakete sollen ein EU-weit einheitlich hohes Niveau an Sicherheit und Resilienz digitaler Infrastrukturen durchsetzen. Neben spezifischen Vorgaben an nationale Cybersicherheitsstrategien und behördliche Strukturen werden auf EU-Ebene Kooperationsgruppen eingerichtet, die im engen Austausch stehen und in Sachen Cybersicherheit die strategische Zusammenarbeit in Europa unterstützen. Nationale Ansprechpartner und Notfallteams sind bei Sicherheitsvorfällen verantwortlich für den Austausch zwischen EU-Ländern und fungieren als eindeutige Kontaktpersonen. Im Falle akuter Krisensituationen sollen sie operative Einsätze schnell, effektiv und grenzüberschreitend abstimmen können.

Die Europäische Cybersicherheitsgesetzgebung NIS wurde 2023 nach nur 6 Jahren umfassend aktualisiert, um mit der schnelllebigen Bedrohungslandschaft Schritt zu halten.

Quelle: Europäische Union, 2013

Quelle öffnen ↗

Parallel gelten bessere Verschlüsselungssysteme und stärkere Überwachungsabwehr [101] sowie der verstärkte Einsatz von Open-Source Software (siehe Kapitel 3.4) als technische Wege, die Cybersicherheit zu verbessern. Die Einführung vertrauenswürdiger Sicherheitszertifikate könnte zu mehr Transparenz und einem erhöhten Sicherheitsbewusstsein auf Anwenderseite verhelfen [99][102]. Die gezielte staatliche Förderung von Forschung und Entwicklung im Bereich Cybersicherheit ist eine wirksame Handlungsoption, um die IT-Sicherheit langfristig zu stärken und auch hier Abhängigkeiten zu reduzieren [103].

Schlüsseltechnologien in Forschung und Entwicklung

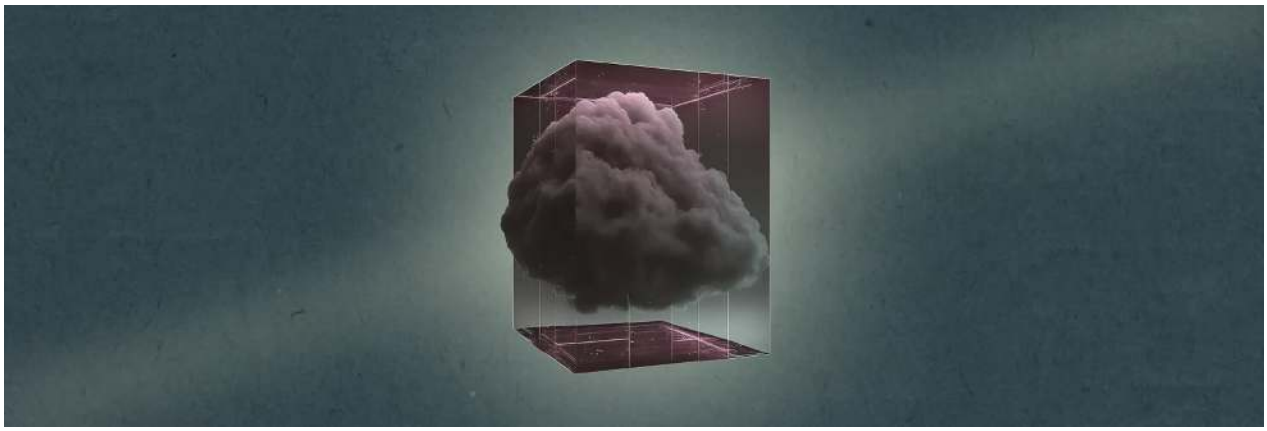
Die langfristige und vorausschauende staatliche Förderung der Forschung und Entwicklung ist nicht nur im Bereich Cybersicherheit relevant. Vielmehr kann man die Förderung von Schlüsseltechnologien als weitere Rahmenbedingung digitaler Souveränität verstehen, die über alle Akteursgruppen und Technologieebenen von Bedeutung ist. Die EU sieht Schlüsseltechnologien als Stützpfeiler der zukünftigen ökonomischen Wertschöpfung an. Viele Maßnahmen der EU zielen deshalb darauf ab, die heimische Forschungs- und Unternehmenslandschaft in der Entwicklung von künstlicher Intelligenz, Quantentechnologien, Cloud-Technologien und natürlich in Halbleitertechnologien gut aufzustellen [97]. Dies einerseits, um mittelfristig wirtschaftliche Abhängigkeiten zu verringern, und die heimische Industrie zu stärken, andererseits auch, um Technologien im Einklang mit eigenen Wertvorstellungen zu gestalten [65]. Konkrete Maßnahmen der letzten Jahre zielten neben direkter finanzieller Förderung auch häufig darauf ab, die Wettbewerbsbedingungen europäischer Anbieter zu verbessern und Markteintrittsbarrieren zu senken [65], zum Beispiel indem Start-up-Ökosysteme gezielt gefördert werden [97]. Parallel können Forschungs- und Entwicklungspartnerschaften sowohl zwischen EU-Mitgliedsländern als auch zwischen Privatunternehmen und Staaten strategisch ausgebaut werden [65].

Massive Förderprogramme sollen Deutschlands Zugang zu Schlüsseltechnologien sichern.

Quelle: Forschungsprogramm Quantensysteme, BMBF 2022

Quelle öffnen ↗

3.3 Digitale Souveränität auf Daten Ebene



Die EU hat in den vergangenen Jahren eine Vielzahl erfolgreicher datenpolitischer Maßnahmen entwickelt. Auf der Datenebene erkennt man deutlich, dass Gesetzgeber bestrebt sind, gegensätzliche Interessen verschiedener Akteursgruppen miteinander in Einklang zu bringen. Einerseits müssen die Daten europäischer Bürger:innen, Unternehmen und Institutionen angemessen geschützt und datenschutzrechtliche Verletzungen geahndet werden. Andererseits sollten sich auch innerhalb der EU innovative datenbasierte Geschäftsmodelle entwickeln können, die mit gesellschaftlichem und wirtschaftlichem Nutzen verbunden sind.

Datenschutz

Beginnen wir mit den Interessen und Rechten der Zivilgesellschaft auf der Datenebene. Als Meilenstein im Datenschutzrecht gilt sicherlich die Datenschutzgrundverordnung (DSGVO), die, seit sie 2018 in Kraft trat, den Schutz personenbezogener Daten von EU-Bürger:innen maßgeblich stärkt und Betroffenen mehr Kontrolle über ihre persönlichen Daten gibt. Sie gilt als eine der strengsten Datenschutznormen weltweit und setzt Standards, die bereits von zahlreichen anderen Ländern übernommen wurden [104]. Dass Nutzende damit die Möglichkeit haben, Daten, die sie selbst generieren, auch zu kontrollieren, gilt als wichtiges Merkmal für ihre digitale Souveränität [84]. Das starke Datenschutzrecht schränkt die Befugnisse datenverarbeitender Unternehmen ein und erhöht das Informationsrecht der Verbraucher mit dem Ziel, vorhandene Informationsasymmetrien (siehe Kapitel 2.3.) abzubauen. Die DSGVO sichert Nutzenden auch die Möglichkeit, ihre personenbezogenen Daten in andere Anwendungen zu übertragen, was wiederum Wechselbarrieren und Abhängigkeiten von einzelnen Anbietern reduziert.

Datenökonomie

In anderen Regulierungsansätzen der EU ist dagegen eine eher privatwirtschaftlich-wachstumsorientierte Datenpolitik zu erkennen. Die EU verfolgt das strategische Ziel, einen funktionierenden europäischen Binnenmarkt für Daten zu entwickeln, der gleichzeitig ein hohes Datenschutzniveau sichert [105]. Sie setzt diesen Plan im Kern mit dem Data Governance Act (DGA) von 2022 und den Data Act von 2024 um. Der DGA soll datenbasierte Kooperationen zwischen Wirtschaft, Wissenschaft, Behörden und Bürgern vereinfachen. Dafür werden unabhängige Vermittlungsdienste und Marktplätze geschaffen, auf denen Anbieter und Abnehmer von Daten in Zukunft zusammenkommen. Daten können so zwischen einzelnen Sektoren einfacher und transparenter geteilt werden. Außerdem soll der DGA zur freiwilligen Datenfreigabe anregen: Er erleichtert Datenspenden und sorgt dafür, dass Zugang und Weiterverwendung von gespendeten Daten eindeutig und transparent geregelt werden. Der Data Act sieht vor, dass Nutzende Zugang zu sämtlichen Daten erhalten, die durch ihre IoT Geräte generiert werden und dass diese auf Wunsch der Nutzenden hin auch dritten

Unternehmen zur Verfügung gestellt werden müssen. Bestenfalls führt dies dazu, dass auch europäische Unternehmen auf größere Datenmengen zugreifen können, aus denen sie Wert schöpfen können [106].

Margrethe Vestager sieht den Data Governance Act als ein alternatives Modell zu den Datenverarbeitungspraktiken großer Tech-Plattformen.

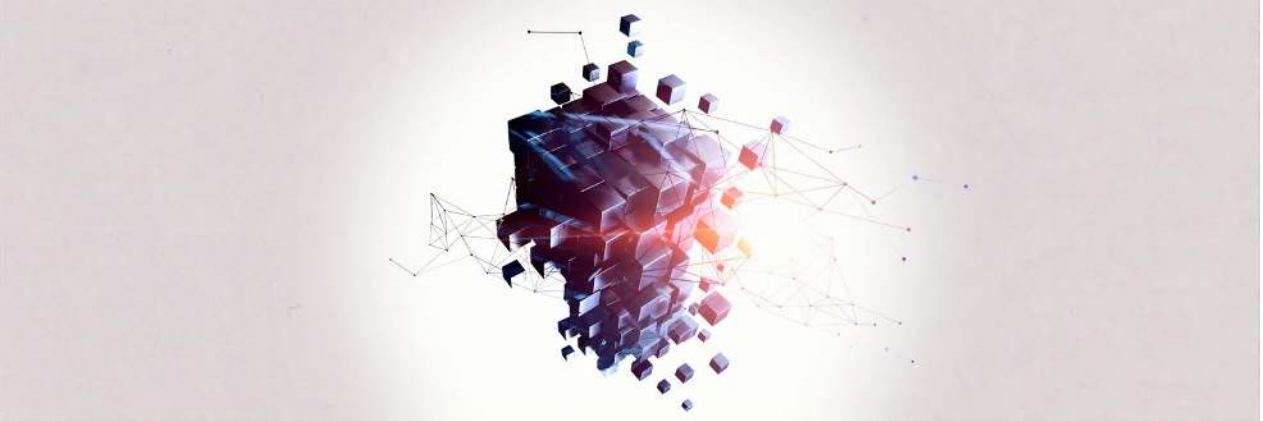
Quelle: Europäische Union, 2020

Quelle öffnen ↗

Datenräume

Die deutsche und französische Regierung initiierten 2019 das Kooperationsprojekt „Gaia-X“ mit dem Ziel, ein gemeinsames, europäisches Daten-Ökosystem zu schaffen [107]. Viele bislang voneinander getrennte Datenräume sollen miteinander verknüpft werden. Dabei gilt es, Regeln und Standards für den kooperativen Austausch und die rechtskonforme Nutzung von Daten zu formulieren und die technischen Anforderungen an diesen neuen Datenraum zu formulieren. Big Tech-Plattformen hätten *„ein hohes Maß an Marktmacht […], da sie große Datenmengen kontrollieren“* [108]. Die europäische Datenstrategie soll dem etwas entgegenstellen und basierend auf „souveränem Datenaustausch“ die eigene Wettbewerbsfähigkeit stärken [73]. Gaia-X begann also mit dem Ziel, die Datenhegemonie der US-amerikanischen und chinesischen Großkonzerne aufzubrechen. Mittlerweile sind allerdings auch genau diese Großkonzerne – Microsoft, Alibaba, Amazon, Google und Palantir – als Partner und Mitglieder in die technischen Arbeitsgruppen des Projekts eingebunden [109]. Als Anbieter von Clouddiensten sollen sie nicht nur an die zu schaffenden Datenräume angebunden werden, sondern auch ihre Expertise in die Entwicklung dieser Infrastrukturen einbringen. Zuletzt standen sie allerdings dafür in der Kritik, die Arbeitsprozesse des Projekts gezielt auszubremsen [110].

3.4 Digitale Souveränität auf Code Ebene



Open Source Software

Auf der Ebene von Software und Anwendungen wird vielfach betont, wie sinnvoll der stärkere Einsatz von quelloffener Software für die digitale Souveränität ist. Konkret betont das Bundesministerium des Innern und für Heimat, dass die verstärkte Nutzung von Open Source Software drei strategische Ziele erfüllt [111], die aber nicht nur für die öffentliche Verwaltung sondern auch für andere gesellschaftliche Teilbereiche gelten. Den Einsatz von Open Source Software kann man also für alle Akteursgruppen als möglichen Hebel betrachten, ihre Handlungsspielräume zu vergrößern.

Quelloffene Software eröffnet **Wechselmöglichkeiten** – einerseits, weil sie stärker modular aufgebaut ist (so können leicht einzelne Komponenten ausgetauscht werden) andererseits, weil sie interoperabler ist als proprietäre Software (durch offene Schnittstellen lassen sich eine größere Vielfalt an Softwarekomponenten miteinander verknüpfen). Die so entstehende Flexibilität reduziert die Abhängigkeit von einzelnen Anbietern. Open Source Software garantiert **Gestaltungsfähigkeit**. Da der zugrundeliegende Code einsehbar und veränderbar ist, kann er besser den eigenen Bedürfnissen angepasst werden und stärkt das Potential für Kooperationen und kreative Zusammenarbeit. Wurden die Möglichkeiten, Quellcode einzusehen und mitzugestalten von Anbietern proprietärer Software zunehmend eingeschränkt, so kann Open Source Software diese wieder öffnen. Für Anwender:innen – und dazu gehören auch Unternehmen und öffentliche Einrichtungen – werden kreative Freiräume und Innovationspotentiale geschaffen. Der Einsatz von Open Source Software erhöht letztlich auch die **Verhandlungsposition** gegenüber den Anbietern proprietärer Software, weil es leistungsfähige Alternativen zu ihren Produkten gibt [111], die aufgrund ihrer Einsehbarkeit als vertrauenswürdiger und sicherer gelten [9].

Plattformregulierung

Die EU versucht, durch die Stärkung individueller digitaler Rechte mehr digitale Souveränität herzustellen und eine stärkere Kontrolle über Technologieunternehmen, insbesondere Plattformkonzerne auszuüben. Auf das empfundene Fehlverhalten der Plattformunternehmen in den vergangenen Jahren (insbesondere in Bezug auf Datenschutz, Desinformation und Monopolisierungstendenzen) reagierte die EU mit zwei groß angelegten neuen Verordnungen

Digital Services Act

Mit dem Digital Services (DSA) sollen die Grundre von Nutzenden im digita Raum besser geschützt werden. Es gilt, „illegale c

Digital Markets Act

Der Digital Markets Act (DMA) soll die Wettbewerbsbedingungen zwischen besonders mächtigen Unternehmen („Gatekeepern“)

schädliche Online-Aktivi
sowie die Verbreitung vo
Desinformation zu verhi
[112], wobei für sehr groß
Plattformen und
Suchmaschinen auch
besonders strenge Regel
formuliert worden sind.

und anderen
Marktteilnehmern angleichen
[113]. Gatekeeper dürfen ihre
eigenen Produkte nicht mehr
bevorzugen oder
konkurrierende Produkte und
Anbieter benachteiligen. Auch
Apps von Gatekeepern wie
Apple oder Google muss man
grundsätzlich vom
Smartphone deinstallieren
können.

Das Regulierungspaket aus DSA und DMA adressiert damit mehrere Herausforderungen, die im Zusammenhang der Diskussion um digitale Souveränität problematisiert werden. Digitale Souveränität erfordert für die Zivilgesellschaft eine effektive Regulierung von Desinformation, Hassrede und Verleumdung [95], um sicherzustellen, dass geltende Grundrechte auch im digitalen Raum durchgesetzt werden. Einzelanwender:innen erhalten durch die strengere Transparenzanforderungen mehr Entscheidungsbefugnisse darüber, ob sie personalisierte Empfehlungen und Inhalte angezeigt bekommen wollen. Gezielte Werbung für Minderjährige wird ganz verboten. Dies soll die Informations- und Machtasymmetrien zwischen Plattformen und Anwender:innen abbauen und – wie auch die Minimierung von Risiken durch die regulierten Inhalte – die autonome Handlungs- und Entscheidungsfähigkeit stärken.

Der DMA stärkt auch die digitale Souveränität der Wirtschaft, weil unfaire Marktbedingungen und unlautere Geschäftspraktiken von Seiten der Marktführer effektiv begrenzt werden. So werden die Möglichkeiten kleinerer und mittlerer Unternehmen gestärkt, sich in der Entwicklung und dem Betrieb digitaler Dienste am Markt durchzusetzen [113].

Rita Gsenger

Doktorandin in der Forschungsgruppe „Normsetzung und Entscheidungsverfahren“ am Weizenbaum-Institut

„Desinformation, rechtswidrige Inhalte, Hassrede und Diskriminierung auf Plattformen können sich auf gesellschaftliche Debatten und demokratische Prozesse auswirken und gefährden das körperliche und geistige Wohlbefinden, gerade von Minderjährigen. Die EU-Kommission tritt diesen Herausforderungen entgegen, indem sie Plattformen und Suchmaschinen in die Pflicht nimmt. Die *Erfolgsaussichten sind jedoch unklar* und werden sich erst in den kommenden Jahren beurteilen lassen.“ (2024)

Go to Profile ↗

3.5 Digitale Souveränität auf der physischen Ebene

Physische Komponenten spielen im Diskurs um digitale Souveränität eine wichtige Rolle. Im Fokus der Politik steht dabei insbesondere der Ausbau der physischen IT-Infrastruktur und die Stärkung der europäischen Forschungs-, Entwicklungs- und Produktionskapazitäten.

Flächendeckender Infrastrukturausbau

Immer wieder wird betont, wie wichtig der flächendeckende Ausbau der technischer Infrastrukturen ist, um der Zivilgesellschaft gleichberechtigten Zugang zum digitalen Raum und damit digitale Souveränität zu ermöglichen [90]. Sei es die mobile Netzabdeckung oder die Verlegung von Glasfaserkabeln: Partizipieren und teilhaben kann nur der Teil der Zivilbevölkerung, der auch barrierefreien Zugang zum digitalen Raum besitzt [114]. Die Verbesserung der Versorgungsabdeckung wird sowohl von der EU als auch von der Bundesregierung gefordert und gezielt unterstützt. Die Gigabitstrategie der Deutschen Bundesregierung sieht zum Beispiel vor, dass bis Ende 2025 die Hälfte aller deutschen Haushalte und Unternehmen Glasfaseranschlüsse besitzen, bis 2026 soll eine „*flächendeckende, unterbrechungsfreie Sprach- und Datenkommunikation*“ auf dem gesamten Bundesgebiet hergestellt werden [115].

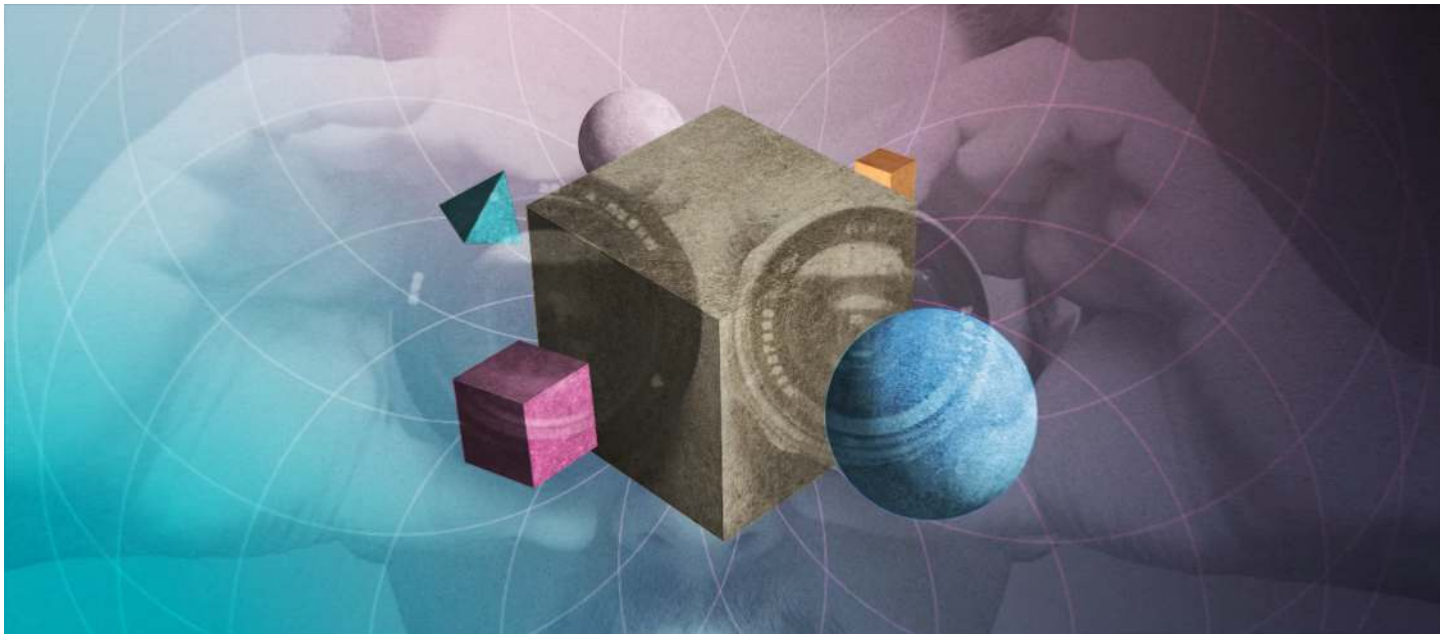
Reduktion von Versorgungsrisiken

Auf der physischen Ebene reduziert die EU wirtschaftliche Abhängigkeiten, indem sie eigene Produktionskapazitäten ausbaut und strategische Partnerschaften in der Beschaffung schließt. Der in EU-Institutionen häufiger verwendete Begriff „strategische Autonomie“ verdeutlicht, dass es im Kern nicht um reinen Protektionismus oder Autarkiebestrebungen geht. Vielmehr sollen zumindest für den Bedarf an essentiellen Hardwarekomponenten Ausfalloptionen und Wahlmöglichkeiten geschaffen werden. Mit dem Europäischen Chip-Gesetz hat die EU einige der umfangreichsten wirtschaftlichen Förderprogramme ihrer Digitalpolitik ins Leben gerufen. Das Gesetz sieht Investitionen in Forschung und Entwicklung aber auch in Produktionsstätten der EU vor [116]. Es stärkt damit die Wettbewerbsfähigkeit europäischer Anbieter in diesem Markt und stellt sicher, das wirtschaftliche Abhängigkeiten abgebaut werden [9].

EU-Kommissar für Binnenmarkt und Industriepolitik Thierry Breton kündigt 2022 massive Investitionen in die europäische Halbleiterindustrie an.

Quelle: Europäische Union, 2022

Quelle öffnen ↗



AUSBLICK

Monopolstrukturen, Überwachung, Lieferengpässe, Cyberangriffe, Desinformation – die Herausforderungen könnten wohl kaum unterschiedlicher sein. Unter dem Dach des Hochwertworts „digitale Souveränität“ finden sie einen gemeinsamen Platz. Sie verbindet, dass in ihnen die Gestaltungsinteressen und Machtansprüche verschiedener gesellschaftlicher Gruppen aufeinandertreffen und politisch ausgehandelt werden müssen. „Digitale Souveränität“ beschreibt im Grunde ein Tauziehen verschiedener Akteure um Hoheitsansprüche, Abhängigkeitsverhältnisse, Entscheidungs- und Gestaltungsspielräume im digitalen Kontext. Mit einem Spektrum von wirtschafts-, sicherheits- und bildungspolitischen Maßnahmen versucht die Politik, die Gestaltungsspielräume verschiedener Akteure gezielt zu stärken oder einzugrenzen. Das politische Abwägen gegenläufiger Interessen wird die zukünftige Gestaltung unserer digitalen Infrastrukturen entscheidend prägen.

Inwieweit einzelne Maßnahmen dann aber wirklich insgesamt zu „mehr digitaler Souveränität“ führen, lässt sich nur schwer beurteilen. Bislang existiert kein Ansatz, der digitale Souveränität in der inhaltlichen Breite wie sie politisch diskutiert wird, messbar macht. So lässt sich natürlich auch nur vage feststellen, ob und wie stark einzelne Maßnahmen die digitale Souveränität beeinflussen. Augenscheinlich wird es empfehlenswert sein, Maßnahmen auf europäischer Ebene zu denken. Besonders, wenn es um Regulierungsvorhaben und Wirtschaftsförderung geht, kann die EU deutlich stärkere Anreize setzen, als eine Regierung im nationalen Alleingang. Zahlreiche Projekte und Verordnungen auf EU-Ebene haben sich bereits als zielführend und erfolgreich erwiesen. Dennoch sind die meisten Gesetzgebungen noch vergleichsweise jung – die Zeit wird zeigen, wie durchsetzbar und effektiv sie letztlich sind. Fest steht, dass die Stärkung der digitalen Souveränität weitsichtige Planung und ein gewisses Maß an Mut und Selbstbewusstsein erfordern wird, an gewachsenen Strukturen zu rütteln und neue Wege einzuschlagen.

Dr. Esther Görnemann

Wissenschaftliche Referentin Forschungssynthesen

Esther Görnemann ist seit 2023 als wissenschaftliche Referentin für Forschungssynthesen am Weizenbaum-Institut beschäftigt. Kern ihrer Arbeit ist es, den Forschungsstand zu zentralen Fragestellungen der digital vernetzten Gesellschaft aufzuarbeiten, um zukünftige Forschung zu informieren und den Wissenstransfer der Forschungsgruppen in Richtung Politik und Öffentlichkeit zu unterstützen.

Go to Profile ↗

Vertiefungstext

Was bedeutet Souveränität? Ein historischer Exkurs

Im Gegensatz zu „digitaler Souveränität“ ist der Begriff der Souveränität schon sehr alt. Seine Interpretation hat sich im Laufe der Jahrhunderte immer wieder gewandelt, um den politischen Gegebenheiten ihrer Zeit Rechnung zu tragen.

Territorialitätsprinzip

Zunächst finden wir den Begriff in den Lehren von Jean Bodin. Der französische Philosoph bezeichnete damit die absolute Autorität des Souveräns (hier: des französischen Königs). Dieser, so postulierte Bodin im späten Mittelalter, besäße also die höchste und letzte Entscheidungsgewalt *über sein Staatsgebiet*. Legitimiert ist der Souverän weder durch eine besondere Ausbildung noch durch Abstimmungen (an freie Wahlen wagte man im 16. Jahrhundert noch nicht zu denken). Bodin zufolge sei ein Souverän keiner höheren Instanz unterworfen, erhalte seinen Machtanspruch auf Lebenszeit und könne diesen weitervererben. *„Das Wesen der souveränen Macht und absoluter Gewalt“*, bestehe vor allem darin, *„den Untertanen in ihrer Gesamtheit ohne ihre Zustimmung das Gesetz vorzuschreiben* [19]“.

Jean Bodin, 16. Jahrhundert

François Stuerhelt, PD, via Wikimedia Commons

Quelle öffnen ↗

Gesellschaftsvertrag

Der englische Philosoph und Mathematiker Thomas Hobbes erlebte Mitte des 17. Jahrhunderts schon als Kind massive politische Unruhen im englischen Bürgerkrieg zwischen König und Parlament. So war es wenig verwunderlich, dass er den Naturzustand der Menschen als „Behemoth“ beschrieb – ein schauerliches Ungeheuer des Alten Testaments. Im Naturzustand, ohne Staat und Gesetz, herrsche unter den Menschen Anarchie und Chaos. Man müsse in Argwohn und in ständiger Furcht vor Enteignung und Tod leben. Hobbes war davon überzeugt, dass es nur ein Mittel gegen diesen Zustand geben könne: Einen „Leviathan“.

Dieses mythologische Seeungeheuer symbolisiert einen souveränen Herrscher, dessen Strafen noch furchteinflößender sind als das Chaos. Aus Angst vor Strafe würde niemand es wagen, die Gesetze zu missachten – Friede und Vertrauen in die Ordnung würden einkehren. Hobbes war damit der Erste, der sich so etwas wie einen Gesellschaftsvertrag vorstellte. Das Volk würde freiwillig auf die anarchische Freiheit verzichten, zu tun und zu lassen was es wolle. Es würde seine Freiheit und Selbstbestimmung an den Souverän abgeben und im Gegenzug dafür die Garantie erhalten, dass der Souverän Recht spricht und Gesetze durchsetzt [20].

Aufklärung und Rechtsstaatlichkeit

Rund ein Jahrhundert später begann in Europa die Zeit der Aufklärung. Ideelle Vorboten der französischen Revolution waren Montesquieu, ein französischer Staatstheoretiker und Jean-Jacques Rousseau, ein Schweizer Gelehrter. Sie ergänzten den Souveränitätsbegriff mit rechtsstaatlichen Aspekten, nicht zuletzt um das Risiko einzudämmen, dass ein Monarch zum willkürlichen Despoten wird. Montesquieu beschrieb 1748 verschiedene Regierungsformen und erklärte dabei die Grundprinzipien der Demokratie. Zu ihnen gehört, dass in einer Demokratie das Volk die souveräne Gewalt besitzt, und zwar, indem es seinen Willen in Wahlen zum Ausdruck bringt [21].

Baron de Montesquieu, 1728

PD-US, via Wikimedia Commons

Quelle öffnen

Rousseau baute auf diesen Gedanken auf. 1762 wagte er es, eine zu dieser Zeit unerhörte These aufzustellen: Die Souveränität habe – unteilbar und unveräußerlich – das Volk inne, nicht der Herrscher (er sprach von *Volkssouveränität*). Allein das Volk stehe über der Verfassung, die es sich selbst gebe und der es sich unterwerfen würde. Im Rahmen eines Gesellschaftsvertrages könne das Volk die Ausübung der Gesetze an einen Herrscher delegieren, es erlasse aber seine Gesetze selbst und bleibe damit souverän [22]. Dieser Grundsatz war seinerzeit die theoretische Rechtfertigung, um Herrscher in Revolutionen gewaltsam zu entmachten und ist bis heute ein fester Bestandteil demokratischer Verfassungen in der ganzen Welt.

Jean-Jacques Rousseau, 1753

PD-US, via Wikimedia Commons

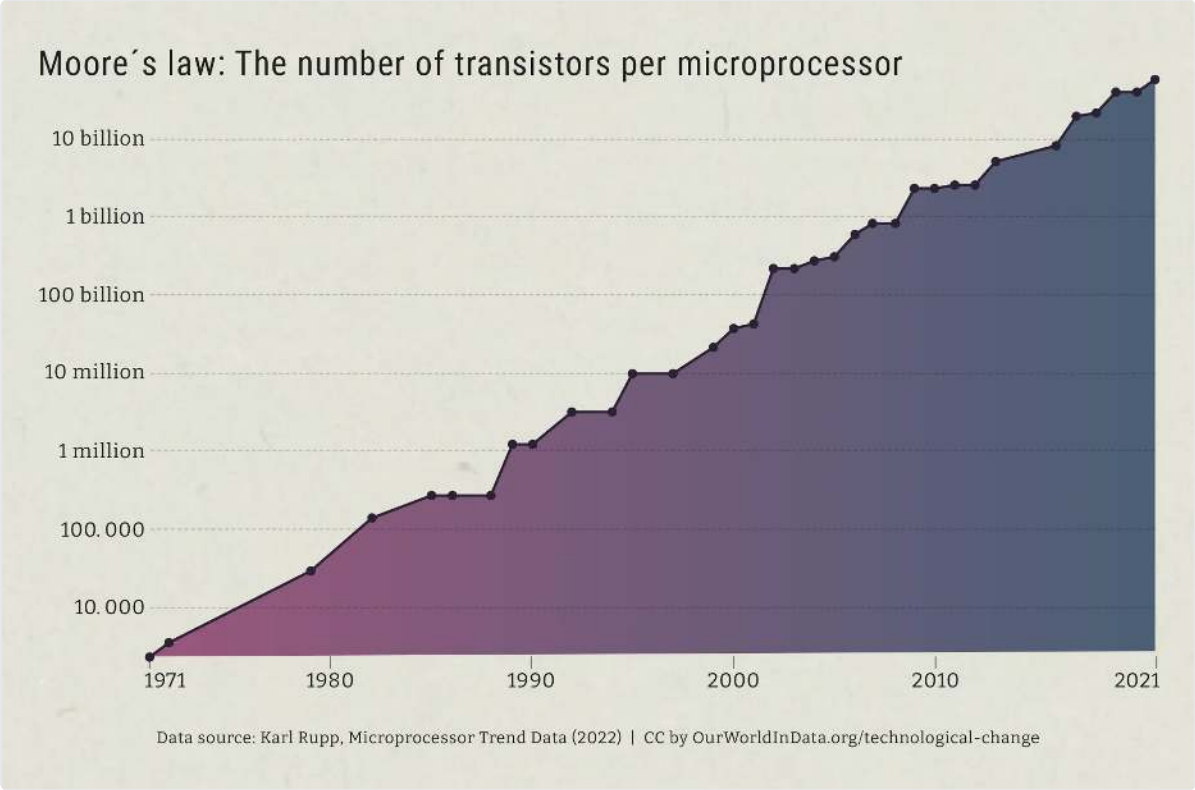
Quelle öffnen

Vertiefungstext

Was sind Mikrochips?

Mikrochips werden auf einer runden Platte aus Halbleitermaterial („Wafer“) aufgebaut, die bis zu 30 Zentimeter Durchmesser haben kann, aber ist nicht dicker ist als ein Millimeter. Das Besondere an Halbleitermaterialien ist, dass man ihre elektrische Leitfähigkeit sehr gezielt steuern kann [75]. Deshalb lassen sich auf einem Wafer elektronische Schaltkreise praktisch „einzeichnen“.

Hierfür bringt man mikroskopisch kleine Schaltkreise an der Oberfläche des Wafers auf, indem man schichtweise winzige Areale des Wafers verätzt, mit UV-Licht belichtet oder mit anderen Materialien beschichtet. Schicht für Schicht entstehen hauchdünne, dreidimensionale Strukturen, durch die Strom geleitet werden kann. Winzige Bereiche in dieser Struktur kann man nun gezielt in den Zustand „leitfähig“ oder „nicht-leitfähig“ versetzen. Diese nennt man Transistoren, und ihr Zustand entspricht im binären System der 1 oder der 0. Schaltet man mehrere Transistoren zusammen, entstehen Schaltkreise, mit denen Daten gespeichert und Befehle verarbeitet werden können.



Moore'sches Gesetz: Die Anzahl der Transistoren auf einem Mikroprozessor verdoppelt sich seit 1970 alle 2 Jahre.

Ein Transistor muss in der Theorie nur einige *Atome* breit sein, um zu funktionieren. Die Herausforderung ist jedoch, solche Größenordnungen technisch umzusetzen. Je mehr Transistoren auf einem Chip untergebracht werden, desto leistungsfähiger und energieeffizienter ist dieser am Ende. Die Chipindustrie hat hier beispiellose Fortschritte verzeichnet. Seit 1970 konnte die Anzahl an Transistoren auf einem Mikrochip alle 2 Jahre verdoppelt werden [76]. Einer der aktuell leistungsfähigsten Chips bringt auf einer Fläche von 1mm² ganze 250 Millionen Transistoren unter. Die kleinsten aufgebrachten Strukturen sind hier nur noch wenige Nanometer breit [77].

Nur noch mit dem Rasterelektronenmikroskop kann man sich ein realistisches Bild von den Größenordnungen der Nanotechnologie machen – hier im Video mit Nahaufnahmen des faszinierenden Innenlebens eines etwa 3mm² großen Microchips [78].

Vertiefungstext

Massenüberwachung und Spionage – was die NSA-Affäre offenbarte

Die politische Brisanz und das schiere Ausmaß der durch Edward Snowden in die Öffentlichkeit gelangten Dokumente ist beispiellos. Es handelte sich um einen Fundus von rund 1,7 Millionen teils streng geheimer Verschlusssachen [44]. Sie lieferten Indizien für eine ganze Reihe geheimdienstlicher Operationen, mit denen der weltweite Datenverkehr systematisch mitgeschnitten, auf Vorrat gespeichert und analysiert wurde.

Wer hat der NSA erlaubt, die ganze Welt abzuhören?

Nach den Terroranschlägen auf das World Trade Center 2001 wurde die Überwachung digitaler Kommunikation durch amerikanische Sicherheitsbehörden massiv ausgebaut. Insbesondere die Geheimdienste CIA und NSA wurden personell aufgestockt und mit nie dagewesenen Budgets ausgestattet. Ihr erklärtes Ziel: Terroristische Netzwerke und verdächtige Personen identifizieren und beobachten [45]. Nur wenige Wochen nach den Anschlägen erließ die Regierung George W. Bush den „Patriot Act“, ein Gesetz, das innerhalb von nur drei Tagen vom Repräsentantenhaus und US-Senat kritiklos abgesegnet wurde. Der Patriot Act sah eine drastische Einschränkung der amerikanischen Bürgerrechte vor und vereinfachte die Bedingungen, unter denen die Überwachung oder Durchsuchung von Personen im In- und Ausland veranlasst werden kann. Nicht zuletzt verpflichtete das Gesetz amerikanische Unternehmen, Sicherheitsbehörden Zugriff auf ihre Server zu gewähren, ohne dass dafür eine richterliche Anordnung erforderlich wäre. Der Patriot Act räumte derartige Zugriffsrechte auch für die ausländischen Tochterfirmen von US-Unternehmen ein, selbst wenn lokale Gesetzgebungen anderer Länder eine solche Weitergabe eigentlich verbieten würden. Der 2008 erlassene FISA Amendments Act erleichterte die Überwachung von nicht-US Staatsbürgern außerhalb der USA nochmals deutlich. Ein Themenpapier des Europäischen Parlaments schließt, dass es in der operativen Praxis von US-Behörden vermutlich keinerlei Einschränkung für das Eindringen in die Privatsphäre von nicht-US-Personen gibt [46].

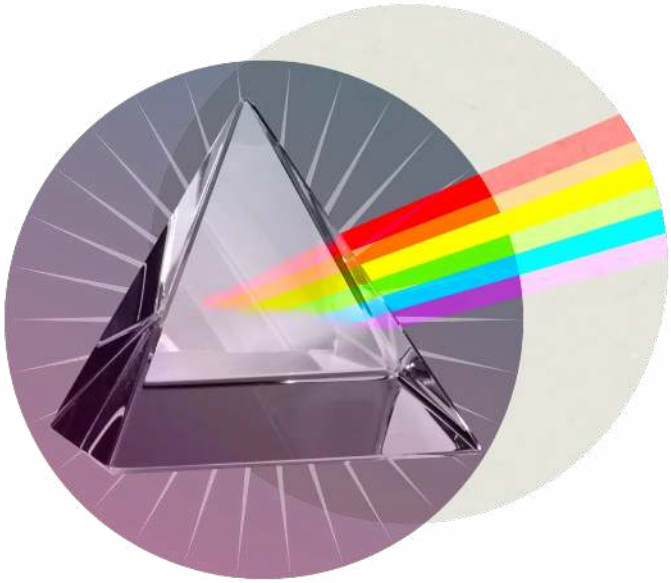
> „Alle für die US-Außenpolitik hilfreichen Daten kommen in Betracht, auch ausdrücklich die politische Überwachung gewöhnlicher und rechtmäßiger demokratischer Aktivitäten.“
>
> Europäisches Parlament | Generaldirektion interne Politikbereiche, 2013

Die Überwachungsprogramme

Hier bekommen Sie Einblick in nur einige der durch Edward Snowden bekannt gewordenen Überwachungsprogramme der NSA.

PRISM

Das Programm PRISM war auf das systematische Sammeln von Kommunikationsdaten ausgerichtet. Nutzerdaten wurden hierbei direkt von den Servern kooperierender Unternehmen mitgeschnitten, die Berichten der Washington Post zufolge zum Teil auch dafür bezahlt wurden [47]. Microsoft, Google, Facebook Skype, Apple, YouTube, AOL und Paltalk räumten der NSA den Dokumenten zufolge in Echtzeit Zugriff auf sämtliche E-Mails, Chatverläufe, Videos, Fotos, Audiodateien, Dateien, Datenübertragungen und Videokonferenzen ihrer Nutzer:innen ein. Zusätzlich erhielten die Geheimdienste persönliche Accountdaten und konnten Berichten zufolge unmittelbar benachrichtigt werden, wenn eine Zielperson sich einloggte [48].



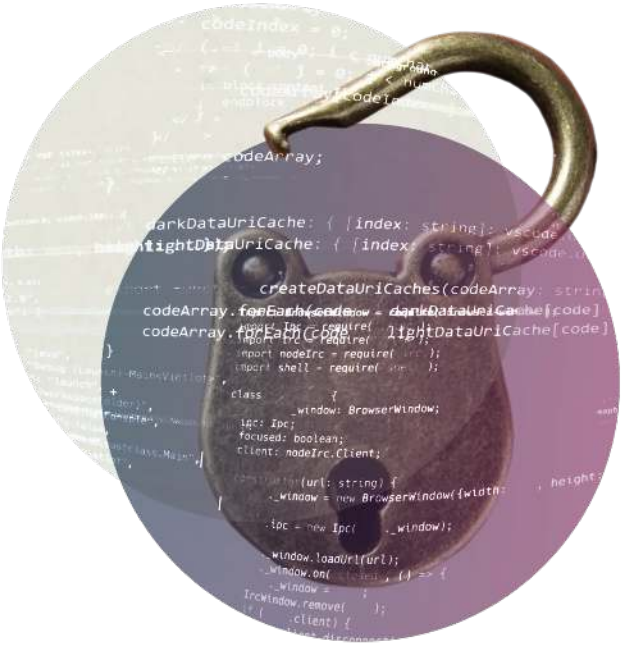
XKEYSCORE

XKeyscore galt als eine der weitreichendsten Analysesoftware für Informationsabfrage und Datenanreicherung im geheimdienstlichen Umfeld. Eine Präsentation der NSA zeigt, dass sie ähnlich einer Suchmaschine verwendet werden konnte. Mittels Angabe einer eindeutigen Kennung, wie E-Mailadresse oder IP-Adresse, konnten in Echtzeit sämtliche vorhandenen Daten über eine Zielperson eingesehen und durchsucht werden [49]. Das verfügbare Material beinhaltete eine nahezu unbegrenzte Vielfalt an Informationen – von getätigten Anrufen über Emailverläufe, Chatprotokolle, Nachrichten und Aktivitäten auf sozialen Netzwerken bis hin zu Browserhistorien und eingegebenen Suchbegriffen. Die NSA argumentierte, dass derartige Abfragen nur zum Schutz der nationalen Sicherheit eingesetzt würden und nur zugelassenem Personal zugänglich sei, das regelmäßigen Kontrollen unterliege [49]. Snowden selbst betonte jedoch, dass die für das Tool freigegebenen Analyst:innen jede Person auf der Welt, zu jederzeit, in Echtzeit abhören konnten, sofern sie nur deren E-Mail Adresse besaßen [50]. Ein Kaufvertrag [51] zwischen

der NSA, dem Bundesnachrichtendienst und dem Bundesamt für Verfassungsschutz bestätigte später, was bis dahin noch dementiert wurde: Auch deutsche Behörden hatten seit April 2013 Zugriff auf XKeyscore. Die Nutzungsvereinbarung ging dem Vertrag nach auch mit umfangreichen Zusagen einher, Daten mit US-Behörden auszutauschen.

BULLRUN

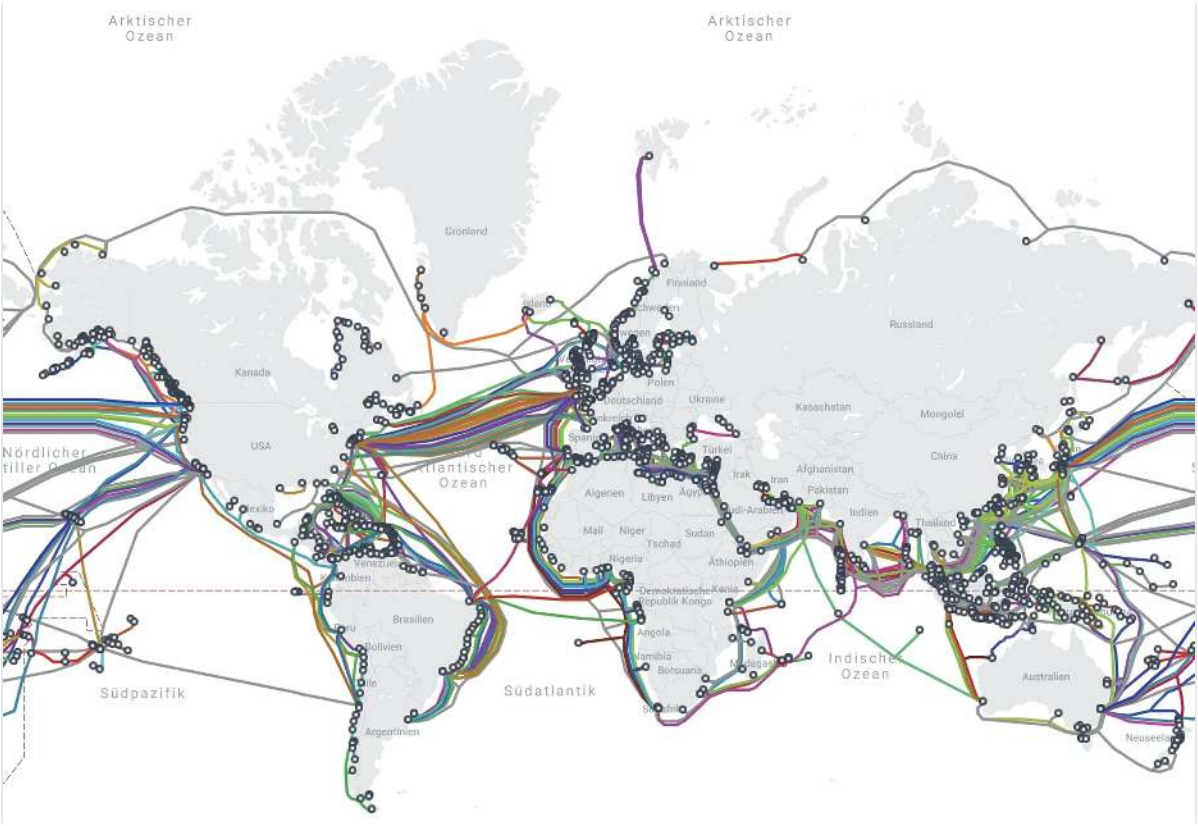
Das Programm Bullrun [46] zielte darauf ab, Verschlüsselungstechnologien zu brechen um verschlüsselte Kommunikation mitlesen zu können. Hierbei wurde parallel mit verschiedenen Methoden operiert – unter anderem wird vermutet, dass die NSA mit Anbietern von IT-Sicherheitsprodukten kooperierte, technische Gremien unterwanderte und dahingehend beeinflusste, unsichere Verschlüsselungsstandards anzunehmen. Auch angenommen wird der systematische Einbau von „Hintertüren" in Verschlüsselungssysteme. Dabei handelt es sich um absichtliche technische Schwachstellen, die Systeme leichter angreifbar machen. Der Einbau von Hintertüren wurde unter Umständen auch mittels richterlicher Zwangsanordnung durchgesetzt [46].



TEMPORA/UPSTREAM

Die Programme Tempora [52] und Upstream [46] beinhalteten das Sammeln großer Datenmengen durch das direkte Anzapfen von Untersee-Glasfaserkabeln und Internetknotenpunkten. Das massenhafte Sammeln und Speichern der Daten geschah dabei anlasslos und verdachtsunabhängig. Erklärtes Ziel des Tempora Programms war nicht weniger als „die Ausbeutung der weltweiten Telekommunikation“ [52]. Es wurde schlicht so viel Datenverkehr wie möglich abgeschöpft, anhand von über 70.000 Stichworten gefiltert, gespeichert und ausgewertet. Im Nachgang wurden Inhalte wie Aufzeichnungen von Telefonaten und E-Mails sowie Metadaten von Geheimdienstmitarbeitern analysiert [53].

In einer Rede beim Chaos Communications Congress 2019 rekapituliert Rainer Rehak, Forscher am Weizenbaum-Institut, die Enthüllungen Snowdens.



Weltweites Netzwerk von Untersee-Glasfaserkabeln

TeleGeography, 2024

Quelle öffnen ↗

Glossar

Quelloffene Software - Open Source bedeutet, dass der einer Software zugrundeliegende Quellcode einsehbar und veränderbar ist.

Sicherheit und Resilienz - Cybersicherheit bedeutet, Angriffe auf digitale Infrastrukturen gar nicht erst geschehen zu lassen, Cyberresilienz heißt, sich im Falle eines Angriffes schnell und koordiniert wieder „aufzufangen"

Colonial Pipelines - Eines der größten Öl-Pipeline-Systeme der USA, das 2021 durch einen Ransomware-Angriff seitens russischer Hacker für mehrere Tage außer Betrieb gesetzt wurde.

Halbleiter - Halbleiter sind Werkstoffe wie Silizium oder Germanium, deren elektrische Leitfähigkeit sich gezielt steuern lässt.

Five Eyes - Eine enge geheimdienstliche Kooperation zwischen den USA, Großbritannien, Neuseeland, Australien und Kanada.

Cambridge Analytica - Die britische Politikberatungsfirma war über umstrittene Wege an die Profildaten von Millionen Facebook Nutzer:innen gelangt und hatte daraus individuelle psychometrische Profile (wie etwa Persönlichkeitstypen) errechnet. Zu den Käufern dieser Profildaten gehörten 2016 der republikanische US-Senator Ted Cruz und der damalige Präsidentschaftskandidat Donald Trump, deren Wahlkampfteams die Profile mutmaßlich gezielt für Wahlwerbung einsetzten.

Desinformation - Falsche oder irreführende Informationen, die gezielt und absichtlich verbreitet werden, um öffentlichen Schaden auszurichten.

Referenzen

[3] „Anmassung in der politischen Sprache - Nicht nur ein Merkmal sogenannter populisten“, Sprachreport, Heft 2, 2017. Quelle öffnen ↗

[4] (2024), “Digital sovereignty—Rhetoric and reality”, Journal of European Public Policy, 31(8), S. 1–22. Quelle öffnen ↗

[5] „Digital sovereignty“, Internet Policy Review, 9(4), 2020. Quelle öffnen ↗

[6] „What does the notion of “sovereignty” mean when referring to the digital?“, New Media and Society, 21(10), S. 2305–2322, 2019. Quelle öffnen ↗

[7] „Digitale Souveränität - Status quo und Handlungsfelder“, Deutsche Akademie der Technikwissenschaften, 2021. Quelle öffnen ↗

[8] „Sovereignty 2.0“, Vanderbilt Journal of Transnational Law, 55(2), S. 283–324, 2022. Quelle öffnen ↗

[9] „Digitale Souveränität als strategische Autonomie“, Kompetenzzentrum Öffentliche IT, 2020. Quelle öffnen ↗

[10] „Significance and challenges of big data research“, Big data research, 2(2), S. 59–64, 2015. Quelle öffnen ↗

[11] „The Fight for Digital Sovereignty“, Philosophy and Technology, 33(3), S. 369–378, 2020. Quelle öffnen ↗

[12] „Digital sovereignty or digital colonialism?“, Sur - International Journal on Human Rights, 15(27), S. 15–27, 2018. Quelle öffnen ↗

[13] „Stärkung der digitalen Souveränität der öffentlichen Verwaltung. Eckpunkte – Ziele und Handlungsfelder“, 2020. Quelle öffnen ↗

[14] „Empfehlungen zur Souveränität und Sicherheit der Wissenschaft im digitalen Raum“, Köln, 2023. Quelle öffnen ↗

[15] „Schwerpunktstudie Digitale Souveränität“, 2021. Quelle öffnen ↗

[16] „Sustainable Digital Sovereignty: Interdependencies Between Sustainable Digitalization and Digital Sovereignty“, Weizenbaum Institute for the Networked Society, Berlin, Working Paper 32, 2023. Quelle öffnen ↗

[17] „14. Bericht der Bundesregierung über ihre Menschenrechtspolitik“, 2020. Quelle öffnen ↗

[18] „Erklärung über Grundsätze des Völkerrechts betreffend freundschaftliche Beziehungen und Zusammenarbeit zwischen den Staaten in Übereinstimmung mit der Charta der Vereinten Nationen“, 1970. Quelle öffnen ↗

[19] Sechs Bücher über den Staat, Bd. I–III, S.222, München: Beck, 1981.

[19] Sechs Bücher über den Staat, Bd. I–III, S.222, München: Beck, 1981.

[20] Reclam, Ditzingen, Bibliographisch ergänzte Ausgabe 2018, [Nachdruck] 2023

[21] Reclam, Ditzingen, Bibliographisch ergänzte Ausgabe 2011, [Nachdruck] 2023

[22] Reclam, Ditzingen, Bibliographisch ergänzte Auflage 2020, [Nachdruck] 2023

[23] „Law and Borders: The Rise of Law in Cyberspace“, Stanford Law Review, 48(5), S. 1367–1402, 1996. Quelle öffnen ↗

[24] „Multi-stakeholderism in Internet governance: putting a fiction into practice“, Journal of Cyber Policy, 1(1), S. 29–49, 2016. Quelle öffnen ↗

[25] „Internet Governance: Past, Present and Future“, Konrad-Adenauer-Stiftung e.V., 2019. Quelle öffnen ↗

[26] „Internet Governance: Territorializing Cyberspace?“, Politics & Policy, 42(5), S. 635–657, 2014. Quelle öffnen ↗

[27] transcript Verlag, 2021, Bielefeld, S. 319–340, Der Wert der Digitalisierung: Gemeinwohl in der digitalen Welt, Hrsg. v. C. Piallat Quelle öffnen ↗

[28] The Future of the Internet-And How to Stop It. New Haven & London: Yale University Press & Penguin UK, 2008. Quelle öffnen ↗

[29] „Long live the web“, Scientific American, 303(6), S. 80–85, 2010. Quelle öffnen ↗

[30] „Manifest für digitale Souveränität“, Open Source Business Alliance - Bundesverband für digitale Souveränität e.V., 2021. Quelle öffnen ↗

[31] „Illusionen der Autonomie? Europas Position in den globalen digitalen Abhängigkeitsstrukturen“, SIRIUS – Zeitschrift für Strategische Analysen, 7(4), S. 390–410, 2023. Quelle öffnen ↗

[32] „Digitale Kommunikationsinfrastrukturen“, in Handbuch Digitalisierung in Staat und Verwaltung, T. Klenk, F. Nullmeier, G. Wewer, Hrsg., Wiesbaden: Springer VS, 2020, S.147-157. Quelle öffnen ↗

[33] „Internet – Platforms – Regulation: Coordination of Markets and Curation of Sociality“. SOI Discussion Paper 2020-02, 2020. Quelle öffnen ↗

[35] „Android: Google setzt Geschäftsbeziehungen zu Huawei aus“, Die Zeit, Hamburg, 20. Mai 2019. Quelle öffnen ↗

[37] „Shoshana Zuboff on the Undetectable, Indecipherable World of Surveillance Capitalism“, Centre for International Governance Innovation, 2019. Quelle öffnen ↗

[38] „Big other: Surveillance Capitalism and the Prospects of an Information Civilization“, Journal of Information Technology, 30(1), S. 75–89, 2015. Quelle öffnen ↗

[39] „How Cambridge Analytica turned Facebook ‚likes‘ into a lucrative political tool“, The Guardian, 17. März 2018. Quelle öffnen ↗

[40] „Leaked: Cambridge Analytica’s blueprint for Trump victory“, The Guardian, 23. März 2018. Quelle öffnen ↗

[41] „Towards a theoretical model of social media surveillance in contemporary society“, Communications, Bd. 40, Nr. 1, Jan. 2015. Quelle öffnen ↗

[42] „Digitale Souveränität“, Kompetenzzentrum Öffentliche IT, Report, 2017. Quelle öffnen ↗

[43] Schlussanträge des Generalanwalts Yves Bot. Rechtssach C-362/14 Maximilian Schrems gegen Data Protection Commissioner, 2015. Quelle öffnen ↗

[44] The New York Times, 08.02.2014 Quelle öffnen ↗

[45] „‘Black budget’ summary details U.S. spy network’s successes, failures and objectives - The Washington Post“, Washington Post, 29. August 2013. Quelle öffnen ↗

[46] „Die Überwachungsprogramme der USA und ihre Auswirkungen auf die Grundrechte der EU-Bürger“, Europäisches Parlament, PE 474.405, 2013. Quelle öffnen ↗

[47] „NSA paying U.S. companies for access to communications networks“, Washington Post, 17. Mai 2023. Quelle öffnen ↗

[48] „Projekt Prism: NSA spioniert weltweit Internet-Nutzer aus“, Der Spiegel, 7. Juni 2013. Quelle öffnen ↗

[49] „XKeyscore: NSA tool collects ‚nearly everything a user does on the internet‘“, The Guardian, 31. Juli 2013. Quelle öffnen ↗

[50] „NSA whistleblower Edward Snowden: ‚I don’t want to live in a society that does these sort of things‘ – video“, The Guardian, 9. Juni 2013. Quelle öffnen ↗

[51] „NSA hilft Verfassungsschutz: XKeyscore – das Dokument“, Die Zeit, Hamburg, 26. August 2015. Quelle öffnen ↗

[52] „GCHQ taps fibre-optic cables for secret access to world’s communications“, The Guardian, 21. Juni 2013. Quelle öffnen ↗

[53] „Abhörskandal: Auch britischer Geheimdienst späht Daten aus“, Handelsblatt, 22. Juni 2013. Quelle öffnen ↗

[54] Europäisches Parlament, nichtständiger Ausschuss über das Abhörsystem ECHELON, 11.07.2001 Quelle öffnen ↗

[55] „Wirtschaftsspionage / Volkswagen ist kein Einzelfall. Sicherheit muss künftig zur Chefsache erklärt werden.“, Handelsblatt, S. 21, 29. August 1996.

[56] „Aktenkrieger“, Süddeutsche Zeitung, S. 19, 29. März 2001.

[57] „French Resent U.S. Coups in New Espionage“, The Washington Post, Washington, D.C., S. A1,A26, 26. Februar 1995.

[58] Wirtschaftswoche, S. 62, 09.11.2000

[59] The New York Times, 03.11.2013 Quelle öffnen ↗

[60] „NSA monitored calls of 35 world leaders after US official handed over contacts“, The Guardian, 25. Oktober 2013. Quelle öffnen ↗

[61] Quelle öffnen ↗

[62] „Secret NSA Documents Show How the US Spies on Europe and the UN“ Quelle öffnen ↗

[63] Der Spiegel, 20. September 2013. Quelle öffnen ↗

[64] „Remarks by H.E. Xi Jinping President of the People's Republic of China At the Opening Ceremony of the Second World Internet Conference“, Wuzhen, 2015 Quelle öffnen ↗

[65] „Navigating Digital Sovereignty and its Impact on the Internet“, 2022 Quelle öffnen ↗

[66] „Data nationalism“, Emory Law Journal, 64(3), S. 677, 2015 Quelle öffnen ↗

[67] „Branding Internet sovereignty: Digital media and the Chinese–Russian cyberalliance“, European Journal of Cultural Studies, 21(5), S. 594–613, 2018 Quelle öffnen ↗

[68] „China Ramps Up Control of Domain Names, Adds New Layer to Great Firewall“, Radio Free Asia, 16.01.2017 Quelle öffnen ↗

[69] „Die Schönheit der Chance: Utopien und das Internet“, Juridikum: Zeitschrift für Kritik, Recht, Gesellschaft, 15(4), S. 459–471, 2014

[70] „Schengen Internet routing“, Deutsche Welle, 20. Februar 2014 Quelle öffnen ↗

[71] „Merkel's European internet“, Deutsche Welle, 17. Februar 2014 Quelle öffnen ↗

[72] „Schengen-Routing, DE-CIX und die Bedenken der Balkanisierung des Internets“, netzpolitik.org e.V., 13.11.2013 Quelle öffnen ↗

[73] „The Road to European Digital Sovereignty with Gaia-X and IDSA“, IEEE Network, 35(2), S. 4–5, 2021 Quelle öffnen ↗

[74] „Speaking sovereignty“, European Security, 31(3), S. 356–376, 2022 Quelle öffnen ↗

[75] „Halbleiter und Chips - wie sie funktionieren und warum sie systemrelevant sind, Neue Zürcher Zeitung, 03. August 2022 Quelle öffnen ↗

[76] Our World in Data, 2022 Quelle öffnen ↗

[77] „Apple: iPhone 15 Pro kommt mit 3-nm-SoC und ohne Schiebeschalter“, golem.de, 12. September 2023 Quelle öffnen ↗

[78] „Zoom into a Microchip video, NISE Network“, 2013 Quelle öffnen ↗

[79] Chip war: the fight for the world's most critical technology. London New York Sydney Toronto New Delhi: Simon & Schuster, 2022

[80] „Cybersicherheitsstrategie für Deutschland 2021“, August 2021 Quelle öffnen ↗

[81] „Die Lage der IT-Sicherheit in Deutschland“, 02.11.2023 Quelle öffnen ↗

[82] Directorate-General for Communications Networks, Content and Technology, Digital Services Act: application of the risk management framework to Russian disinformation campaigns, Brüssel, 2023 Quelle öffnen ↗

[83] „The European Union's governance approach to tackling disinformation – protection of democracy, foreign influence, and the quest for digital sovereignty“, L'Europe en Formation, 396(1), 2023, S. 11-36 Quelle öffnen ↗

[84] „Safeguarding european values with digital sovereignty“, Internet Policy Review, 10(3), 2021 Quelle öffnen ↗

[85] „Die Stärkung der digitalen Souveränität - Wege der Annäherung an ein Ideal im Wandel“, Diskussionspapier von iRights.Lab, Deutsches Institut für Sicherheit und Vertrauen im Internet - DIVISI, 2018 Quelle öffnen ↗

[86] „Europe fit for the Digital Age: Artificial Intelligence“, Brüssel, 2021 Quelle öffnen ↗

[87] The Brussels Effect: How the European Union Rules the World, Oxford University Press, 2020

[88] „Vorschlag für einen BESCHLUSS DES EUROPÄISCHEN PARLAMENTS UND DES RATES über das Politikprogramm für 2030 ‚Weg in die digitale Dekade'“, 2021/0293 (COD), Brüssel, 2021 Quelle öffnen ↗

[89] „Europäische Erklärung zu den digitalen Rechten und Grundsätzen für die digitale Dekade“, Brüssel, 2022 Quelle öffnen ↗

[90] „Digitainability—Digital competences post-COVID-19 for a sustainable society“, Sustainability, 13(17), S. 9564, 2021 Quelle öffnen ↗

[91] „Digitale Selbstbestimmung“, Cologne Center for Ethics, Rights, Economics, and Social Sciences of Health (ceres), Köln, 2016. Quelle öffnen ↗

[92] „Initiative Digitale Bildung“, 2021. Quelle öffnen ↗

[93] „Digitalführerschein, 2023. Quelle öffnen ↗

[94] „Artificial Intelligence and Democratic Norms: Meeting the Authoritarian Challenge, Sharp Power and Democratic Resilience Series, 2020. Quelle öffnen ↗

[95] in "Power and authority in internet governance", Hrsg. v. B. Haggart, N. Tushikov, J. A. Scholte, London: Routledge, 2021, S. 171–194s

[96] „Vier Forderungen für eine digital-souveräne Gesellschaft“, 2021. Quelle öffnen ↗

[97] Auf dem Weg zu einem resilienteren, wettbewerbsfähigeren und nachhaltigeren Europa, Brüssel, 2023. Quelle öffnen ↗

[99] „Cybersecurity, our digital anchor“, EUR 30276 EN, Publications Office of the European Union, Luxembourg, 2020. Quelle öffnen ↗

[100] „Neue Cybersicherheitsstrategie der EU und neue Vorschriften zur Erhöhung der Widerstandsfähigkeit kritischer physischer und digitaler Einrichtungen, Brüssel, 2020. Quelle öffnen ↗

[101] „Digitalisierung nachhaltig und souverän gestalten“, CODINA Positionspapier, 2022. Quelle öffnen ↗

[102] „Narratives of digital sovereignty in German political discourse“, Governance, 36(3), 2023, S. 293-709. Quelle öffnen ↗

[103] „Digital Sovereignty in the EU“, Bertelsmann Stiftung, 2020. Quelle öffnen ↗

[104] „Digital sovereignty for Europe“, EPRS | European Parliamentary Research Service, PE 651.99, 2020. Quelle öffnen ↗

[105] „Europäische Datenstrategie“, Brüssel, 2020. Quelle öffnen ↗

[106] „Gestaltung der digitalen Zukunft Europas“, Brüssel, 2019. Quelle öffnen ↗

[107] „Öffentliches Geld – Öffentliches Gut!: Wem sollen Daten nützen?“, netzpolitik.org e.V., 2020. Quelle öffnen ↗

[108] „Data Governance Act explained | Shaping Europe's digital future“, 2024, Brüssel, Quelle öffnen ↗

[109] „Amerikanische Anbieter dürfen bei EU-Cloud Gaia-X mitmachen“, c't Magazin, 07. Dezember 2020. Quelle öffnen ↗

[110] „‚Ich erwarte nicht, dass Gaia-X liefert, was wir brauchen': Yann Lechelle, CEO des Cloud-Anbieters Scaleway, im c't-Interview über Gaia-X“, c't, 2022, Nr. 1, Heise, S. 14–16, 17. Dezember 2021. Quelle öffnen ↗

[111] „Zentrum für Digitale Souveränität der öffentlichen Verwaltung“, Der Beauftragte der Bundesregierung für Informationstechnik, o.D. Quelle öffnen ↗

[112] „Das EU-Gesetz über digitale Dienste“, Brüssel, o.D. Quelle öffnen ↗

[113] „Das Gesetz über digitale Märkte: für faire und offene digitale Märkte“, Brüssel, o.D. Quelle öffnen ↗

[114] „Achter Altersbericht - Ältere Menschen und Digitalisierung“, 2020. Quelle öffnen ↗

[115] „Gigabitstrategie der Bundesregierung“, Die Bundesregierung informiert | Startseite, 2023. Quelle öffnen ↗

[116] „Europäisches Chip-Gesetz“, Brüssel, o.D. Quelle öffnen ↗