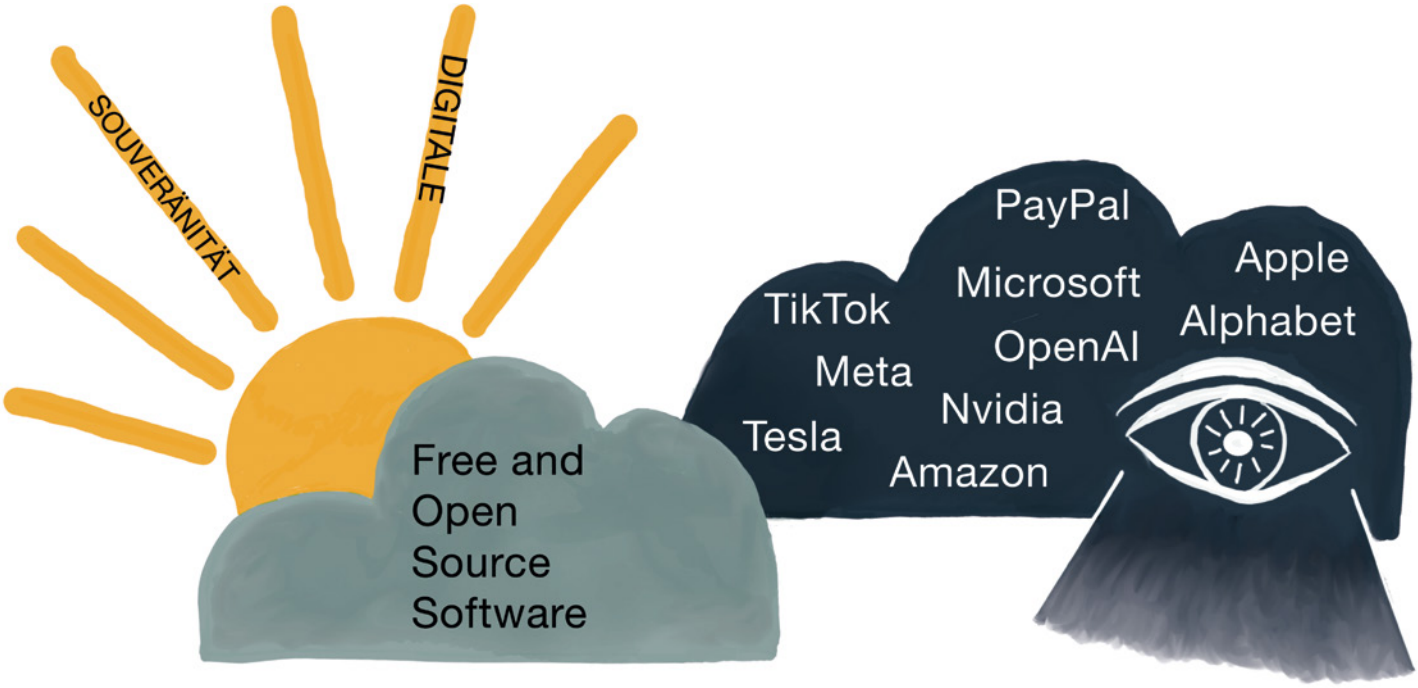
H 7625

FIfF-Kommunikation

Zeitschrift für Informatik und Gesellschaft

43. Jahrgang 2026 Einzelpreis: 7 EUR 2/2026 – Juni 2026



Digitale Souveränität

ISSN 0938-3476

• Tim Berners-Lee: „This Is for Everyone“ • Digitaler Omnibus • netzpolitik.org •

FIfF Kommunikation

Zeitschrift für Informatik und Gesellschaft

Titelbild: *Karin Vosseberg*

Inhalt

Ausgabe 2/2026

inhalt

Editorial

Die Tech Bros, die Broligarchie und ihre Auswirkungen beschäftigen uns auch in dieser Ausgabe der *FIfF-Kommunikation*. Dabei soll es diesmal vor allem um Gegenkonzepte gehen: *Digitale Souveränität gegen Big Tech und Big Brother* ist der Titel unseres diesmaligen Schwerpunkts, den Ulrike Erb und Karin Vosseberg zusammengestellt haben.

Nachdem im Schwerpunkt der *FIfF-Kommunikation 4/2025* der Komplex der Tech-Giganten und der *geopolitische Innovationswettlauf durch KI* aus ökonomischer, politischer und ökologischer Sicht beleuchtet wurden, geht es in dieser Ausgabe um Ansätze und Möglichkeiten, sich auf europäischer, nationaler, gesellschaftlicher und individueller Ebene digital unabhängig zu machen von Technologien monopolistischer Tech-Konzerne, und es geht um politische und technologische Gestaltungsansätze digital souveräner Infrastrukturen.

Dabei werden auch kontroverse Perspektiven dargestellt, etwa der Disput zwischen OSBA[1] und BSI[2] über die Erreichbarkeit von Digitaler Souveränität oder unterschiedliche Konzepte im Hinblick auf Komplexität und Beherrschbarkeit von Cloud-Architekturen.

Zudem werden konkrete Schritte zu Digitaler Souveränität aufgezeigt, sowohl auf politischer Ebene, wie etwa vom ZenDiS[3], vom Land Schleswig-Holstein und von der Stadt München, als auch auf technischer Ebene, wo insbesondere Gestaltungsmöglichkeiten von IT-Infrastrukturen, souveränen Clouds und Online-Plattformen auf Basis von Open-Source-Software skizziert und Ansätze für die Verankerung entsprechender Softwareentwicklungs-Kompetenzen in der Informatikausbildung erörtert werden. Es geht aber auch um gesellschaftliche Risiken von Big-Tech-Anwendungen, insbesondere für Datenschutz und Souveränität bei Finanzdaten, aber auch für Umwelt und Gemeinwohl sowie um zivilgesellschaftliche Initiativen gegen Abhängigkeiten von großen Tech-Konzernen wie die *End-of-10*-Kampagne und diverse Aktivitäten der Bits & Bäume-Bewegung, wo z. B. für dezentrale Konzepte Digitaler Souveränität plädiert wird.

Zu den einzelnen Beiträgen:

In ihrem Beitrag *Wege zu Digitaler Souveränität – Kompetenzvermittlung für die Gestaltung digital souveräner Systeme* beleuchten Ulrike Erb und Karin Vosseberg zunächst unterschiedliche Auslegungen und Realisierungsansätze von Digitaler Souveränität. Anschließend skizzieren sie, welche Kompetenzen in der Informatik und insbesondere der Softwareentwicklung erforderlich und zu verankern sind, um IT-Systeme zu gestalten, die Digitale Souveränität ermöglichen.

Auf den *öffentlichen Briefwechsel* zwischen dem BSI und der *Open Source Business Alliance* (OSBA) zur Frage, *ob Digitale Souveränität überhaupt erreichbar ist*, geht Miriam Seyffahrt aus Sicht der OSBA ein. Sie erläutert die Kritik am BSI und an dessen Kooperation mit US-Hyperscalern und macht die Positionen der OSBA deutlich.

Angesichts der Übermacht von Tech-Eliten und der sogenannten Cyber Dominance, d. h. der Möglichkeit von Herstellern digitaler Produkte, dauerhaft Zugriff auf Systeme und Daten ihrer Kunden zu behalten, entwirft das BSI eine *Doppelstrategie*. Die Präsidentin des BSI, Claudia Plattner, zeigt auf, *wie digitale Innovationen vorangetrieben und dabei digitale Souveränität gestärkt werden soll*.

Aus Sicht des Zentrum Digitale Souveränität (ZenDiS) erläutert Lea Beiermann konkrete *Kriterien zur Bewertung Digitaler Souveränität*, die vom ZenDiS erarbeitet und bis Mitte Mai 2026 in einem offenen Konsultationsprozesses über die Plattform openCode zur Diskussion gestellt wurden. Bei diesem Souveränitätscheck geht es nicht nur um die Bewertung einzelner Softwarelösungen, sondern um die Frage, in welchem Umfang öffentliche Institutionen insgesamt ihre IT-Infrastruktur wählen und ihren Anforderungen entsprechend (mit)gestalten können.

Die Abhängigkeit und Verletzlichkeit unseres Finanzsystems von US-Anbietern thematisiert Thilo Weichert in seinem Beitrag *Wie souverän sind wir bei unseren Finanzdaten?* Zum Ausgangspunkt nimmt er das Beispiel der US-Sanktionen gegen den Internationalen Strafgerichtshof (IstGH), die dazu führen, dass Mitarbeitende des IStGH sowie deren Familienangehörige nicht mehr mit PayPal und anderen US-amerikanischen Bezahlsystemen bezahlen können. Er setzt sich mit datenschutzrechtlichen Risiken dieser Bezahlsysteme auseinander und zeigt mögliche europäische finanzsouveräne Alternativen auf.

In ihrem Beitrag *Sovereign Cloud Stack – Baustein Digitaler Souveränität jenseits von Big Tech* beschreibt Lisa Seifert von der OSBA den Sovereign Cloud Stack (SCS), eine europäische Initiative, die ein offenes, transparentes und anbieterneutrales Cloud-Ökosystem schafft, welches Souveränität gewährleisten soll. Sie erläutert die Grundlagen des SCS, der auf Open Source, einen modularen Software-Stack und offene zertifizierbare Standards setzt und so eine Alternative zu dominierenden Hyperscaler-Cloud-Plattformen darstellt.

Um auf die Herausforderungen der digitalen Souveränität zu reagieren und aktiv gestaltend einzugreifen, wurde 2022 in Dresden der Verein ALASCA e. V. gegründet mit der Mission, die digitale Souveränität Europas durch Open-Source-Zusammenarbeit zu stärken. Maria Vaquero und Daniel Gerber skizzieren im Beitrag *Vertrauen ist gut, Open Source ist besser: Wie ALASCA Digitale Souveränität durch Open Source schafft* die Aktivitäten des Vereins und die derzeit sieben von ALASCA beherbergten Open-Source-Projekte, die jeweils wichtige Beiträge zu offenen, transparenten Cloud-Infrastrukturen leisten.

Ausgehend von der These, dass moderne Cloud-Metaphern oft neue Abhängigkeiten hinter einer ‚Abstraktions-Bürokratie' verschleiern, plädiert Oliver Radfelder in seinem Beitrag für *robuste und beherrschbare (Cloud-)Architekturen, die wirklich souveränes Handeln ermöglichen*. Er fordert eine Informatiklehre, die zu kritischem Denken und Analysieren befähigt und solides ingenieur:innenwissenschaftliches Handwerkszeug zum Erstellen verstehbarer Architekturen vermittelt.

Joseph De Veaugh-Geiss, Community Manager des Projektes KDE Eco, beschreibt *das Opt-Green-Projekt von KDE Eco und*

die zugehörige Kampagne End of 10, deren Ziel es ist, Endgeräte auf Freie Open Source Software umzustellen, um ihre Lebensdauer zu verlängern und die Nutzungsautonomie zu erhöhen.

Am Beispiel der Initiative *foodsharing* gehen Anton Ballmaier und Philip Engelbutzeder auf die Frage ein, *was Digitale Souveränität im Kontext von selbstorganisierten Gruppen bedeuten kann*. Sie beschreiben die Herausforderungen bei der Community-getriebenen Entwicklung und Pflege der digitalen Infrastruktur für die *foodsharing*-Initiative.

Anne Mollen diskutiert in ihrem Beitrag *unterschiedliche Auffassungen von Digitaler Souveränität*: von souveränem Internet über nationalstaatliche Souveränität zu Selbstbestimmung als individuellem und kollektivem Recht. Sie stellt die Frage *Wer ist der Souverän?*, lotet Risiken und Möglichkeiten verschiedener Antworten aus, und stellt insbesondere dezentrale Konzepte den zentralistischen gegenüber.

Inspiriert von der *Cables of Resistance Conference* im April 2026 und von Diskussionen im Bits & Bäume-Netzwerk schlägt Friederike Hildebrandt unter dem Titel *Für eine digitale Souveränität ohne Generative KI* einen Bogen von der europäischen Debatte um Digitale Souveränität und KI über Ressourcenverschwendung von KI-Rechenzentren zu möglichen ökologischen und gemeinwohlorientierten Alternativen auf Basis von Freier und Open Source Software.

Ausgehend von der These, dass u. a. ökonomische Netzwerkeffekte zur Dominanz von Big-Tech-Produkten und -Diensten geführt haben, zeigt der Beitrag *Big Tech und die Probleme der digitalen Souveränität* von Werner Winzerling politische und technische Schwierigkeiten auf, die daraus für die angestrebte Digitale Souveränität in Deutschland und der EU resultieren.

In dem Beitrag *Digitale Souveränität in München: Ein Leitfaden für die Zukunft unserer Städte* beschreibt Dr. Laura Dornheim, IT-Referentin und *Chief Digital Officer* (CDO) der Stadt München, die vier Säulen der digitalen Souveränität, die München in seinem Ansatz verfolgt: Infrastruktur, Software, Daten und Menschen. Als entscheidender Schritt zu digitaler Souveränität wird zudem die systematische Bewertung der IT-Services angesehen.

Mit seiner *Digitalstrategie 2026* setzt Schleswig-Holstein als digitaler Vorreiter im Norden Europas auf digitale Souveränität, Open Source und gesellschaftlichen Nutzen. Ziel ist eine moderne, resiliente und bürgernahe Verwaltung. Mit freundlicher Genehmigung der Staatskanzlei Schleswig-Holstein werden hier einige Auszüge aus dem über 100-seitigen Strategiepapier nachgedruckt.

Unsere digitale Souveränität wird ebenso von privatwirtschaftlichen Oligarchen wie auch durch politische Akteure bedroht. Dagmar Boedicker kommentiert das Konzept *Digitaler Omnibus*, mit dem, vorgeblich zur Vereinfachung und Entbürokratisierung, unter anderem Schutzrechte aus der KI-Verordnung und der Datenschutz-Grundverordnung aufgeweicht werden sollen. Tomas Rudl stellt in seinem Beitrag aus *netzpolitik.org* fest, dass bereits heute Rechte gegen die Tech-Oligarchen nur unzulänglich durchgesetzt werden, wobei die Europäische Kommission und ihre Präsidentin Ursula von der Leyen in beiden Fällen offenbar eine eher unrühmliche Rolle spielen.

Zwei weitere Beiträge aus *netzpolitik.org* behandeln die alltägliche Überwachung. Die Vorratsdatenspeicherung, bereits mehrfach durch höchstrichterliche Entscheidungen gestoppt, wird von Bundesjustizministerin Hubig und Bundesheimatminister Dobrindt erneut aus der Schublade geholt – und ist zum Zeitpunkt des Entstehens dieses Heftes durch die Bundesregierung bereits beschlossen. Mit der Annahme durch die Koalitionsfraktionen im Bundestag ist wohl zu rechnen. Und dann kann sich erneut das Bundesverfassungsgericht damit beschäftigen – warten wir mal ab, ob es angesichts der immer wieder vorgetragenen Initiativen gegen die Grundrechte langsam mürbe geworden ist.

Eine etwas undurchsichtige Rolle spielen gerade Bündnis 90/Die Grünen. Haben sie in der Opposition in Berlin gegenüber der Vorratsdatenspeicherung noch „erhebliche juristische Bedenken", sind sie in Baden-Württemberg, wo sie wieder in die Regierung eingetreten sind, weniger zimperlich. Martin Schwarzbeck stellt die Regelungen des Koalitionsvertrags vor, der unter anderem KI-basierte Gesichtserkennung und Verhaltensanalyse vorsieht. Die Zeiten der Grünen als Bürgerrechtspartei sind – zumindest in Stuttgart – wohl endgültig vorbei. Und es wird vermutlich nicht besser: Rechtsautoritäre Parteien in Europa, im Bund und in den Ländern werden an der hier aufgebauten Überwachungsinfrastruktur ihre helle Freude haben, umso mehr, wenn sie perspektivisch selbst an die Regierung kommen.

Angesichts des Umbaus des Internet und der Kommunikationsinfrastruktur in ein Instrument der staatlichen Überwachung und einer Gelddruckmaschine für Oligarchen erinnert man sich mit Wehmut daran, dass das Ganze einmal ganz anders gedacht war. *This is for Everyone* ist der Titel der Biographie von Tim Berners-Lee, der anfang der 1990er-Jahre die Grundlagen des *World Wide Web* entwickelt hat. Dietrich Meyer-Ebrecht hat sich den Band angeschaut; seine Rezension findet sich ebenfalls in dieser Ausgabe.

Wir wünschen unseren Leserinnen und Lesern eine interessante und anregende Lektüre – und viele neue Erkenntnisse und Einsichten.

Ulrike Erb, Karin Vosseberg und Stefan Hügel
für die Redaktion

Anmerkungen

1 Open Source Business Alliance

2 Bundesamt für Sicherheit in der Informationstechnik

3 Zentrum für Digitale Souveränität der Öffentlichen Verwaltung

Technologie, Künstliche Intelligenz und Faschismus

Wir formen die Künstliche Intelligenz
und danach formt die Künstliche Intelligenz uns.
frei nach Marshall McLuhan[1]

Liebe Freundinnen und Freunde des FIfF, liebe Mitglieder,

die politische und gesellschaftliche Entwicklung nach rechts geht weiter. Was sich in den letzten Wochen immer stärker andeutete, ist inzwischen unbestreitbare Realität: Die *Alternative für Deutschland* (AfD) hat bundesweit die bisher stärkste Partei, die Union, in Umfragen anscheinend stabil überholt; in einzelnen Bundesländern trifft sie bereits seit einiger Zeit Vorbereitungen für eine Regierungsübernahme. Die SPD hat bei der Landtagswahl in Baden-Württemberg mit 5,5 % einen historischen Tiefstand erreicht. Gerade ehemalige Wähler:innen der SPD scheinen sich verstärkt der AfD zuzuwenden – vielleicht eine Spätfolge der *Agenda 2010* der Regierung unter Gerhard Schröder, die die Partei allem Anschein nach immer noch nicht überwunden hat.

Nun erscheinen auch Studien, die diese Entwicklung erklären wollen. Eine auch in der breiten Öffentlichkeit verbreitete These besagt, dass es vor allem die Verlierer:innen der wirtschaftlichen und gesellschaftlichen Entwicklung hin zur Globalisierung und zu „hypermoralischen" urbanen Milieus sind, die sich rechtsautoritären Parteien zuwenden, nicht nur in Deutschland. Dazu mag bei Einzelnen ein Gefühl der Bevormundung kommen. Andererseits ist es sicherlich erklärungsbedürftig, warum – vermeintlich oder tatsächlich – benachteiligte Gruppen ausgerechnet eine westliche Elitenpartei wählen – besonders fällt diese Diskrepanz natürlich in den östlichen Bundesländern ins Auge, wo die AfD inzwischen klar stärkste Partei ist, zumindest, wenn man den Umfragen folgt, die regelmäßig veröffentlicht werden.[2] Doch die AfD als „Ostphänomen" abzutun ist offensichtlich nicht mehr angemessen, wie spätestens die Landtagswahlen in Baden-Württemberg und Rheinland-Pfalz deutlich zeigen.

Ein kürzlich erschienener Sammelband[3] geht dagegen von der These aus, dass der Rechtspopulismus eben nicht eine Reaktion der Beherrschten auf die Globalisierung ist, sondern das Projekt von Teilen der herrschenden Klassen. Unterschieden wird auf der einen Seite nach einem politisch-ökonomischen Erklärungsansatz, nach dem sich die Wähler:innen gegen die Folgen der Globalisierung wenden, einem politischen Erklärungsansatz, der eine mangelnde Responsivität gegen die Anliegen der benachteiligten Schichten in den Blick nimmt, und einem kulturellen Erklärungsansatz, der sich auf die Ablehnung von Liberalisierungsprozessen konzentriert.[4] Dem steht auf der anderen Seite die Analyse der Strategien politischer Unternehmer gegenüber, die bestehende Gelegenheiten nutzen, rechtsautoritäre Parteien zu ihrem eigenen Vorteil aufzubauen.[5]

Bereits zum zweiten Mal in kurzer Zeit setzt sich die *FIfF-Kommunikation* mit der Broligarchie, der Herrschaft einzelner Technologie-Milliardäre auseinander. Diese nutzen ihre Monopolstellung nicht nur, um immer reicher zu werden, sondern auch – besonders in den USA – um politischen Einfluss zu gewinnen. Monopole, bisher als Anomalie der Marktwirtschaft angesehen, werden dabei Mittel zum Zweck; Konkurrenz wird als Störfaktor empfunden.[6] Die dadurch gewonnene Macht wird zur Durchsetzung einer Politik genutzt, die in Teilen als faschistisch bezeichnet werden muss. Das Technologieunternehmen Palantir, das Überwachungssoftware für Militär, Geheimdienste und Diktaturen (und, leider, auch für deutsche Polizeibehörden in einigen Bundesländern) entwickelt, hat ein Manifest mit 22 Punkten veröffentlicht, das die Weltsicht seiner Autor:innen in erschreckender Klarheit vor Augen führt.[7] Das Manifest, eine Zusammenfassung der bereits zuvor in Buchform veröffentlichten Ideologie[8], sieht die „weiche" Macht, in Form von Rhetorik an ihre Grenzen gekommen und fordert „harte" Macht, die auf Software aufgebaut sei (These 4). Die Frage sei dabei nicht, ob künftig KI-gestützte Waffen gebaut werden, sondern wer sie baut und zu welchem Zweck (These 5). Gefordert wird ein nationaler Pflichtdienst (These 6) und die Herstellung von Waffen, seien es bessere Gewehre oder bessere Software (These 7). Die USA seien das Land mit den fortschrittlichsten progressiven Werten der Geschichte (These 13), dessen Macht einen außerordentlich langen Frieden ermöglicht habe (These 14). Europa und Asien zahlten dagegen für die Entmachtung und Abrüstung Deutschlands und Japans nach dem 2. Weltkrieg einen hohen Preis; diese Entmachtung müsse rückgängig gemacht werden (These 15). Kritisiert wird auch eine wahrgenommene Intoleranz der Elite gegenüber dem religiösen Glauben, der widerstanden werden müsse (These 20) und abgelehnt wird Inklusion als *seichte Versuchung eines leeren und hohlen Pluralismus* (These 22). Das beunruhigende daran ist, dass einige Punkte dieser dystopisch anmutenden Weltsicht offenbar bereits tief in die Gedankenwelt bürgerlicher Parteien vorgedrungen sind, wie beispielsweise die zunehmende Tendenz zur Hochrüstung und Vorbereitung zur KI-gestützten Kriegführung[9] auch in Europa zeigt. Dass diese Ideologie nicht zuletzt ihr Fundament in einem christlichen Fundamentalismus hat, der den herannahenden Antichristen beschwört[10], macht es nicht besser. Peter Thiel, der bereits vor langer Zeit erklärt hat, Freiheit und Demokratie seien nicht miteinander kompatibel[11], war einer der ersten der *Tech-Bros*, die sich zur Politik von US-Präsident Donald Trump bekannten; mittlerweile sind ihm anscheinend viele gefolgt – von Elon Musk, der, nicht zuletzt durch öffentliche Aufträge, inzwischen zum vermögendsten Menschen der Welt geworden ist und zu Beginn der zweiten Präsidentschaft Trumps mit Hilfe des dafür eigens geschaffenen DOGE einen Kahlschlag in der US-amerikanischen Administration inszenierte, bis hin zu Tim Cook, dem CEO von Apple, auf einem derer Produkte, soviel sei zugegeben, gerade dieser Text entsteht. Mit Wehmut denkt man an die Ideale eines Steve Wozniak[12] und Tim Berners-Lee[13] zurück, deren Absicht es vielleicht nicht in erster Linie war, ein Instrumentarium zur Überwachung,

zur Kriegführung und zur unermesslichen Bereicherung Einzelner zu schaffen.

Dies alles wird befeuert durch die stürmische Entwicklung der Künstlichen Intelligenz, die inzwischen Technologie, Wirtschaft und zunehmend die Politik beherrscht und – bei aller Kritik und allem Zweifel – wohl zu massiven Veränderungen führen wird in der Art, wie wir Software entwickeln, welche Software wir entwickeln und wie wir Software nutzen, mit erheblichen Auswirkungen auf unser tägliches Leben und unsere Arbeit. Dies sind Veränderungen in den Arbeitsprozessen, zunehmende Möglichkeiten zur Leistungs- und Verhaltensanalyse im Betrieb, Überwachungstechnologien auch in der Öffentlichkeit.[14]

Rainer Mühlhoff[15] analysiert zudem das Zusammenspiel einiger Technologieunternehmen mit der neuen Rechten und die sich daraus ergebenden faschistischen Tendenzen bei einer zweifellos faszinierenden und in vielen Bereichen auch nutzenstiftenden Technologie. Als solche Tendenzen nennt er antidemokratisches Wirken, um die parlamentarische und demokratische Ordnung zu zerstören – Beispiel DOGE –, Gewaltbereitschaft, indem sprachliche, mediale, physische oder politische Gewalt darauf abzielt, Menschen unterzuordnen und Integration und Gleichberechtigung von Minderheiten durch ein Recht des Stärkeren zu ersetzen – Beispiel Umgestaltung von Twitter zum Hetzportal – und zuletzt Technologie als Machtinstrument, um eigene Interessen zu realisieren – Beispiel Nutzung Künstlicher Intelligenz zur softwaregestützten Überwachung.[16] Es wird eine große Herausforderung sein, die sich ergebenden massiven Auswirkungen[17] auf Gesellschaft, Politik, Umwelt und Wirtschaft in den Griff zu bekommen, die heute in ihren Konsequenzen vielleicht überhaupt noch nicht absehbar sind. Dies kann offensichtlich nur gelingen, wenn wir die Entscheidungen, wie wir künftig leben wollen, nicht von den Interessen einzelner Milliardäre und ihrer Technologieunternehmen abhängig machen.

Mit FIfFigen Grüßen
Stefan Hügel

Anmerkungen

1 *„Wir formen unser Werkzeug, und danach formt unser Werkzeug uns." Zitiert nach https://www.zeit.de/kultur/literatur/2011-05/mcluhan-coupland*
2 *Aktuelle Informationen zu Wahlumfragen werden laufend auf https://wahlrecht.de zusammengestellt.*
3 *Geiselberger H Hg. (2026) Oben rechts. Rechtspopulismus als Klassenprojekt. Berlin: Suhrkamp-Verlag*
4 *ebd. S. 7*
5 *ebd. S. 9*
6 *Thiel P (2014) Zero to one. Wie Innovation unsere Gesellschaft rettet. Frankfurt, New York: Campus-Verlag*
7 *Palantir (2026) "Because we get asked a lot. The Technological Republic, in brief". https://x.com/PalantirTech/status/2045574398573453312?lang=de*
8 *Karp AC, Zamiska, NW (2025) The Technological Republic. Über die Macht des Silicon Valley und die Zukunft des Westens. München: FinanzBuchVerlag*
9 *AK bewaffnete Drohnen, IMI, FIfF (2024) Targeted Killing. FIfF-Kommunikation 2/2024, S. 7-12*
10 *Kilian N (2026) Warum die Welt bald untergeht, Zeit online, https://www.zeit.de/2025/48/peter-thiel-antichrist-donald-trump-j-d-vance-usa*
11 *Thiel P (2009) The Education of a Libertarian. https://www.cato-unbound.org/2009/04/13/peter-thiel/education-libertarian/*
12 *Wozniak S, Smith G (2008 [2006]) iWoz. Wie ich den Personal Computer erfand und Apple mitgründete. München: Deutscher Taschenbuch-Verlag*
13 *Berners-Lee T (2026) This is for everyone. Die unvollendete Geschichte des World Wide Web. Hamburg: Rowohlt-Verlag*
14 *Schwarzbeck M (2026) Kameras sollen prüfen, wer und wie brav du bist. https://netzpolitik.org/2026/koalitionsvertrag-baden-wuerttemberg-kameras-sollen-pruefen-wer-und-wie-brav-du-bist/; auch in diesem Heft, S. 71-72*
15 *Mühlhoff R (2025) Künstliche Intelligenz und der neue Faschismus. Stuttgart: Reclam-Verlag*
16 *ebd. S. 14-16*
17 *Jaff A (2025) Broligarchie: Die Machtspiele der Tech-Elite und wie sie Fortschritt verhindern. Berlin: Ullstein-Verlag/Econ*

Das FIfF bittet um Eure Unterstützung

Viermal im Jahr geben wir die FIfF-Kommunikation heraus. Sie entsteht durch viel ehrenamtliche, unbezahlte Arbeit. Doch ihre Herstellung kostet auch Geld – Geld, das wir nur durch eure Mitgliedsbeiträge und Spenden aufbringen können.

Auch unsere weitere politische Arbeit kostet Geld für Öffentlichkeitsarbeit, Aktionen und Organisation. Dazu gehören unsere jährlich stattfindende FIfF-Konferenz, der Weizenbaum-Preis, weitere Publikationen und die Kommunikation im Web: Neben der tatkräftigen Mitwirkung engagierter Menschen sind wir bei unserer Arbeit auf finanzielle Unterstützung angewiesen.

Bitte unterstützt das FIfF mit einer Spende. So können wir die öffentliche Wahrnehmung für die Themen weiter verstärken, die euch und uns wichtig sind.

Spendenkonto:
Bank für Sozialwirtschaft (BFS) Köln
IBAN: DE79 3702 0500 0001 3828 03
BIC: BFSWDE33XXX

Dagmar Boedicker

Projekt *Digital Omnibus*

Wie die Europäische Kommission unsere informationelle Selbstbestimmung verkauft

Informationelle Selbstbestimmung ist nicht alles, aber ohne informationelle Selbstbestimmung ist alles nichts. Hoffentlich hat das wenigstens das Europäische Parlament nicht vergessen. Sicher bin ich mir nicht mehr, weil im Parlament – wie in den europäischen Mitgliedstaaten – ein wachsender Teil der Abgeordneten demokratiefeindlich und autoritär ist. Es wird von den anderen Abgeordneten abhängen, ob Engagierte in Europa auch weiter den Mund aufmachen und sich dabei sicher fühlen können. Gerade ist die EU-Kommission dabei, den Datenschutz irreparabel zu beschädigen, alles im Namen von Vereinfachung und Entbürokratisierung.

Die Exekutive griff die informationelle Selbstbestimmung schon früher an, mit Begründungen wie der Gefahr durch den Terrorismus. Deutlich wurde das in den Jahren seit dem 11. September 2001. Die Konkurrenz zwischen Freiheit und Sicherheit nahm zu; Ende der 2010er-Jahre musste der *Gefährder* für immer mehr Überwachung herhalten. Ängstliche Gemüter mochten das nachvollziehen. Wem an der lebendigen, aktiven Demokratie lag, die oder der hatte andere Prioritäten. Immer wieder musste der Staat daran erinnert werden, dass ihn das Grundgesetz und die europäische Charta der Grundrechte nicht nur zum Respekt, sondern sogar zum Schutz von personenbezogenen Daten gegenüber Dritten verpflichten. Der Schutz der Privatsphäre in Europa ist mehr als das Recht, vom Staat „in Ruhe gelassen" zu werden.

Informationelle Selbstbestimmung in Europa

Natürlich geht es beim Datenschutz nicht darum Daten zu schützen. Nur da, wo sie sich auf uns beziehen oder sich eine solche Beziehung herstellen lässt, sind es personenbezogene Daten[1]. Dann sind sie schutzwürdig, denn sie erlauben Erkenntnisse über uns, unser Denken und Tun, über das was wir glauben und wollen. Lebendige Demokratie braucht Möglichkeiten, sich offen und unzensiert eine Meinung zu bilden und diese zu äußern.

Durch die Datenschutz-Grundverordnung (DSGVO)[2] sind *besondere Kategorien personenbezogener Daten* bisher strenger geschützt als andere. Diese Daten enthüllen Informationen über unsere politische oder sexuelle Orientierung, Gesundheit oder ähnlich intime Information über uns. Ein früherer Entwurf des *Omnibus*-Gesetzes sollte den Schutz aufheben, wenn sie nicht direkt mitgeteilt oder erhoben, sondern wenn sie abgeleitet wurden, wenn auf sie geschlossen wurde. Hätten wir solche Information also für uns behalten wollen, indem wir beispielsweise die elektronische Patientenakte in ihrer jetzigen Form ablehnen (ePA), hätte jede Internet-Apotheke sie auswerten können.[3]

Für Erhebung, Speicherung, Übermittlung und Verarbeitung personenbezogener Daten gelten bisher eindeutige Kriterien. Die EU-Kommission (EK) will die jetzt vereinfachen. Die EK versteht darunter, dass diese Kriterien der Praxis in der Wirtschaft nicht mehr entgegenstehen sollen. Das Kriterium der Rechtmäßigkeit[4] (gesetzliche Grundlage, Rechte der Betroffenen gewahrt, Integrität und Vertraulichkeit, Rechenschaftspflicht des Verantwortlichen) haben große, nicht nur US-amerikanische Konzerne schon immer verletzt, nur *pro forma* eingehalten oder erst dann, wenn ihnen empfindliche Strafen drohten (Ausnahmen bestätigen die Regel).

Hier tagt das Europäische Parlament in Straßburg

Unternehmen, die personenbezogene Daten verarbeiten (die *Verantwortlichen),* können deren Schutz durch *Anonymisierung* stärken, viele Verarbeitungen brauchen keinen Personenbezug. Anders ist es bei einer Verarbeitung zum Zweck personalisierter Werbung oder Kontrolle. Oft wäre es im Sinn der Verantwortlichen, statt der stärkeren Anonymisierung eine Pseudonymisierung zu nutzen. Dazu schreibt Thilo Weichert in der DANA:

> *Anders als bei der Anonymisierung ist es bei der Pseudonymisierung oft leicht möglich, die Person zu reidentifizieren. […] In einem neuen Artikel 41a DSGVO soll die EU-Kommission die Befugnis erhalten, in einem Durchführungsrechtsakt zu definieren, wann keine personenbezogenen Daten mehr vorliegen, da eingesetzte Pseudonymisierungstechniken ausreichend sind.*[5]

Durchführungsrechtsakte und delegierte Rechtsakte standen bereits im Gesetzgebungsprozess für die DSGVO zahlreich auf dem Wunschzettel der Wirtschaft. Viele wurden vom Parlament herausverhandelt. In Zukunft werden Unternehmen wie Meta, Alpha (Google), Salesforce und andere große Daten-Broker den

Druck auf die Kommission verstärken, den sie schon bei Entstehung der DSGVO ausgeübt haben. Das große Profiling wird möglich und wir werden schutzlos sein. Welche Datenschutz-Aufsichtsbehörden sollen helfen, wenn sie schon jetzt hoffnungslos überlastet sind?

EDRi[6] kritisiert, dass mit der Datenverordnung (Data Act), die mehrere Gesetze zusammenfasst und harmonisiert, der europäische Rahmen für den Umgang mit personenbezogenen Daten umgeschrieben wird:

> *Das ist keine kleine technische Aktualisierung. Der Entwurf macht aus der Datenverordnung (Data Act) die zentrale Plattform für den Zugang, die Wiederverwendung und Governance von Daten. Dadurch schreibt er das institutionelle Gleichgewicht des Daten-Rahmenwerks der EU neu. Die Änderungen regeln den Zugang öffentlicher Einrichtungen zu den Daten nicht-öffentlicher Stellen, die Vorgehensweise von Daten-Intermediären und wie geschützte Daten aus dem öffentlichen Bereich weiter verwendet werden können.[7]*

Es sei ein riskanter Weg, das vorhandene Rahmenwerk zu ändern, bevor es sich praktisch bewähren konnte. Manche Bestimmungen seien noch in der Implementierung, was unnötig Unsicherheiten schaffe.

Verhältnismäßigkeit *(proportionality)*[8] beschreibt, was die EK für einen idealen, ökonomischen Kompromiss hält zwischen informationeller Selbstbestimmung der Bürgerïnnen und effizienten – also Kosten-sparenden oder Profit-maximierenden – Maßnahmen:

> *Die Änderungen sind verhältnismäßig, denn sie erlegen den Unternehmen und Behörden, wenn überhaupt, vernachlässigbare Übergangs- und Anpassungskosten auf, ermöglichen aber in den nächsten Jahren hohe Kosteneinsparungen.[9]*

Mit diesem Vorschlag will die Kommission personenbezogene Daten neu definieren:

> *In Nummer 1 würde die Definition des Begriffs „personenbezogene Daten" nach Artikel 4 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung) präzisiert: Demnach gelten in einer bestimmten Einrichtung Informationen dann nicht als personenbezogene Daten, wenn sie nach vernünftigem Ermessen nicht zur Identifizierung der natürlichen Person, auf die sie sich beziehen, dienen können. Folglich fiele eine solche Einrichtung grundsätzlich nicht in den Anwendungsbereich der genannten Verordnung.[10]*

Damit gefährdet die EU-Kommission die Grundrechte aller in der Europäischen Union.

Rundumschlag gegen bisherige IKT-Regulierung

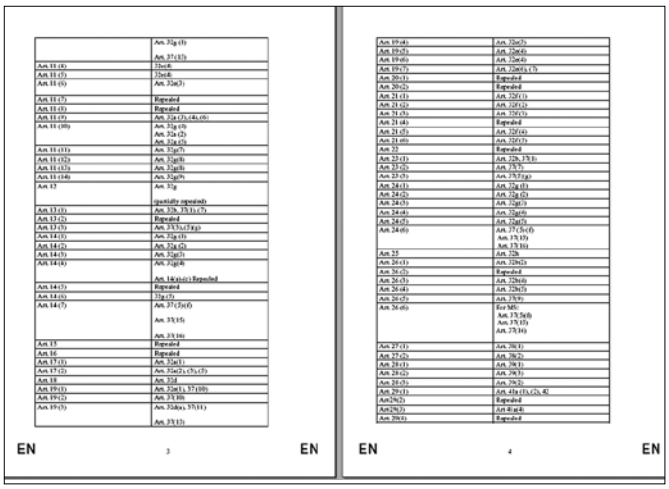
Es ist der zweite Digitale Omnibus, er ändert oder streicht 15 Richtlinien oder Verordnungen. Den ersten hatte die konservative EVP 2019 mit Stimmen von ganz rechts abgesegnet.[11] Jetzt sind die KI-Verordnung (AI Act)[12], die DSGVO, die Cookie-Regelung und die Cyber-Sicherheit der EU dran.

KI-Training mit personenbezogenen Daten, auch Gesundheitsdaten, betrachtet die Kommission generell als legitimes Interesse. Lediglich technisch-organisatorische Maßnahmen sind gefordert. Wie sollen die bitte aussehen? Mit solchen Minimalanforderungen sind unsere Daten Freiwild. Unsere Rechte sind nicht gewahrt, denn wie sollen wir Auskunft, Berichtigung oder Löschung verlangen, wissen wir doch nichts von der Verarbeitung. Eine Einwilligung hat es nie gegeben. Die KI-Verordnung sollte nach langer Umsetzungsfrist im August dieses Jahres endlich wirken. Ausgerechnet der Teil, der die hoch riskanten Systeme behandelt, soll jetzt um mehr als ein Jahr verschoben werden. Bis dahin brauchen wir ihn wahrscheinlich gar nicht mehr, bis dahin produzieren KI-Systeme ohnehin nur noch Inhalte für andere KI-Systeme. (Pardon, ein schlechter Scherz.)

Ich finde, die Kommission beschädigt dramatisch das bewährte Vorsorge-Prinzip europäischer Regelungen und folgt statt dessen angelsächsischen Rechtsgrundsätzen. In den USA dürfen Unternehmen grundsätzlich fast alles. Dafür sind die Strafen drakonisch, wenn sie dabei die Rechte anderer verletzen oder anderweitig Schaden anrichten.

Methode „Move fast and break things"

Mir missfällt, wie hier mit einem Federstrich, in Form eines maximal unübersichtlichen Artikelgesetzes/Omnibus wesentliche Grundlagen der bürgerlichen Freiheiten beschädigt werden. Zuletzt ist mir das erinnerlich bei Otto Schilys Sicherheitspaketen für Deutschland 2001, den sogenannten Otto-Katalogen. Schily sorgte in zwei Artikelgesetzen für Änderungen an elf Gesetzen.[13] Eine so gewaltige Änderungsflut, wie sie die Kommission jetzt durchzieht, ist von Nichtregierungs-Organisationen (NROs) kaum zu bearbeiten, das schaffen nur sehr spezialisierte Menschen. Trotzdem haben sich 127 NROs, darunter auch FIfF, im November letzten Jahres zum Protest zusammengetan. Sie be-



Beispielhafter Auszug aus dem Annex 1 des Digitalen Omnibus mit Verweisen auf die Artikel der Data Governance Verordnung, die in der Datenverordnung (Data Act) geändert oder durch sie gestrichen werden

anstanden die geänderten Definitionen von personenbezogenen Daten, die es jetzt dem Verantwortlichen für die Datenverarbeitung überlassen, ob das Unternehmen einen Personenbezug sehen möchte oder nicht. Sicherheitsvorfälle sind weiterhin zu melden, jetzt aber erst nach 96 Stunden, die Meldepflicht wurde auf hohe Risiken beschränkt. Dafür – wie passend für die Verantwortlichen! – müssen Hochrisiko-KI-Systeme noch immer nicht angemeldet werden. An der breiteren Öffentlichkeit ging die Aufforderung der EU-Kommission zu Stellungnahmen vorbei, nur Fachmedien informierten über das Projekt.

Richtlinien und Verordnungen von großer Tragweite, die teilweise noch kaum in Kraft sind, waren dem geballten Widerstand der Musks, Zuckerbergs und Co. schon lange ausgesetzt. Da ist es empörend, dass das Projekt zu ihrer Entschärfung in größter Eile durchgedrückt werden soll. Es betrifft nahezu alle Bürgerinnen und Bürger der EU. Alle haben wir ein Smartphone in der Tasche, alle nutzen wir die elektronische Kommunikation, ob mit oder ohne sogenannte soziale Netze oder LLMs. Bedauerlicherweise wissen wir wenig über die rechtlichen Hintergründe unserer Nutzung der so bequemen, allgegenwärtigen IT.

Die Kommission scheint nicht nur dem massiven Druck der Big-Tech Unternehmen durch deren Klagen wie Lobbying nachzugeben. Sie erweckt auch den Eindruck, dass sie zu Lasten unserer Privatsphäre und letztlich der Demokratie in Europa bestimmten Wirtschaftsbereichen, beispielsweise den deutschen Auto- und Zubehörproduzenten, das Leben erleichtern möchte. Ein irrlichternder US-Präsident könnte sich an europäischen Exportindustrien *rächen,* wenn die Interessen seiner Kumpels in der Tech-Oligarchie wie geplant beschnitten werden. Europas Feinde sind mächtig.

Risiken, und nein: nichts zu Chancen

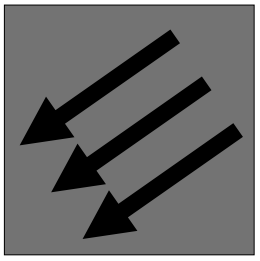
Ich habe keine Lust mehr, von Risiken und Chancen dieser *Vereinfachung* zu schreiben, wenn die Risiken so ungeheuerlich sind und Chancen vorwiegend für Charaktere bestehen, deren Wohl mir kein bisschen am Herzen liegt. Wie konnte es eigentlich passieren, dass ein kleines Oligopol Unsummen investiert, erfolgreich Netzwerkeffekte genutzt und die Vorteile der sogenannten Digitalisierung abgegriffen hat, während unser Planet und (fast?) alle Länder auf den Kosten und Schäden sitzen bleiben? Nach dem papierlosen Büro, der menschenleeren Fabrikhalle und der *Insecurity* of Things (IoT) ist der letzte Coup die sogenannte Künstliche Intelligenz. Für deren Ausbau werden die Rohstoffe vom Meeresboden gekratzt und die Satelliten und das CO_2 in den Weltraum geblasen. Gleichzeitig steuern die selben Milliardäre die Finanzmärkte in die nächste Blase, während sie sich alle unsere Daten einverleiben und uns wie unsere Kinder daran hindern, freie Entscheidungen über Technik und Politik zu treffen. Der neue Kolonialismus ist da und wir merken gar nicht, dass wir Sklaven geworden sind.

Die *Iron Front USA*[14] schreibt auf ihrer Website:

> *Die Geschichtswissenschaft erkennt im Verschmelzen von staatlichen und Konzerninteressen ein bestimmendes Merkmal des Faschismus im 20. Jahrhundert. (Übersetzung d. A.)*[15]
>
> *Faschismus zeichnet sich dadurch aus, sich moderne Technologie als Machtinstrument zur Durchsetzung antidemokratischer Destruktion anzueignen. Das futuristische populäre Bild von KI und die Tech-Ideologien, die hinter diesem Bild stehen, tragen die Idee einer solchen Indienstnahme von KI-Technologie bereits in sich.*[16]

Ein Schuft, wer Böses hierbei denkt:

> *Es wurde eindeutig gefordert, den Besitzstand im Bereich des Datenschutzes zu straffen und die Vorschriften zu konsolidieren. Der Vorschlag behandelt diesen Punkt neben gezielten, von den Interessenträgern unterstützten Änderungen, unter anderem hinsichtlich der Datenschutz-Grundverordnung und der Ermüdung aufgrund der Cookie-Banner. Darüber hinaus wiesen Unternehmen auf weitere Bewertungen des Zusammenspiels zwischen den Datenvorschriften hin, die eine eingehendere Analyse anhand der Instrumente für eine bessere Rechtsetzung rechtfertigen – insbesondere die bevorstehende digitale Eignungsprüfung.*[17]



Symbol der Eisernen Front Deutschland
CC BY-SA 3.0 Fusslkopp

Das große Geld hat vor und nach dem ersten und nach dem zweiten Weltkrieg seinen Einfluss auf politische Entscheidungen geltend gemacht. Sollte das jemals aufgehört haben, tut das Kapital das heute verstärkt. Gerade hat die chilenische Regierung ausländischen Konzernen die unentgeltliche Nutzung aller im Land veröffentlichten Bücher gestattet.[18] Gleichgültig, ob die *Political Action Committees (PACs)* in den USA ihren Kandidaten den politischen Sieg kaufen oder ob durch Morde der Versuch vereitelt wird, alternative politische Systeme wie den Eurokommunismus in Italien zu verwirklichen, ob es staatliche oder wirtschaftliche russische, chinesische oder US-Akteure sind, die den Frieden unterminieren: Auf der Strecke bleiben wir Bürgerïnnen, die gegenüber dem Kapital immer weniger handlungsfähig werden.

Wer hat die EK bevollmächtigt, unsere Grundrechte zu verkaufen?

Die Kommission steckt in der Situation, die rechtlich als *regulatory capture* bezeichnet wird, weil die US-Regierung in unheiliger Allianz mit den Betreibern der großen Plattformen Regelungsvorhaben vorab mit dem europäischen Gesetzgeber verhandelt.[19] Da klingen Phrasen von digitaler Souveränität doch wahrhaft hohl.

Soviel ich weiß, hat keine Versammlung europäischer Bürgerïnnen ihre nationale Regierung oder die EU-Kommission beauftragt, im Dienste internationaler, vorwiegend US-amerikanischer Konzerne und im Namen einer obskuren Vereinfachung und

Entbürokratisierung ihre ureigene Aufgabe und ihre Existenzberechtigung abzugeben. Ihre Aufgabe ist nicht nur der Respekt vor sondern auch das Durchsetzen des Schutzes unserer informationellen Selbstbestimmung gegenüber Dritten. Wo bleibt die Technikfolgen-Abschätzung ihrer Aktivitäten?

Lasst uns Zeichen setzen!

Ein rücksichtsloser Kapitalismus der technisch-militärischen Oligopole hat sich so fest in die deutschen und europäischen Gesellschaften gekrallt, dass der nötige Strukturwechsel schwer genug fällt. Ein Verlust der informationellen Selbstbestimmung würde ihn unmöglich machen. Demokratie funktioniert nicht, wenn diejenigen, die sie verteidigen und umsetzen sollen, eingeschüchtert sind. Vollständig erfasste und beobachtete Menschen werden nicht mehr wagen den Mund aufzumachen, um Kritik zu üben, Forderungen zu stellen oder sich für Minderheiten einzusetzen. Wir wollen aber Achtsamkeit, Fürsorge und Respekt für unsere Mitwelt, menschlich oder nicht, empfinden und leben, mit all jenen, die das auch wollen. Es gibt zu viele, die uns in *wir und die* teilen und gegeneinander aufhetzen wollen, und sie sind zu laut.

> *Es ist leicht, mit den anderen mitzulaufen. Es kann ein eigenartiges Gefühl sein, etwas anderes zu tun oder zu sagen. Aber ohne dieses Unbehagen gibt es keine Freiheit.*[20]

Timothy Snyder nennt in seinem Buch *Über Tyrannei* 20 Lehren aus dem 20. Jahrhundert, eine Auswahl möchte ich vorschlagen: [21]

1. Leiste keinen vorauseilenden Gehorsam.
2. Verteidige Institutionen.
3. Übernimm Verantwortung für das Antlitz der Welt.
4. Denk an deine Berufsehre.
5. Setze ein Zeichen.
6. Glaube an die Wahrheit.
7. Lerne von Gleichgesinnten in anderen Ländern.
8. Achte auf gefährliche Wörter.
9. Sei so mutig wie möglich.

> *Nur eine aktive und aufgeklärte Kontrolle über die Entwicklung und den Einsatz neuer Technologien kann es verhindern, dass diese zu Instrumenten faschistischer politischer Kräfte werden.*[22]

Dieses Paket darf nicht verabschiedet werden! Hoffentlich ist es nicht zu spät. Im Juni sollen Parlament und Rat die Ergebnisse des Trilogs absegnen.

Anmerkungen

1 *Art. 4 (2) DSGVO*
2 *Art. 9 DSGVO*
3 *Dieser Entwurf wurde geleakt und der Punkt gestrichen.*
4 *Art.5 DSGVO*
5 *Weichert, T Der „Digitale Omnibus" der EU-Kommission und der Datenschutz. In Datenschutz Nachrichten 1/2026, S. 18*
6 *die NRO European Digital Rights*
7 *https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/16232-Communication-on-better-regulation/F33370923_en (abgerufen 5.5.2026, Übersetzung die Autorin)*
8 *COM(2025) 837 Digital Omnibus S. 10*
9 *ebda.*
10 *COM(2025) 837 Digital Omnibus S. 23*
11 *Weichert T Der „Digitale Omnibus" der EU-Kommission und der Datenschutz. In Datenschutz Nachrichten 1/2026, S. 21*
12 *https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf*
13 *Sicherheitsüberprüfungsgesetz, Passgesetz und Gesetz über Personalausweise, Vereinsgesetz, Bundeszentralregistergesetz, 10. Buch Sozialgesetzbuch, Luftverkehrsgesetz, Energiesicherungsgesetz, Bundesverfassungsschutzgesetz, MAD-Gesetz, BND-Gesetz, Ausländergesetz und andere ausländerrechtliche Vorschriften.*
14 *Der Name geht zurück auf die deutsche Eiserne Front, eine anti-faschistische Widerstandsgruppe. Sie wurde im Dezember 1931 von der SPD der Weimarer Republik gegründet und kämpfte für die Demokratie gegen Faschismus, Kommunismus und Monarchismus.*
15 *https://ironfrontusa.org/about-us*
16 *Mühlhoff R Künstliche Intelligenz und der neue Faschismus. Reclam Stuttgart 2025. S. 144f*
17 *COM(2025) 837 Digital Omnibus. S. 16*
18 *DLF Kulturzeit. 3.5.2026, 17.30 Uhr*
19 *DLF Kulturzeit. 3.5.2026, 17.30 Uhr*
20 *Snyder T Über Tyrannei. Bonn 2017. S. 51*
21 *Snyder T Über Tyrannei. Bonn 2017*
22 *Mühlhoff R Künstliche Intelligenz und der neue Faschismus. Reclam Stuttgart 2025. S. 147*
23 *Snyder T Über Tyrannei. Bonn 2017*

> *„Die Symbole von heute ermöglichen die Realität von morgen. Achte auf die Hakenkreuze und die anderen Zeichen des Hasses. Schau nicht weg und gewöhne dich nicht daran. Entferne sie selbst und setze damit ein Beispiel für andere, das auch zu tun."*
>
> Timothy Snyder, Über Tyrannei[23]

Dagmar Boedicker

Dagmar Boedicker ist Journalistin und technische Redakteurin.
Sie hat Politikwissenschaft studiert.

Keine Panik! Resilienz in der Polykrise

Call-for-Participation (CfP)

Egal, wohin wir gerade schauen, begegnen uns Krisen. Aktuelle Kriege in der Ukraine und in West-Asien bestimmen die politische Debatte. Die Tech-Bros untergraben nicht erst seit gestern die Demokratie, aber Welthunger und die Umweltkatastrophe gibt es ja auch noch – wir befinden uns mitten in der Polykrise! Diesen Begriff prägten Edgar Morin und Anne-Brigitte Kern im Jahr 1993 in ihrem Buch *Terre-Patrie (Heimatland Erde. Versuch einer planetarischen Politik)*. Um die eskalierende Weltlage zu beschreiben, griff der New Yorker Wirtschaftshistoriker Adam Tooze den Begriff im Jahr 2022 erneut auf, denn die globale Situation hatte sich weiter verschärft.

Sind wir hoffnungslos verloren und rutschen unaufhaltsam in die Poly-Dystopie, wie gehen wir überhaupt mit der aktuellen Entwicklung um, woraus können wir noch Kraft schöpfen und was sind tatsächlich vielversprechende Lösungsansätze? 42 Jahre nach Gründung des FIfF proklamieren wir **„Keine Panik! Resilienz in der Polykrise".**

Gemeinsam mit euch möchten wir an der Schnittstelle von Informatik mit allem anderen folgende Fragen diskutieren, Themen besser verstehen, Aktive zusammenbringen und Pläne schmieden. Wir freuen uns auf kritsch-konstruktive Einreichungen zu Themen wie:

- Krisen: Kriege, Umwelt, digitale Sucht, Ausbeutung, Militarismus
  - Militarisierung der Gesellschaft und des Digitalen
  - Zivilklausel an Hochschulen und Wiedereinführung des Wehrdienstes
  - Klimakatastrophe und Nachhaltigkeitsfragen

- Die Rolle von IT bei Faschisierung und Autokratisierung
  - Beteiligung von BigTech an Konflikten/Aushöhlung der Demokratie
  - KI-Hype und Rechenzentren-Resource-Exhaustion

Dabei sind Bezüge zu folgenden Themen ebenfalls willkommen:

- Strategien für Resilienz in der Polykrise
  - Solidarisches Preppen und Lektionen aus der Kollapsbewegung
  - Praktiken der Dezentralität (von Mastodon bis Solidarische Landwirtschaft)

- Post-Aktivismus, Care-Arbeit und Regeneration
  - Kunst und Kultur für die gesellschaftliche Transformation
  - Blockade, Widerstand und direkte Aktionen

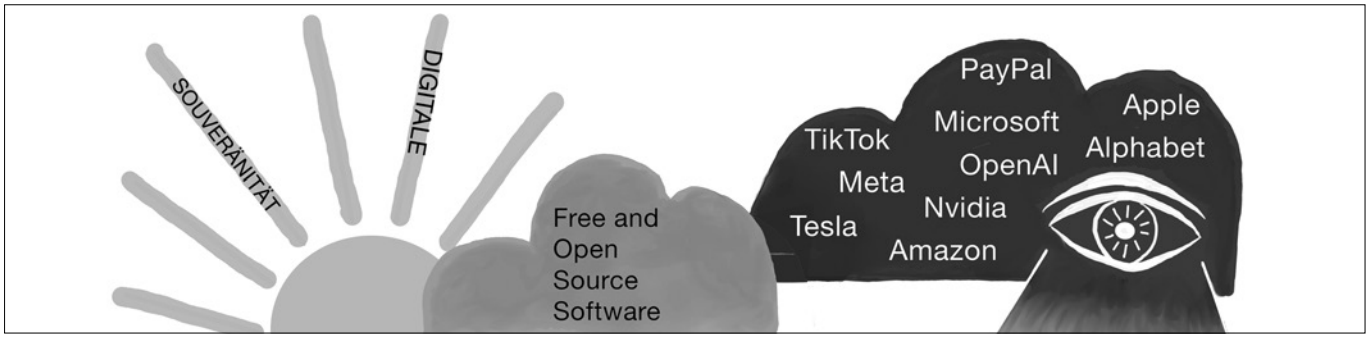
Wenn ihr Euch bei Eurer Idee unsicher seid, ob sie denn wirklich zur Konferenz passt, dann reicht sie bitte ein. Die Beiträge werden anschließend in Artikelform in der FIfF-Kommunikation veröffentlicht.

Formate

Von Vorträgen (lang: max 45 Min./kurz: 20 Min. inkl. Fragen) über Paneldiskussionen, partizipative Formate, multimediale Performances und Ausstellungen bis hin zu Livemusik freuen wir uns über Ideen und schauen, wie wir das ins Tagungsprogramm integrieren können.

Eure Vorschläge könnt ihr hier einreichen:
https://fahrplan.2026.fiffkon.de/fiffkon26/cfp

Die Konferenz findet vom 30. Oktober bis 1. November 2026 in Berlin-Weißensee im *Theater im Delphi*, Gustav-Adolf-Straße 2, 13086 Berlin statt.



Ulrike Erb, Karin Vosseberg, Hochschule Bremerhaven, Informatik

Wege zu Digitaler Souveränität – Kompetenzvermittlung für die Gestaltung digital souveräner Systeme

Zunächst beleuchten wir unterschiedliche Vorstellungen darüber, wie Digitale Souveränität erreicht werden kann und welche Rolle Open Source Software und offene Schnittstellen dabei spielen. Anschließend wird es darum gehen, welche Kompetenzen zur Entwicklung digital souveräner Systeme erforderlich sind und in der Softwareentwicklungs- und Informatikausbildung vermittelt werden sollten.

Unterschiedliche Vorstellungen zum Erreichen Digitaler Souveränität

Digitale Souveränität wird definiert als „Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können" (IT-Planungsrat[1]) oder auch als „Fähigkeit des Staates, seine digitalen Infrastrukturen jederzeit selbstbestimmt zu gestalten und zu kontrollieren"(ZenDiS[2]).

Die Vorstellungen darüber, wie Digitale Souveränität erreicht werden kann, gehen jedoch auseinander:

US-amerikanische Big-Tech-Konzerne versuchen, den europäischen Bestrebungen nach Digitaler Souveränität zu begegnen, indem sie eigene Produkte mit Serverstandort in Deutschland als souverän vermarkten. Das ZenDiS bezeichnet diese Form des Etikettenschwindels in einem Whitepaper als „Souveränitäts-Washing – also die Vermarktung von scheinbar souveränen Lösungen, die sich bei genauerer Betrachtung jedoch als neue Verpackung altbekannter Abhängigkeiten entpuppen."[3] Weiter wird dort der Versuch von Interessenvertreter:innen kritisiert, „Digitale Souveränität in ihrem Sinne umzudeuten – sie wird hierzu häufig fälschlich mit Abschottung bzw. Autarkie gleichgesetzt."[4] Mit dieser Begriffsdeutung wird suggeriert, dass digitale Vernetzung und freier Informationsaustausch durch Digitale Souveränität infrage gestellt werden.

Beim EU-Gipfel zur europäischen Digitalen Souveränität im November 2025 wurde Digitale Souveränität vor allem im Hinblick auf die Stärkung der Wettbewerbsfähigkeit europäischer IT-Unternehmen ausgelegt: *„Für Europa bedeutet digitale Souveränität"* laut Friedrich Merz, *„die Fähigkeit, Technologie entlang der gesamten Wertschöpfungskette im Einklang mit europäischen Interessen und Bedürfnissen zu gestalten."*[5]

Auch das *Cloud Sovereignty Framework* der EU-Kommission[6] fokussiert auf die europäische Produktion von Informationstechnologien und auf das Betreiben von IT-Systemen im Geltungsbereich europäischer Rechtsvorschriften und ohne Abhängigkeit von Nicht-EU-Anbietern. Closed-Source-Anbieter werden also nicht ausgeschlossen, solange es sich um europäische Unternehmen handelt.

Entsprechend heißt es im Strategiepapier der Bundesregierung zum Deutschland-Stack unter *Digitale Souveränität*:

- „Die Lösungen werden primär dynamisch am europäischen Markt eingekauft.
- Die notwendigen eigenen Anteile an Lösungen werden als Open Source entwickelt.
- Die Lösungen erfüllen die bündelungsfähigen Bedarfe und bieten offene Schnittstellen sowie lokale Datenhaltung."[7]

Diese Ansätze werden insbesondere von der *Open Source Business Alliance* – Bundesverband für digitale Souveränität e. V. (OSBA) – als zu halbherzig kritisiert, da auch bei europäischen Closed-Source-Anbietern *Lock-in*-Effekte eintreten können, die den Wechsel zu anderen Anbietern erschweren. Nur *Open Source Software* stellt laut OSBA sicher, „dass die verwendeten Systeme unabhängig überprüfbar, gestaltbar und austauschbar sind"[8] und Digitale Souveränität im Sinne von Herstellerunabhängigkeit, Wechselfähigkeit, Anpassbarkeit, Gestaltungsfähigkeit sowie Transparenz und Kontrolle über den Quellcode der Software ermöglichen.[9]

Immerhin hat der IT-Planungsrat im März 2026 die Standards des unter dem Dach der OSBA entwickelten *Sovereign Cloud Stack (SCS)* verbindlich in den Deutschland-Stack aufgenommen[10] und damit eine Weiche für die Verankerung von Open-Source-basierten Cloud- und Container-Infrastrukturen und offenen Schnittstellen in der öffentlichen Verwaltung gestellt.

Wie lässt sich erreichen, dass Open Source Software konkurrenzfähig ist und Digitale Souveränität ermöglicht?

Die Veröffentlichung unter Open-Source-Lizenzen garantiert nicht per se, dass Software bedarfsgerecht, qualitativ hochwertig und digital souverän ist.

Um dies zu erreichen, ist es erforderlich,

- die Entwicklung und Pflege von bedarfsgerechter Open Source Software einschließlich sicherer Software-Lieferketten zu koordinieren,
- Open-Source-Projekte mit personellen und finanziellen Ressourcen zu unterstützen,
- bei der Beschaffung von Software durch öffentliche Stellen vorzugeben, dass Open Source, offene Standards und offene Schnittstellen als verbindliche Kriterien für Digitale Souveränität zu berücksichtigen sind (*public money – public code*),
- Softwarequalitäts- und Souveränitätskriterien bereits bei der Entwicklung von Open Source Software zu berücksichtigen und
- entsprechende Kompetenzen in *Open Source Communities* und in der Software-Engineering-Ausbildung zu vermitteln.

Auf diese Punkte gehen wir im Folgenden ausführlicher ein.

Unterstützung von Open-Source-Projekten

Beispiel ZenDiS – openCode

Eine sehr konkrete Unterstützung von Open-Source-Entwicklungen leistet das 2022 vom Bundesinnenministerium gegründete Zentrum für Digitale Souveränität der Öffentlichen Verwaltung (ZenDiS). Es versteht sich als Kompetenz- und Servicezentrum, das die Verwaltung dabei unterstützt, „sich aus kritischen Abhängigkeiten von einzelnen Technologieanbietern zu lösen." Weiter heißt es im Selbstverständnis des ZenDiS: „Wir beraten, befähigen, begleiten und stellen Zugang zu modernen, leistungsfähigen und skalierbaren Alternativlösungen bereit."[11] Mit der Plattform *openCode*[12] ermöglicht das ZenDiS einen einfachen und sicheren Zugang zu bereits erprobten Open-Source-Lösungen. Über openCode werden verbindliche Sicherheitsstandards etabliert und nachvollziehbare Herkunftsnachweise für kritische Softwarekomponenten geschaffen.[13] Die Verwaltung kann die auf openCode bereitgestellten Anwendungen in der Regel ohne Ausschreibung beziehen. Seit März 2026 sind die Beschaffungsregelungen so gestaltet, dass öffentliche Auftraggeber in Bund, Ländern und Kommunen Open Source Software in Vergabeverfahren rechtssicher beschaffen können.[14]

Zudem wird in der openCode Community die verwaltungsübergreifende Zusammenarbeit zur bedarfsorientierten Weiterentwicklung von Anwendungen gefördert sowie der Austausch von Entwickler:innen und Verwaltungsmitarbeitenden und der Aufbau von IT-Expertise (Abbildung 1). So entsteht ein „lebendiges Netzwerk für Digitale Souveränität" mit einem Gitlab-Zugang, über den Code geteilt, Projekte eingereicht und qualitätsgesichert weiterentwickelt werden können.[15]

Aufgrund des kooperativen Vorgehens in der openCode-Community lässt sich Geld für Parallelentwicklungen verschiedener Verwaltungseinheiten sparen und die Qualität der entwickelten Open-Source-Anwendungen steigern.

Beispiel Open-Source-Strategie in Schleswig-Holstein

Wie bei openCode wird auch bei der Digitalisierungsstrategie in Schleswig-Holstein die Forderung *public money – public code* in die Tat umgesetzt. Als erstes Bundesland verfolgt Schleswig-Holstein eine konsequente Open-Source-Strategie bei seiner IT-Infrastruktur: Durch eine vielfältige Anbieterlandschaft, offene Standards und Open-Source-Systeme soll, laut Digitalisierungsminister Dirk Schrödter, die Unabhängigkeit von einzelnen IT-Anbietern und damit die Sicherstellung der Digitalen Souveränität gewährleistet werden.[17]

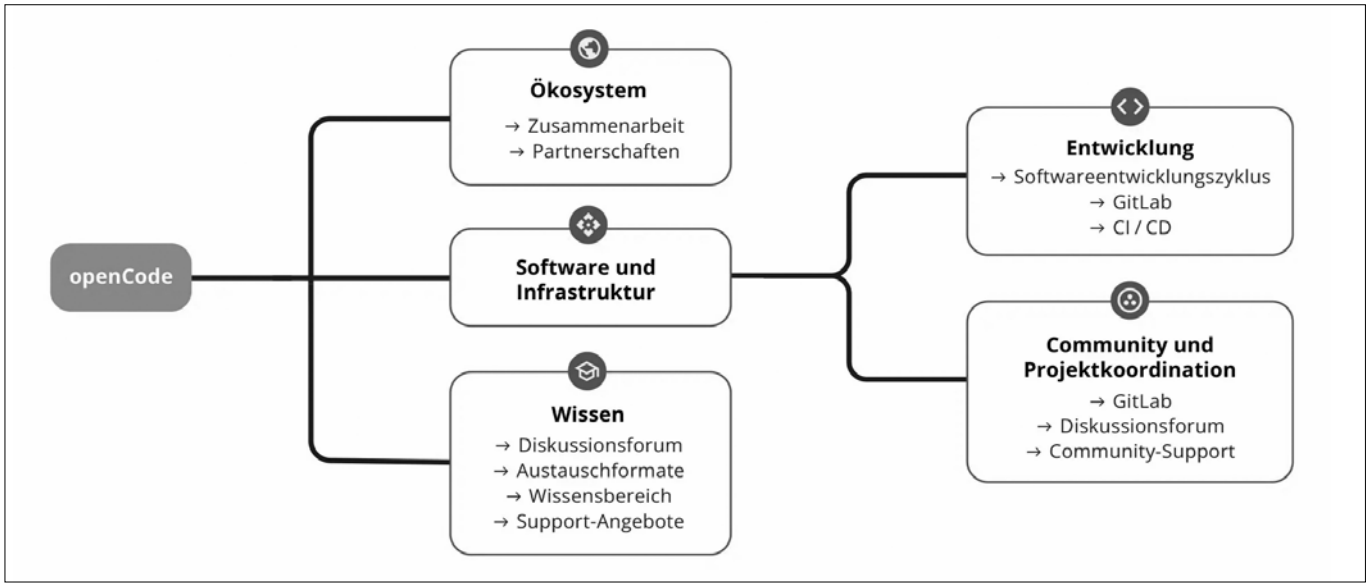


Abbildung 1: openCode-Handlungsfelder[16]

Zur Umsetzung der Strategie fördert das Land Open-Source-Projekte, „die konkrete Bildungseinrichtungen und gemeinnützige Organisationen aus ganz Schleswig-Holstein adressieren."[18] 2025 wurden 17 Projekte durch eine Fachjury ausgewählt, nach Kriterien wie Praxisrelevanz, Skalierbarkeit und Nachnutzbarkeit. Dafür wurden insgesamt knapp drei Millionen Euro bereitgestellt.[19]

Damit die entwickelten Anwendungen auch langfristig für viele weitere Akteure nutzbar sind, soll der Quellcode auf openCode veröffentlicht werden.

Durch den Umstieg auf Open-Source-Anwendungen spare das Land, so Schrödter, „schon jetzt mehr als 15 Millionen Euro an Lizenzkosten." Dem stünden im Jahr 2026 neun Millionen Euro an einmaligen Investitionen für die Migration und die Weiterentwicklung der Open-Source-Lösungen gegenüber.[20]

Bundesländer wie beispielsweise Thüringen und Berlin folgen diesem Beispiel und haben sich auf den Weg zu Digitaler Souveränität durch Open Source gemacht. Man kann sich vorstellen, welchen Qualitätsschub es für Open-Source-Anwendungen bedeuten würde, wenn weitere Bundesländer diesem Beispiel folgten und ihre öffentlichen Gelder für die Unterstützung von Open-Source-Projekten bereitstellten, statt damit die Lizenzkosten von Closed-Source-Anbietern und Big-Tech-Unternehmen zu begleichen.

Kompetenzvermittlung zur Gestaltung digital souveräner Software und Infrastrukturen

Allerdings ist das Erreichen Digitaler Souveränität kein Selbstläufer bei der Open-Source-Entwicklung. Zum Teil gilt auch im Open-Source-Bereich, dass Softwaresysteme oft von so hoher Komplexität sind, dass sie Transparenz und Gestaltbarkeit erschweren und selbst für Entwickler:innen schwer zu durchdringen sind.

Verstehbare Systeme

Um dem zu begegnen, sollte eine bewusste Reduzierung von Komplexität angestrebt werden, so dass Systeme verstehbar bleiben und eine im Hinblick auf Digitale Souveränität und auch auf Ressourcensparsamkeit optimierbare Gestaltung ermöglichen. Dies erfordert entsprechende Kompetenzen der Entwickler:innen und stellt spezielle Anforderungen an die Informatik-Ausbildung.

Als unabdingbare Voraussetzung sehen wir an, dass das etablierte Grundlagenwissen der Programmierung und Softwareentwicklung einen hohen Stellenwert erhält und behält, angesichts der Menge an Abstraktionen durch Frameworks, LowCode-Umgebungen, Serviceorientierung und KI-Generierung.

Neben dem Verinnerlichen gut verstandener Basistechniken sollten Kompetenzen für souveräne, qualitätsgesicherte und nachhaltige Systementwicklung stärkere Verbreitung in der Informatik-Ausbildung und Praxis finden und insbesondere in Open Source Communities verankert sein. Eine gute Orientierung hierfür bieten die in der ISO/IEC 25010:2023 standardisierten Qualitätsmerkmale von Software, die um weitere Kriterien für Digitale Souveränität zu ergänzen sind.

Softwarequalitäts- und Souveränitätskriterien

Unter den neun Kategorien der ISO/IEC 25010:2023 sind Qualitätskriterien für Software definiert, die bereits einige Kriterien für digital souveräne Systeme enthalten, siehe Abbildung 2, in der entsprechende Souveränitätskriterien durch Umrandung hervorgehoben sind.

Schaut man sich die von der OSBA genannten Anforderungen an digital souveräne Systeme an wie *Herstellerunabhängigkeit, Wechselfähigkeit, Anpassbarkeit und Gestaltungsfähigkeit, Transparenz und Kontrolle über den Quellcode*, so werden diese teilweise bereits abgedeckt durch die Kriterien unter den Kategorien *Hohe Kompatibilität, Wartbarkeit und Flexi-*

Adäquate Funktionalität	Effiziente Performance	Hohe Kompatibilität	Benutzungs-freundliche Interaktion	Verlässlich-keit	Sicherheit	Wartbarkeit	Flexibilität	Betriebs-sicherheit
vollständig hinsichtlich Software-funktionen	gutes Zeitverhalten	optimale Coexistenz zu weiterer Software	erkennbare Interaktionen	ausgereifte Software-qualität	Vertraulich-keit	modularer Aufbau	gute Adaptivität	Betriebsbe-schränkung auf sichere Parameter
funktional korrekt	effektive Ressourcen-nutzung	Interopera-bilität	Leicht erlernbar	Fehlertoleranz	Integrität	Wiederver-wendbarkeit	Skalierbarkeit	Risikoidenti-fizierung
funktional angemessen	Kapazitäten schonen		gut bedienbar	Verfügbarkeit	nachvollzieh-bare Herkunfts-nachweise	gut analysierbar	leicht zu installieren	Ausfallsicher-heit
			Inklusivität	Wiederher-stellbarkeit	sichere Administra-tion und geschützte Benutzer-Accounts	leicht modifizierbar	einfach austauschbar	Gefahren-warnung
			Benutzungs-unterstützung			Testbarkeit		Sichere Integration
			selbst-beschreibend					
			Schutz vor Fehlbedienung					
			Motivierende Interaktion		Authentifizier-barkeit			

Abbildung 2: Qualitätsmerkmale von Software gemäß ISO/IEC 25010:2023[21]

bilität. Die geforderte *Kontrolle über Softwarelieferketten*, die insbesondere verhindern soll, dass Schadsoftware durch Software-Updates eingeschleust wird, wird durch das Kriterium *nachvollziehbare Herkunftsnachweise* adressiert.

Anforderungen, die sich aus dem Kriterium *Nutzungsautonomie* des Blauen Engel für ressourceneffiziente Software[22] ergeben, wie *Offenlegung, Datenformate und Schnittstellen, Kontinuität des Softwareprodukts, Vermeidung von Tracking* und insbesondere die *Dokumentation des Softwareprodukts, der Lizenz- und Nutzungsbedingungen*, werden bisher noch nicht durch die Qualitätskriterien abgedeckt und sollten bei einer Weiterentwicklung der ISO 25010:2023 berücksichtigt werden.

Natürlich reicht die Definition von Qualitäts- und Souveränitätskriterien allein nicht. Zum einen ist die Informatik gefordert, Konzepte und Werkzeuge bereitzustellen, mit denen sich solche Anforderungen überprüfbar umsetzen lassen. Zum anderen müssen entsprechende Kompetenzen in der Informatik- und Software-Engineering-Ausbildung verbindlich vermittelt werden.

Kompetenzen für Digitale Souveränität in IT-Lehrplänen verankern

Kompetenzen zur Entwicklung digital souveräner Systeme betreffen alle Phasen und Rollen der Softwareentwicklung, wie

- Spezifikation von Softwareanforderungen unter Einbeziehung der Qualitäts- und Souveränitätskriterien,
- Entwicklung nachhaltiger, transparenter, modularer Systeme mit offenen Schnittstellen,
- Gestaltung souveräner Software-Architekturen und Cloud-Infrastrukturen auf Basis von Open-Source-Komponenten und offenen Schnittstellen,
- Kooperation mit/in Open Source Communities,
- Lizenzrecht,
- Analyse-, Bewertungs-, Diskursfähigkeiten im Hinblick auf Chancen und Probleme digital souveräner IT-Gestaltung.

Auch in der Ausbildung zur Modellierung von Fachverfahren und Geschäftsprozessen ist entsprechendes Know-how zu verankern, wie

- Anbieter-unabhängige Workflow-Modellierung,
- Nutzung offener Standards und Austauschformate,
- Kenntnisse souveräner Clouds und rechtlicher Anforderungen.

In der IT-Beschaffung ist neben Kenntnissen

- der Qualitäts- und Souveränitätskriterien,
- offener Standards, offener Software- und Cloud-Lösungen

auch der Umgang mit Open-Source-Plattformen wie openCode wichtig, um kompetente Entscheidungen zur Beschaffung digital souveräner Software-Lösungen treffen zu können.

Beispiel Hochschule Bremerhaven

An der Hochschule Bremerhaven machen wir gute Erfahrungen damit, den Dreiklang von *Digitaler Souveränität – Open Source – Nachhaltigkeit* als Querschnittsthemen in vielen Modulen des gesamten Studiums zu integrieren. Mit der Bedeutung von Open Source und offenen Standards für das durchdringende Verstehen von Softwaresystemen setzen sich die Studierenden schon ab dem ersten Semester aktiv auseinander – durch Nutzung von Open-Source-Werkzeugen für die Softwareentwicklung anhand von zunächst kleinen Beispielen. Die Studierenden arbeiten vom ersten Tag an in einer open-source-basierten IT-Infrastruktur des Studienbereichs Informatik, mit der die Idee der Digitalen Souveränität umgesetzt wird.

Die konkrete Vermittlung grundlegender Kompetenzen für digital souveränes Handeln von Entwickler:innen ist bereits in verschiedensten Modulen der Informatik-Grundausbildung verankert. In den Pflicht- und Wahlmodulen der Software-Engineering-Ausbildung liegt ein besonderer Fokus auf durchdringendem Verstehen von Konzepten und deren konkreter Umsetzung auf Basis von Open Source Software. Komplexitätsreduzierung, offene Schnittstellen, ressourcenschonende Softwareentwicklung, die Integration von Qualitätssicherungsmaßnahmen sowie rechtliche Rahmenbedingungen stehen hier im Vordergrund. Dabei gilt es, die Bezüge zu Digitaler Souveränität und zu einem nachhaltigen Umgang mit Ressourcen konkret herzustellen. Insbesondere in Anbetracht einer zunehmenden KI-Generierung von Software muss das Erlernen der Grundfertigkeiten bewahrt werden. Zusätzlich sollte das Thema natürlich auch in Projekten und Wahlmodulen integriert werden. Insbesondere in den einjährigen Projekten können die erlernten Fertigkeiten weiter vertieft werden. Begleitet wird das Erlernen von Grundfertigkeiten der digital souveränen Softwareentwicklung durch Diskussionen zu einem verantwortungsbewußtem Handeln von Entwickler:innen im Rahmen des Pflichtmoduls Technologiefolgenabschätzung.

Besonders interessierte Studierende beteiligen sich zudem gemeinsam mit Lehrenden und Labormitarbeitenden in einer außercurricularen Lerngemeinschaft an der Weiterentwicklung der IT-Infrastruktur der Informatik. Sie lernen dadurch, sich mit einer digital souveränen Umgebung auseinanderzusetzen und sammeln Erfahrungen, die Anforderungen an Digitale Souveränität konkret umzusetzen.

Fazit

Aus Sicht von Informatik- und Software-Engineering-Ausbildung kann Digitale Souveränität gestärkt werden durch

- die Kompetenzvermittlung in der Aus- und Weiterbildung zur Entwicklung, Beschaffung, Administration, Nutzung und Pflege digital souveräner, sicherer und ressourcensparsamer Software und IT-Infrastrukturen,
- die Befähigung zur Beteiligung in Open Source Communities und zur Nutzung von kollaborativen Plattformen wie openCode zur Entwicklung souveräner Software und zur Kontrolle über Softwarelieferketten,

- die Beteiligung am Auf- und Ausbau von open-source-basierten Cloud- und Kommunikationsinfrastrukturen, die von vertrauenswürdigen Stellen im Geltungsbereich der DSGVO gehostet werden.

Referenzen

Blauer Engel (2020): Blauer Engel für ressourcen- und energieeffiziente Softwareprodukte, DE-UZ 215 – Hintergrundbericht zur Entwicklung der Vergabekriterien. Ausgabe Januar 2020, Version 4. https://www.umweltbundesamt.de/system/files/medien/479/publikationen/texte_119-2021_umweltzeichen_blauer_engel_fuer_ressourcenund_energieeffiziente_softwareprodukte.pdf

BSI & ZenDiS (2025): Sichere Softwarelieferketten: openCode als Baustein einer souveränen digitalen Infrastruktur. Strategiepapier des BSI & ZenDiS. 10.04.2025. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ZenDiS/Strategiepapier-Softwarelieferketten.pdf

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

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

OSBA (2025): Stellungnahme zum Deutschland-Stack. https://osb-alliance.de/publikationen/statements/stellungnahme-der-osba-zum-deutschland-stack

OSBA (2026): Call for Evidence: European Open Digital Ecosystems. Stellungnahme der Open Source Business Alliance. 3. Februar 2026. https://osb-alliance.de/wp-content/uploads/2026/02/2026-01-27_OSBA_Feedback_European_Open_Digital_Ecosystems.pdf

ZenDiS (2025): Souveränitäts-Washing bei Cloud-Diensten erkennen. Warum Digitale Souveränität mehr ist als ein Standortversprechen. Whitepaper. https://www.zendis.de/media/pages/newsroom/publikationen/souveraenitaets-washing/87412539a0-1755243871/zendis-whitepaper-souveraenitaets-washing.pdf

Anmerkungen

1 *IT-Planungsrat (2021)*
2 *BSI & ZenDiS 2025, S. 11*
3 *ZenDiS 2025, S. 3*
4 *a. a. O.*
5 *Friedrich Merz beim EU-Gipfel zur europäischen Digitalen Souveränität im Nov. 2025, siehe https://bmds.bund.de/aktuelles/aktuelle-meldungen/detail/eu-summit-das-war-der-gipfel-zur-europaeischen-digitalen-souveraenitaet*
6 *https://commission.europa.eu/document/download/09579818-64a6-4dd5-9577-446ab6219113_en?filename=Cloud-Sovereignty-Framework.pdf*
7 *https://deutschland-stack.gov.de/gesamtbild/*
8 *OSBA 2026*
9 *OSBA 2025*
10 *https://www.it-planungsrat.de/beschluss/b-2026-03-it und https://www.it-planungsrat.de/fileadmin/beschluesse/2026/Beschluss_2026_03_Deutschland-Stack_Standards.pdf*
11 *https://www.zendis.de/unser-auftrag*
12 *https://opencode.de*
13 *BSI & ZenDiS 2025, S. 6*
14 *https://bmds.bund.de/aktuelles/pressemitteilungen/detail/open-source-rechtssicher-beschaffen*
15 *https://opencode.de/de/open-source*
16 *https://opencode.de/de/was-ist-opencode*
17 *https://www.schleswig-holstein.de/DE/landesregierung/ministerien-behoerden/I/Presse/PI/2024/CdS/241125_cds_open-source-strategie*
18 *https://www.schleswig-holstein.de/DE/landesregierung/ministerien-behoerden/I/Presse/PI/2025/cds/251014_cds_open-source-projekte*
19 *https://www.schleswig-holstein.de/DE/landesregierung/ministerien-behoerden/I/Presse/PI/2025/cds/251014_cds_open-source-projekte*
20 *https://www.schleswig-holstein.de/DE/landesregierung/ministerien-behoerden/I/_startseite/Artikel2025/IV/251204_cds_digitale_souveraenitaet*
21 *In Anlehnung an https://iso25000.com/images/figures/iso_25010_en.png*
22 *Blauer Engel 2020*

Ulrike Erb und Karin Vosseberg

Prof. Dr.-Ing. **Ulrike Erb** war bis März 2024 Informatik-Professorin an der *Hochschule Bremerhaven* mit dem Schwerpunkt Software Engineering. Zusammen mit einigen ihrer Informatik-Kolleg:innen führt sie weiterhin Projekte und Veranstaltungen zu den Themenbereichen Nachhaltigkeit in der IT und Digitale Souveränität durch. Sie engagiert sich außerdem im *FIfF e. V.* sowie in der *GI-Fachgruppe Frauen und Informatik*.
Homepage: *https://informatik.hs-bremerhaven.de/uerb/*

Prof. Dr.-Ing. **Karin Vosseberg** ist seit 2009 Professorin in den Studiengängen Informatik und Wirtschaftsinformatik an der *Hochschule Bremerhaven*. Ihr Schwerpunkt ist Software Engineering mit dem Fokus auf Qualität von Software. Ihr besonderes Interesse gilt der Frage, wie Nachhaltigkeit und digitale Souveränität als nichtfunktionale Qualitätskriterien in der Softwareentwicklung verankert werden können. Neben dem Engagement in der *GI-Fachgruppe Frauen und Informatik* und dem *FIfF* ist sie Vizepräsidentin im *ASQF*.
Homepage: *https://informatik.hs-bremerhaven.de/kvosseberg/*

Miriam Seyffarth, *OSBA*

Ist digitale Souveränität überhaupt erreichbar – und falls ja, wie?

Ein öffentlicher Briefwechsel zwischen dem BSI und der Open Source Business Alliance

Nach einem viel beachteten dpa-Interview der BSI-Präsidentin Claudia Plattner entspann sich im August 2025 ein öffentlicher Briefwechsel zwischen ihr und der Open Source Business Alliance über die Frage, ob digitale Souveränität in der Verwaltung überhaupt erreichbar ist, falls ja, wie, und welche Rolle das BSI hierbei spielen sollte.

Digitale Souveränität durch Open Source

Vor dem Hintergrund geopolitischer Spannungen ist digitale Souveränität das Gebot der Stunde – schließlich sind Wirtschaft, Verwaltung, Wissenschaft und Zivilgesellschaft in Deutschland massiv von der Software einzelner monopolartiger US-amerikanischer Hersteller abhängig. Die Angst wächst, dass schon morgen kein Zugriff mehr auf die genutzten Cloudsysteme oder die eigenen Daten möglich sein könnte, wenn die US-amerikanische Regierung es so will, oder dass sensible Daten von unbefugten Dritten abgegriffen werden könnten. Auch explodierende Lizenzkosten, mangelnde Transparenz und Anpassbarkeit der Software sowie abnehmende Innovations- und Wettbewerbsfähigkeit werden immer mehr zum Problem.

Unter digitaler Souveränität wird nach der Definition des IT-Planungsrates die Fähigkeit verstanden, die eigenen IT-Systeme unabhängig überprüfen, gestalten und austauschen zu können.[1] Open Source Software ermöglicht aufgrund der Transparenz des Quellcodes und der Freiheiten, die Open-Source-Lizenzen gewähren, auf einzigartige Weise digitale Souveränität im Sinne dieser Definition. Denn Open Source Software gewährleistet Kontroll- und Gestaltungsfähigkeit über die genutzten digitalen Infrastrukturen sowie Herstellerunabhängigkeit und Wechselfähigkeit.

Digitale Souveränität als strategisches Ziel der Bundesregierung

Die Bundesregierung hat sich daher wie auch die vorangegangenen Regierungen im Koalitionsvertrag zur Stärkung von digitaler Souveränität und Open Source Software verpflichtet:

> *„Digitalpolitik ist Machtpolitik. Wir wollen ein digital souveränes Deutschland. Dazu werden wir digitale Abhängigkeiten abbauen […] Wir definieren Ebenen übergreifend offene Schnittstellen, offene Standards und treiben Open Source mit den privaten und öffentlichen Akteuren im europäischen Ökosystem gezielt voran […]. Dafür richten wir unser IT-Budget strategisch aus und definieren ambitionierte Ziele für Open Source.“*[2]

Dieses strategische Vorhaben schlägt sich in verschiedenen Initiativen der Bundesregierung nieder. So beschlossen Bund und Länder im März 2026 für den Deutschland-Stack, dass vorrangig Open-Source-Lösungen zum Einsatz kommen sollen.[3] Offene Standards und Schnittstellen und eine Veröffentlichung der Software auf der Plattform openCode wurden ebenfalls festgeschrieben. Die gleichen Ziele wurden auch in der föderalen Modernisierungsagenda festgehalten.[4]

Im März 2026 veröffentlichten Bund und Länder zudem die neuen Open-Source-fähigen *EVB-IT*-Vertragsvorlagen.[5] Das sind Musterverträge, die der öffentlichen Hand die Softwarebeschaffung erleichtern sollen. Mit den neuen Vertragsvorlagen wird die öffentliche Beschaffung von Open Source Software vereinfacht, bei neu zu entwickelnder Software wird Open Source Software durch die neuen Musterverträge sogar zum Standard.

Die Beispiele zeigen, welchen wichtigen Stellenwert die Bundesregierung dem strategischen Ziel einräumt, durch den Einsatz von Open Source Software die digitale Souveränität von Wirtschaft und Verwaltung zu stärken.

Alle Behörden der Bundesregierung sind im Sinne des Koalitionsvertrages in der Pflicht, bei diesem Vorhaben mitzuwirken. Das gilt also auch für das Bundesamt für Sicherheit in der Informationstechnik (BSI), die zentrale Bundesbehörde in Deutschland für Fragen der IT-Sicherheit.

BSI-Präsidentin sät Zweifel

Umso mehr überraschte eine dpa-Meldung mit der Überschrift „BSI-Präsidentin: Digitale Souveränität für Deutschland vorerst unerreichbar“, die am 12. August 2025 über den Ticker ging. Diese Agenturmeldung mit Auszügen aus dem Interview, das die dpa mit der BSI-Chefin Claudia Plattner geführt hatte, wurde von vielen großen Medien wie der Süddeutschen Zeitung[6], der ZEIT[7] und heise[8] übernommen.

Plattner argumentiert in dem Interview, dass Deutschland die bestehenden digitalen Abhängigkeiten von außereuropäischen Cloud-Anbietern und anderen Softwareprodukten so bald nicht überwinden könne. Große Digitalunternehmen aus den USA hätten gut zehn Jahre Vorsprung was Investitionen anginge, es sei unrealistisch zu glauben, „dass wir das kurzfristig alles selbst können werden“. Und da diese Abhängigkeiten nun mal gegeben seien, müsse sich das BSI vorrangig darum kümmern, welche Kontrollmechanismen das BSI einrichten könne, um diese Closed-Source-Software aus dem Ausland so sicher wie möglich einzusetzen. Zu diesem Ziel hatte das BSI Anfang 2025 u. a. eine Kooperation mit *Google* geschlossen.

BSI-Kooperation mit US-Hyperscalern

Die Äußerungen der BSI-Chefin aus der dpa-Meldung stießen auf starken Widerspruch, sowohl bei den Mitgliedern der Open Source Business Alliance, dem größten Open-Source-Unternehmensverband in Europa, als auch in der allgemeinen Öffentlichkeit.

In einigen Reaktionen auf Social Media spiegelte sich neben dem Ärger über die Behauptung, digitale Souveränität sei nicht erreichbar, auch eine Frustration darüber, dass das BSI immer wieder Initiativen startet, die dem Ziel der digitalen Souveränität diametral entgegenzulaufen scheinen.

Unter einem *Linkedin*-Post von Claudia Plattner zu diesem Thema schrieb ein Nutzer zum Beispiel: „Bestehende Technologien von Hyperscalern zu nutzen ist bequem, aber ganz bestimmt nicht sicher […]. Die Strategie des BSI ist in meinen Augen extrem fragwürdig und wird es so lange bleiben, bis diese Vereinbarung mit Google endet."[9]

Die Kooperationsvereinbarung mit Google soll laut BSI dazu dienen, den sicheren Einsatz der *Public Cloud* des Hyperscalers in der deutschen Verwaltung sicherzustellen. Es sollen also bestehende Risiken u. a. mit Blick auf IT- und Datensicherheit nach Möglichkeit kontrolliert und minimiert werden. In vielen Behörden und auch in großen Teilen der Öffentlichkeit wird diese Kooperationsvereinbarung aber als Ritterschlag oder besondere Sicherheitsauszeichnung durch das BSI wahrgenommen. Eine Behörde, die eine Cloud-Lösung beschaffen muss, wird sich aufgrund der Zusammenarbeit mit dem BSI vielleicht eher für ein Produkt von Google entscheiden, da dieses als „durch das BSI besonders sicher geadelt" wirkt – auch wenn das BSI das ausdrücklich nicht so meint. Allein das Wort „Kooperationsvereinbarung" klingt weniger nach „Risikominimierung" und mehr nach „produktiver und erfolgreicher Zusammenarbeit." Eine alternative, transparente und digital souveränere Lösung eines anderen Unternehmens hingegen gilt einer Behörde im Vergleich dazu wohl erst mal als Unbekannte, wenn dieses Unternehmen im Gegensatz zu Google keine Kooperationsvereinbarung mit dem BSI vorweisen kann. Das BSI hat neben Google u. a. auch noch mit *Oracle* eine Kooperationsvereinbarung, eine Kooperation mit *AWS* ist geplant.[10]

Ein anderes Beispiel für die Zusammenarbeit des BSI mit einem US-Hyperscaler ist das Anfang 2026 vom BSI neu eingerichtete NIS-2-Meldeportal, das auf einer Cloud-Infrastruktur von Amazon Web Services (AWS) basiert. Im Rahmen der NIS-2-Umsetzung müssen sich knapp 30.000 Unternehmen und Behörden in Deutschland verpflichtend auf der Plattform registrieren.[11] An der Wahl von AWS für diese Plattform gab es breite Kritik: Das Portal soll sensible Daten der kritischsten Unternehmen in Deutschland entgegennehmen, dabei kann es laut Datenschutzerklärung der Plattform „zu einer Übermittlung der IP-Adresse in die USA kommen".[12]

Hierbei besteht u. a. die Gefahr, dass Unternehmen oder Bürger:innen davon absehen, das Meldeportal des BSI zu nutzen, da sie nicht sicher sein können, ob ihre sensiblen Daten sicher sind oder von unbefugten Dritten ausgelesen werden können. Und die Nutzung einer proprietären Cloud-Software, die nicht transparent kontrolliert oder unabhängig überprüft werden kann, und die zudem der US-amerikanischen Jurisdiktion des *CLOUD Act* und dem Zugriff der US-amerikanischen Regierung unterliegt, widerspricht in jeder Hinsicht den Zielen der Bundesregierung zur Stärkung der digitalen Souveränität aus dem Koalitionsvertrag.

Wer keine Alternativen sucht, wird auch keine finden

Durch die enge Zusammenarbeit des BSI mit US-amerikanischen Closed-Source-Unternehmen wie Google oder Amazon entsteht ein Henne-Ei-Problem: Das BSI postuliert, es gebe noch nicht genug verfügbare Alternativen und kooperiert daher weiterhin eng mit den Hyperscalern. Ohne entsprechende Nachfrage können alternative Angebote aber auch nicht wachsen oder in die Weiterentwicklung ihrer Produkte oder Marketing investieren – und das verstärkt wiederum das Narrativ, dass nicht ausreichend Alternativen vorhanden seien.

Ein anderer Nutzer verwies unter einem Linkedin-Post von Claudia Plattner auf dieses Henne-Ei-Problem und brachte die Sorge zum Ausdruck, dass die Äußerungen der BSI-Präsidentin Behörden oder Unternehmen davon abhalten könnten, sich überhaupt nach digital souveränen Alternativen umzuschauen: „Der Umstieg ist nicht einfach, so habe ich Angst, dass viele mit dem Argument ‚es gibt ja gar nichts' erst gar nicht anfangen zu suchen."[13]

Die enge Kooperation des BSI mit den US-Hyperscalern ist umso unverständlicher, da in Deutschland und Europa bereits verschiedene leistungsfähige und digital souveräne Open-Source-Cloud-Angebote wie zum Beispiel der *Sovereign Cloud Stack (SCS)* verfügbar sind.

Digitale Souveränität ist möglich!

Aus diesem Grund veröffentlichte die Open Source Business Alliance (OSBA) Ende August 2025 unter der Überschrift „Digitale Souveränität für Deutschland und Europa ist möglich!" einen offenen Brief an Claudia Plattner.[14] 60 Organisationen und Personen aus Wirtschaft und Zivilgesellschaft unterstützten den offenen Brief als Mitunterzeichner, um deutlich zu machen, dass digital souveräne Software-Alternativen schon heute verfügbar sind.

In ihrem offenen Brief griff die OSBA drei zentrale Punkte auf:

1. Wer behauptet, dass US-amerikanische Unternehmen mit ihrem Investitionsvorsprung der europäischen Digitalwirtschaft „zehn Jahre voraus" seien, spielt damit – willentlich oder unwillentlich – genau in die Karten der Big-Tech-Unternehmen, die gar nicht wollen, dass Deutschland und Europa eigene, unabhängige Software-Alternativen aufbauen. Das Narrativ, dass es ohnehin schon zu spät sei, verhindert Initiative und Innovation, verstärkt im Zweifel bestehende *Lock-In*-Effekte, und sendet ein fatales Signal an Öffentlichkeit, Politik und Verwaltung. Dabei hat der Staat mehr Spielraum als er selbst manchmal glaubt. Das Beispiel Schleswig-Holstein zeigt, dass es primär vom politischen Willen abhängt, ob Abhängigkeiten abgebaut werden und gezielt in den Aufbau von Alternativen investiert wird.

   Zudem gibt es zahlreiche Beispiele aus der Tech-Branche wie das Aufkommen generativer KI oder auch den Launch von *DeepSeek*, die zeigen, dass es alle paar Jahre eine große Dis-

ruption oder unerwartete Innovationen gibt, die den Markt ganz grundsätzlich umwälzen. Das beweist: Die vermeintlich in Stein gemeißelte Vorherrschaft einzelner Software-Lösungen oder Unternehmen ist genauso vergänglich wie alles andere auf der Welt.

2. Es gibt keinen Zwang, weiter mit den US-Hyperscalern zu kooperieren, auch wenn Politiker:innen oder Behörden wie das BSI das manchmal so empfinden. Digital souveräne Open-Source-Alternativen sind in vielen zentralen Bereichen wie Cloud, *Low-Code*, Kommunikation und Kollaboration usw. bereits verfügbar und einsatzbereit. Etliche dieser Lösungen sind bereits heute weit verbreitet und werden weltweit von hunderten Behörden, Unternehmen und anderen Organisationen erfolgreich eingesetzt. Sie reduzieren Abhängigkeiten und ermöglichen eine volle Kontrolle über die verarbeiteten Daten.

   Mit Blick auf das Henne-Ei-Problem und die Wahrnehmung, dass es noch nicht genug Alternativen gebe, sind strategische Investitionen des Staates in Open Source Software und offene Standards vonnöten. Eine gezielte Nachfrage nach Open Source bei Beschaffungsverfahren der öffentlichen Hand stärkt das deutsche und europäische Open-Source-Ökosystem und damit auch die lokale Wirtschaft sowie den Kompetenzaufbau. Wenn der Staat Open Source in den Ausschreibungen verlangt, liefert die IT-Branche. Und die Verwaltung wird merken, dass bereits mehr Alternativen vorhanden sind, als sie bisher dachte. Das BSI muss gemeinsam mit der restlichen Bundesverwaltung planvoll den Abbau der bestehenden Abhängigkeiten vorantreiben und Alternativen aufbauen und einsetzen.

3. Der Koalitionsvertrag der Bundesregierung gibt ganz klar vor, dass Abhängigkeiten abgebaut und Open Source zur Stärkung der digitalen Souveränität eingesetzt werden soll. Bundesdigitalminister Dr. Karsten Wildberger hat bei verschiedenen Gelegenheiten öffentlich erklärt, Open Source und offene Standards zum Leitprinzip in der IT-Architektur des Bundes machen zu wollen. Diesen Ankündigungen müssen Taten folgen. Es wäre falsch, mit Blick auf die Abhängigkeiten von den Hyperscalern zu resignieren. Denn digitale Souveränität für Deutschland ist möglich. Man muss sie nur wollen und beherzt vorantreiben.

Frau Claudia Plattner
Bundesamt für Sicherheit in der Informationstechnik BSI
Godesberger Allee 87
53175 Bonn

OSBA
Open Source
Business Alliance

Digitale Souveränität für Deutschland und Europa ist möglich!

Sehr geehrte Frau Plattner,

wir nehmen Bezug auf Ihre Aussagen gegenüber der dpa, die in vielen Medien veröffentlicht wurden. Ihre Beschreibung des Ist-Zustands ist in Teilen korrekt: Deutschland ist in zentralen Feldern von US-Anbietern abhängig und kurzfristig ist selbstverständlich mehr Kontrolle und Risikobegrenzung notwendig. Aber: Digitale Souveränität ist erreichbar und die Voraussetzung für unsere Sicherheit, wirtschaftliche Stärke und die eigenständige Gestaltung unserer Zukunft. Wenn wir uns ständig allein mit Schadensbegrenzung abmühen, kommen wir aus der misslichen Lage der erdrückenden Abhängigkeiten nicht heraus.

Ihre Aussage, US-amerikanische Unternehmen seien in Bezug auf Investitionen „zehn Jahre voraus", wiederholt in dieser Pauschalität ein Marketing-Narrativ, das häufig mit dem Ziel angewandt wird, Wirtschaft und Verwaltung vom Einkauf europäischer Lösungen abzuhalten. Dieses Argument wird politisch häufig als Begründung herangezogen, um dringend notwendige Beschaffungs- und Investitionsentscheidungen zu vertagen. In Wirklichkeit könnten viele Abhängigkeiten kurzfristig abgebaut werden, wenn die Politik vorhandene Lösungen auch aus Europa gezielt in Ausschreibungen berücksichtigen und fördern würde.

Offene, funktionierende Alternativen und starke europäische Anbieter gibt es etwa in den Bereichen Cloud, Low-Code, Kommunikation und Kollaboration, BPM, KI und vielen mehr. Etliche dieser offenen Technologien sind bereits heute weit verbreitet und werden von hunderten Behörden sowie Unternehmen und anderen Organisationen weltweit erfolgreich eingesetzt. Sie reduzieren so Abhängigkeiten und behalten volle Kontrolle über Daten.

Was wir strategisch brauchen, sind gezielte Investitionen in Open Source Software und eine Ausgabenpolitik der öffentlichen Hand, die Nachfrage nach offenen, europäischen Lösungen schafft. Nur so kann ein belastbares Ökosystem entstehen, das Abhängigkeiten tatsächlich reduziert, statt sie nur zu verwalten. Praxistaugliche Kriterien für eine solche Beschaffung liegen vor; als Unternehmen und Verbände der Digitalwirtschaft und Zivilgesellschaft bringen wir dazu seit Jahren konkrete Vorschläge ein.

Der offene Brief der OSBA an das BSI …

Die Antwort von Claudia Plattner

Claudia Plattner antwortete postwendend auf den offenen Brief der OSBA und veröffentlichte ihr Antwortschreiben auch auf der BSI-Webseite.[15] In ihrer Antwort stellte sie zunächst klar, dass die dpa sie falsch zitiert habe, sie habe nie gesagt, dass sie digitale Souveränität grundsätzlich für unerreichbar halte. Einige Punkte aus dem Schreiben von Claudia Plattner lohnen eine besondere Betrachtung.

Plattner betont in ihrem Brief: „Die Aufgabe des BSI besteht nicht darin, Beschaffungsentscheidungen zu treffen". Das ist zwar grundsätzlich richtig, blendet aber aus, dass das BSI an vielen Stellen Entscheidungen trifft, die starken Einfluss auf Beschaffungs- und Vergabeverfahren sowie größere politische Entwicklungen und Diskurse haben. Es wirkt fast ein bisschen so, als wollte Plattner das BSI als unpolitische Behörde darstellen, die sich nur um IT-Sicherheit kümmert, und sich ansonsten aus politischen Fragen raus hält – und mit der Forderung nach einem verstärkten Einkauf und Einsatz von Open Source gar nichts zu tun hat.

Aber natürlich ist jede Entscheidung des BSI politisch und wird von Wirtschaft, Politik, Verwaltung und der Öffentlichkeit auch als solche wahrgenommen. Von der Kooperationsvereinbarung mit Google über das neue NIS-2-Meldeportal bis zu der Äußerung, dass US-Digitalunternehmen um zehn Jahre voraus seien, beeinflussen alle diese Handlungen, wie das Thema digitale Souveränität in der Öffentlichkeit wahrgenommen wird.

… und die Liste der Unterzeichner

Die Doppelstrategie des BSI zur digitalen Souveränität

Die BSI-Chefin erklärt in ihrer Antwort noch einmal die Doppelstrategie des BSI, mit der digitale Souveränität angestrebt werden soll: Zum einen müsse „der europäische Markt und die hiesige Digitalindustrie" gestärkt werden. Zum anderen müssten „außereuropäische Produkte bei Bedarf technisch angepasst oder eingebettet werden, so dass eine sichere und selbstbestimmte Nutzung möglich wird."

Im Klartext bedeutet das: Ja, es gibt digital souveräne Alternativen, und diese sollen gestärkt werden. Aber Plattner rückt eben auch nicht von ihrem Kooperationsansatz mit den US-Hyperscalern ab. Das wirkt in Teilen widersprüchlich – oder wie eine Souveränitätsstrategie mit angezogener Handbremse.

Und so kommentiert auch ein Nutzer auf Social Media unter einem Mastodon-Post des BSI: „Eine Doppelstrategie ist problematisch, weil's kein vollständiges Commitment zu Open Source Software ist. Dass Unternehmen wie Microsoft qua *CLOUD Act* nicht in der Lage sind, sich an DSGVO und Bundesdatenschutzgesetz zu halten und dies mit der staatlichen Sorgfaltspflicht nicht vereinbar ist, wissen die Behörden auch nicht erst seit gestern!"[16] Ein anderer Nutzer argumentiert ähnlich: „Ich verstehe noch nicht, wie man bei der Doppelstrategie irgendeine Form von seriöser Kontrolle über Closed Source Software erlangen will. Insbesondere wenn diese gleichzeitig Updates erhalten soll. Wie soll man verhindern, dass ein Anbieter da (evtl. per Update) Funktionalität reduziert oder ganz einstellt?"[17]

Und selbst, wenn man Plattners Konzept der Doppelstrategie zunächst als gegeben annimmt, bleibt doch das Gefühl, dass diese in der Praxis sehr unausgewogen ist. Müssten die beiden Stränge der Doppelstrategie nicht mindestens gleich wichtig sein, bzw. müsste der Aufbau von digital souveränen Alternativen nicht mit deutlich mehr Intensität und Ressourcen vorangetrieben werden als die Zusammenarbeit mit US-Hyperscalern? Bei dem, was in der Öffentlichkeit von den Aktivitäten des BSI ankommt, entsteht der Eindruck *US-Hyperscaler first, digital souveräne Alternativen second*.

Das BSI muss sich deutlich engagierter als bisher auf den zweiten Teil der Doppelstrategie konzentrieren. Dazu gehört auch ein enger Austausch mit der Open-Source-Branche und eine intensivere Unterstützung von lokalen Unternehmen bei der Verbesserung ihrer IT-Sicherheit und dem Aufbau lokaler Fachkompetenz. Plattner schreibt in ihrer Antwort an die OSBA: „Wir haben hier bei uns in Europa durchaus einige Unternehmen, die sich anschicken, einen Unterschied zu machen, und in einigen Feldern auch bereits dabei sind, aufzuschließen. Die gilt es zu unterstützen!" Jetzt muss das BSI die Frage beantworten, wie diese Unterstützung konkret aussehen soll.

Ein unterschiedliches Verständnis von digitaler Souveränität

In der Debatte spiegeln sich auch verschiedene Auffassungen davon, wie digitale Souveränität eigentlich definiert ist. Claudia Plattner baut ihre Argumentation in erster Linie auf dem Aspekt der Wahlfreiheit auf: Am wichtigsten sei es, dass man zwischen verschiedenen Software-Produkten auswählen könne. In ihrer Antwort schreibt sie: „Resilienz – und mit ihr untrennbar verbunden Digitale Souveränität – bedeutet für uns als BSI vor allem, Optionen zu haben: Je mehr vertrauenswürdige Produkte verfügbar sind, desto souveräner können wir entscheiden."[18]

Wenn man dieser Sichtweise folgt, ist es naheliegend, dass die immer wiederkehrende Kooperation mit den US-Hyperscalern als gar nicht so problematisch empfunden wird. Schließlich hat man eine Wahl und entscheidet sich halt aus – pragmatisch empfundenen – Gründen immer wieder für die US-Konzerne.

Als OSBA fußt unser Verständnis von digitaler Souveränität wie eingangs dargestellt auf der Definition des IT-Planungsrates: Wechselmöglichkeit, Gestaltungsfähigkeit und Einflussnahme sind hierbei die zentralen Kriterien. Die Nutzung US-amerikanischer Closed-Source-Cloud-Lösungen trägt in dieser Hinsicht nichts zur digitalen Souveränität bei, da die Software nicht transparent ist, und es keine Möglichkeit zur Anpassung der Lösung gibt. Die Konzerne haben kein Interesse an einer Wechselfähigkeit, im Gegenteil: Das Forcieren von *Lock-In*-Effekten gehört untrennbar zum Geschäftsmodell.

Austausch zwischen BSI und OSBA

Claudia Plattner betont in ihrem Antwortschreiben, dass ihr die Zusammenarbeit mit Open-Source-Communities wichtig sei, und macht der OSBA ein konkretes Gesprächsangebot. In der Folge fand Anfang November 2025 ein erster konstruktiver Austauschtermin zwischen Claudia Plattner, dem OSBA-Vorsitzenden Peter Ganten, sowie weiteren Mitarbeitenden der beiden Organisationen statt. Dabei ging es u. a. darum, dass das BSI im

Miriam Seyffarth

Miriam Seyffarth leitet seit Anfang 2022 die Politische Kommunikation bei der *Open Source Business Alliance*. Von 2016 bis 2021 arbeitete sie als wissenschaftliche Mitarbeiterin und Büroleiterin der Bundestagsabgeordneten Tabea Rößner und betreute in dieser Funktion diverse bundespolitische Digitalthemen.

Rahmen seiner Doppelstrategie mehr Fokus auf Open-Source-Lösungen legen sollte.

Der öffentliche Briefwechsel und die nachfolgenden Austauschtermine haben die Debatte vorangebracht und Positionen geschärft. Und sie haben gezeigt: Es ist wichtig, klar und deutlich für Überzeugungen einzustehen und die Bundesregierung daran zu erinnern, warum digitale Souveränität wichtig ist und wie sie erreicht werden kann.

Wir hoffen, dass wir dem BSI Impulse geben konnten, sich selbst kritischer zu hinterfragen, die richtigen Prioritäten zu setzen und nicht so resigniert auf die bestehenden Abhängigkeiten zu schauen.

Anmerkungen

1 *IT-Planungsrat 2021: Strategie zur Stärkung der Digitalen Souveränität für die IT der Öffentlichen Verwaltung [online]. https://www.it-planungsrat.de/fileadmin/beschluesse/2021/Beschluss2021-09_Strategie_zur_Staerkung_der_digitalen_Souveraenitaet.pdf [abgerufen am 13.4.2026].*

2 *CDU, CSU, SPD 2025: Verantwortung für Deutschland. Koalitionsvertrag zwischen CDU, CSU und SPD [online]. https://www.koalitionsvertrag2025.de/sites/www.koalitionsvertrag2025.de/files/koav_2025.pdf [abgerufen am 13.4.2026].*

3 *Bundesministerium für Digitales und Staatsmodernisierung 2026: Deutschland-Stack. Sachstand [online]. https://bmds.bund.de/fileadmin/BMDS/Dokumente/260129_Deutschland-Stack_Standard_barrierefrei.pdf [abgerufen am 13.4.2026].*

4 *Bundesregierung 2025: Besprechung des Bundeskanzlers mit den Regierungschefinnen und Regierungschefs der Länder am 4. Dezember 2025[online]. https://www.bundesregierung.de/resource/blob/975228/2397654/c57248be7fa2d61ab6d8b12c0f29f05b/2025-12-04-mpk-staatsmodernisierung-data.pdf?download=1 [abgerufen am 13.4.2026].*

5 *Open Source Business Alliance 2026: Neue EVB-IT-Vertragsvorlagen stärken die Beschaffung von Open Source Software durch die Verwaltung [online]. https://osb-alliance.de/pressemitteilungen/neue-evb-it-vertragsvorlagen-staerken-die-beschaffung-von-open-source-software-durch-die-verwaltung [abgerufen am 13.4.2026].*

6 *Annette Riedl/dpa 2025: Digitale Souveränität für Deutschland vorerst unerreichbar [online]. https://www.sueddeutsche.de/politik/it-sicherheit-digitale-souveraenitaet-fuer-deutschland-vorerst-unerreichbar-dpa.urn-newsml-dpa-com-20090101-250812-930-900852 [abgerufen am 13.4.2026].*

7 *Alexander Eydlin/dpa 2025: BSI beklagt deutsche Abhängigkeit von digitalen US-Technologien [online]. https://www.zeit.de/digital/2025-08/digitale-souveraenitaet-bsi-abhaengigkeit-usa [abgerufen am 13.4.2026].*

8 *Anne-Béatrice Clasmann/dpa: BSI-Präsidentin: Digitale Souveränität für Deutschland vorerst unerreichbar [online]. https://www.heise.de/news/BSI-Praesidentin-Digitale-Souveraenitaet-fuer-Deutschland-vorerst-unerreichbar-10517756.html [abgerufen am 13.4.2026].*

9 *Christian Höffner 2025: Linkedin-Post [online]. https://www.linkedin.com/feed/update/urn:li:ugcPost:7366088941680095232?commentUrn=urn%3Ali%3Acomment%3A%28ugcPost%3A7366088941680095232%2C7363895093131714 57%29&dashCommentUrn=urn%3Ali%3Afsd_comment%3A%2873663895093131714 57%2Curn%3Ali%3AugcPost%3A7366088941680095232%29 [abgerufen am 13.4.2026].*

10 *BSI 2025: Cloud Computing: BSI und Schwarz Digits planen Kooperation [online]. https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2025/250318_BSI_Resilienz_Cloud-Loesung.html [abgerufen am 13.4.2026].*

11 *BSI 2026: Zweiter Schritt zur NIS-2-Registrierung: BSI-Portal ab sofort freigeschaltet [online]. https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2026/260601_NIS2_BSI-Portal.html [abgerufen am 13.4.2026].*

12 *Tobias Glemser 2026: Das Meldeportal in der AWS-Cloud: Warum nur, BSI? [online]. https://www.heise.de/meinung/Das-Meldeportal-in-der-AWS-Cloud-Warum-nur-BSI-11142071.html [abgerufen am 13.4.2026].*

13 *Carsten Mickeleit 2025: Linkedin-Post [online]. https://www.linkedin.com/feed/update/urn:li:ugcPost:7366088941680095232?commentUrn=urn%3Ali%3Acomment%3A%28ugcPost%3A7366088941680095232%2C7371887435414253568%29&dashCommentUrn=urn%3Ali%3Afsd_comment%3A%2873718874354142 53568%2Curn%3Ali%3AugcPost%3A7366088941680095232%29 [abgerufen am 13.4.2026].*

14 *Open Source Business Alliance 2025: Offener Brief an Claudia Plattner (BSI): Digitale Souveränität für Deutschland und Europa ist möglich! [online]. https://osb-alliance.de/pressemitteilungen/offener-brief-claudia-plattner-bsi-digitale-souveraenitaet-ist-moeglich [abgerufen am 13.4.2026].*

15 *Claudia Plattner 2025: Antwortbrief von -Präsidentin Claudia Plattner an die Open Source Business Alliance (OSBA) vom 26.8.2025 [online]. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Presse/Antwort_offenerBrief_OSBA.pdf.html [abgerufen am 13.4.2026].*

16 *Kevin Karhan 2025: Mastodon-Post [online]. https://infosec.space/@kkarhan/115095359777123482 [abgerufen am 13.04.2026].*

17 *T_X 2025: Mastodon-Post [online]. https://chaos.social/@T_X/115099155218234138 [abgerufen am 13.4.2026].*

18 *Claudia Plattner 2025: Antwortbrief von -Präsidentin Claudia Plattner an die Open Source Business Alliance (OSBA) vom 26.8.2025 [online]. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Presse/Antwort_offenerBrief_OSBA.pdf.html [abgerufen am 13.4.2026]*

OSBA | Open Source Business Alliance

Veranstaltung der OSBA zum Thema Souveräner Arbeitsplatz in der Verwaltung, *Quelle: Pressematerial OSBA*

Claudia Plattner, *BSI*

Welt(un)ordnung im digitalen Raum: Cyber Dominance als Sicherheitsrisiko

Im Jahr 2026 regiert bei vielen von uns das Gefühl, dass in unserer Welt etwas Grundlegendes aus den Fugen geraten ist. Dieser Eindruck wird beinahe täglich von Verzerrungen genährt, die wir vor nicht allzu langer Zeit nur aus dystopischen Romanen oder Filmen kannten. Was nach und nach ins globale Bewusstsein rückt, ist die Tatsache, dass Technologie die Kräfteverhältnisse zunehmend beeinflusst: Neben militärischer Stärke und wirtschaftlicher Macht ist die digitale Sphäre zu einer eigenständigen Weltordnungs-Dimension geworden.

Im Spannungsfeld von Geopolitik, wirtschaftlicher Rezession und multidimensionalen Abhängigkeiten erkennen wir die gefährliche Übermacht von Tech-Eliten, erleben wir, wie unsere Normen erodieren, und müssen wir feststellen, dass unsere Demokratie in Bedrängnis gerät. Im digitalen Raum geschieht das in Form von Cyber-Aggression: Deutschland und Europa stehen unter dem permanenten Druck von *Cyber Crime* (Straftaten im digitalen Raum, die vorrangig aus finanziellen Motiven begangen werden), *Cyber Conflict* (staatlich gelenkte Angriffe mit ideologischem, politischem oder militärischem Hintergrund) und *Cyber Dominance* (Möglichkeit von Herstellern digitaler Produkte, dauerhaft Zugriff auf die Systeme und Daten ihrer Kunden zu behalten).

Insbesondere die letztgenannte Bedrohungsart ist in den vergangenen Monaten mehr und mehr ins gesellschaftliche Bewusstsein gerückt. Die Liste der Produkte, die entsprechende Risiken mit sich bringen, ist leider nicht kurz: Die empfindlichen Abhängigkeiten, die uns im Ernstfall verwundbar machen, betreffen Themen wie Mobilfunk, die Energiewende und eine Vielzahl digitaler Produkte und Dienste, die wir tagtäglich nutzen – etwa Betriebssysteme mobiler Endgeräte, Social-Media-Angebote oder Cloud-Dienste. Cyber Dominance hat aber noch viel weitreichendere Ausprägungen: Angesichts neuer KI-Modelle, die in Sekundenschnelle Sicherheitslücken in Software-Produkten aufspüren können, stehen wir vor einem Paradigmenwechsel in der Cybersicherheitslandschaft. Es stellt sich die Frage, ob – und wenn ja, wie lange – derart wirkmächtige Werkzeuge auf dem freien Markt verfügbar sein werden. Daraus wiederum ergeben sich Fragen nationaler wie europäischer Sicherheit und Souveränität.

Evident ist, dass der Schutz unserer Gesellschaft von unseren eigenen digitalen Fähigkeiten abhängt. Um die Verteidigung im digitalen Raum sicherzustellen, muss Deutschland parallel zu einem automatisierten Cyberschutz die eigene Digitalisierung strategisch voranbringen. Deshalb gilt es, einen strategischen Ansatz zu finden, der folgende Fragen beantwortet: Welche digitalen Technologien wollen und können wir einfach einkaufen und *out of the box* verwenden? Für welche digitalen Technologien streben wir für Teile der digitalen Wertschöpfungskette die globale Exzellenz aus nationaler oder europäischer Hand an? Welches sind die außereuropäischen Technologien, die wir vorerst weiterverwenden wollen und die technisch so *veredelt* werden können, dass die Kontrolle über Daten und Steuerung bei uns liegt?

Doppelstrategie

Um digitalen Innovationen nicht nur gerecht zu werden, sondern sie auch voranzutreiben und dabei gleichzeitig die digitale Souveränität zu stärken, verfolgen wir als Cybersicherheitsbehörde Deutschlands eine Doppelstrategie:

Uns allen ist klar, dass der europäische Markt und die hiesige Digitalindustrie in wichtigen Technologiefeldern gestärkt werden müssen. Dabei hilft das BSI im Bereich der Cybersicherheit aktiv mit. Gleichzeitig müssen außereuropäische Produkte – überall dort, wo wir diese weiterhin verwenden wollen – durch so genannte Kontrollschichten so abgesichert werden, dass eine selbstbestimmte Nutzung möglich wird.

Nationale und europäische Anbieter unterstützen wir zum Beispiel dabei, Systeme und Architekturen zu entwickeln, die für Bundes- und Landesbehörden nutzbar gemacht werden können – das betrifft auch und gerade den Umgang mit sensiblen Informationen. So haben wir den Messenger-Dienst Wire in einer speziellen Version (*Wire Bund*) für den Einsatz in der Bundesverwaltung zugelassen – auch für Verschlusssachen auf der Ge-

Claudia Plattner

Claudia Plattner ist seit dem 1. Juli 2023 Präsidentin des *Bundesamtes für Sicherheit in der Informationstechnik* (BSI). Claudia Plattner wurde 1973 in Mainz geboren. Sie verfügt über mehr als 20 Jahre Erfahrung in IT-Funktionen für Unternehmen und Institutionen. Zuletzt war sie Generaldirektorin für Informationssysteme bei der *Europäischen Zentralbank* und zuvor als Chief Information Officer (CIO) der *DB Systel GmbH*, dem internen IT-Dienstleister der Deutschen Bahn, in leitender Funktion tätig. Claudia Plattner ist Diplom-Mathematikerin (TU Darmstadt) und hat einen Master-Abschluss in Angewandter Mathematik der Tulane University (USA). *Quelle: BMI, Foto: BMI/Henning Schacht*

heimhaltungsstufe *Nur für den Dienstgebrauch*. Wire ermöglicht sichere Kommunikation, Dateiaustausch und Videokonferenzen – mobil und auf dem Desktop. Mit Blick auf Cloud-Dienste helfen wir nationalen und europäischen Providern dabei, ihre Produkte ebenfalls für die Speicherung und Verarbeitung besonders schützenswerter Daten abzusichern – dafür schauen wir auf Basis von Kooperationsvereinbarungen tief in den Quellcode.

C3A – Criteria enabling Cloud Computing Autonomy

Erst kürzlich hat das BSI mit den *C3A – Criteria enabling Cloud Computing Autonomy* – einen richtungsweisenden Handlungsrahmen vorgelegt, der die Souveränitätseigenschaften von Cloud-Diensten transparent macht. Während die Sicherheitseigenschaften von Cloud-Diensten im *Cloud Computing Compliance Criteria Catalogue (C5)* des BSI adressiert werden, ermöglicht der Kriterienkatalog C3A eine Bewertung, ob ein Cloud-Angebot im jeweiligen Risikokontext selbstbestimmt genutzt werden kann. Die C3A können sowohl von Cloud-Anbietern als auch von Cloud-Kunden genutzt werden. Cloud-Anbieter können die Einhaltung der Kriterien durch ein Audit nachweisen. Cloud-Kunden können das Framework nutzen, um für das eigene Nutzungsszenario relevante Anforderungen zu identifizieren und so ihr angestrebtes Maß an Souveränität festlegen.

Hinsichtlich außereuropäischer Produkte ist in diesem Kontext unser Ziel, das Kontrollschichten-Prinzip für kritische Produktsparten fruchtbar zu machen und mit möglichst vielen Herstellern umzusetzen. So kann etwa eine geeignete Ausgestaltung der Sicherheitsarchitektur einschließlich Verschlüsselung und externem Schlüsselmanagement den Klartextzugriff durch den Cloud Service Provider selbst unterbinden. In diesem Falle wären Daten beispielsweise auch gegenüber Anfragen auf Basis des CLOUD Act geschützt, da dem Cloud Service Provider technisch die Möglichkeit entzogen ist, sich Zugang zu den geforderten Daten zu verschaffen.

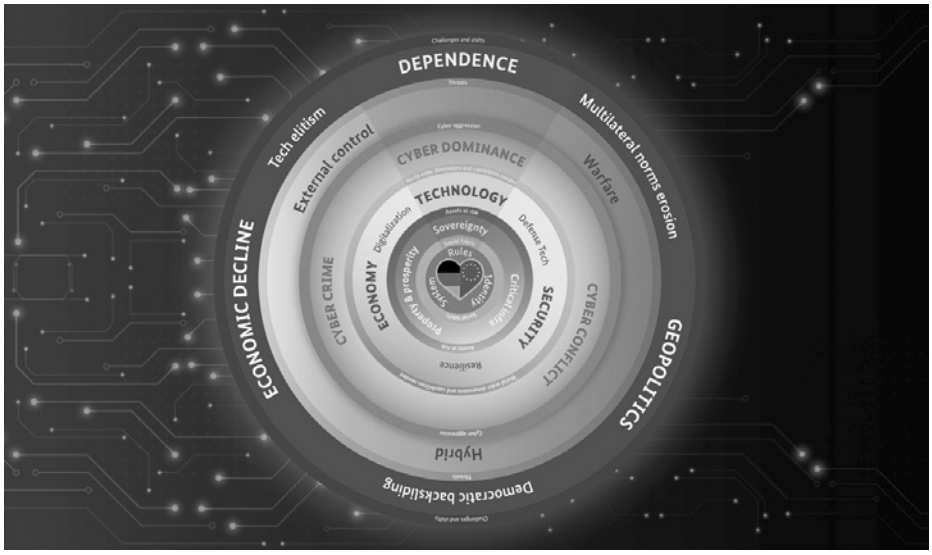
Natürlich liegt hier noch viel Arbeit vor uns, teilweise auch Grundlagen- und Forschungsarbeit. Schon jetzt ist aber klar: Digitale Souveränität bedeutet aus Sicht des BSI, Optionen zu schaffen. Denn je mehr vertrauenswürdige Produkte verfügbar sind, desto souveräner kann entschieden werden und desto sicherer wird die digitale Zukunft. Die Aufgabe des BSI besteht dabei übrigens nicht darin, Beschaffungsentscheidungen zu treffen, sondern darin, den Faktor Cybersicherheit für bestehende ebenso wie für künftige Produkte zu fördern und einzufordern – und damit Resilienz, die auch Souveränität umfasst, in die Fläche zu bringen. Um dieses Ziel zu erreichen, arbeiten wir mit nationalen, europäischen und internationalen Herstellern ebenso wie mit Open Source Communities zusammen.

Open Source strategisch stärken

Um Open Source strategisch zu stärken, haben wir ein BSI-eigenes *Open Source Program Office (OSPO)* gegründet. Dort laufen derzeit Pilotprojekte, die darauf abzielen, Open-Source-Produkte nicht nur im Verwaltungs-Backend, sondern auch in Verwaltungs-Workplaces stark zu machen. Doch mit der Stärke wächst die Verantwortung: Open Source betrachten wir nicht als Software zum Nulltarif – sondern als Produkte, deren Nutzerinnen und Nutzern eine gewisse Verantwortung zuteil wird, wenn es um Lebenszyklusmanagement oder Sicherheitsupdates geht. Und die Anforderungen werden steigen. Die bereits erwähnten KI-geboosteten Schwachstellen-Suchmaschinen werden auch den Druck auf das Open-Source-Ökosystem exponentiell erhöhen. Open Source stark machen heißt deshalb auch: Open Source sicher halten. Diese Verantwortung lässt sich nicht delegieren – sie liegt bei uns allen.

Fazit

Deutschland und Europa können digital souverän und wehrhaft werden – aber nur, wenn wir das gemeinsam angehen. Staat, Wirtschaft, Wissenschaft und Gesellschaft – Behörden, Hersteller, Tech-Communities: Wir müssen an einem Strang ziehen und das vorhandene Potenzial pragmatisch nutzen. Kluge, anwenderfreundliche Standards können dabei Sicherheit und Souveränität zu echten Wachstumsfaktoren machen. Und smarte Regulierung schafft Planungssicherheit, ohne Innovationen aus Europa zu bremsen.



***Wheel of Distortion**: Welt(un)ordnung im digitalen Raum – ein von Claudia Plattner entwickeltes Modell*
Quelle: Claudia Plattner, https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Blog/Wheel_of_Distortion_250213.html

Lea Beiermann, *ZenDiS*

Wie digital (un)abhängig ist die öffentliche Verwaltung? Kriterien zur Bewertung Digitaler Souveränität

Die Digitale Souveränität der öffentlichen Verwaltung wurde durch den IT-Planungsrat (IT-PLR) anhand dreier strategischer Ziele definiert: Wechselmöglichkeit, Gestaltungsfähigkeit und Einfluss auf IT-Anbieter. Das Zentrum Digitale Souveränität (ZenDiS) übersetzt diese Ziele in konkrete Prüfkriterien – und einen Souveränitätscheck. Grundlage ist ein offener Konsultationsprozess mit allen Interessierten aus Verwaltung, Wissenschaft, Wirtschaft und Zivilgesellschaft.

Warum braucht es Kriterien für Digitale Souveränität? Die öffentliche Verwaltung kann heute selbst in wesentlichen Bereichen häufig keine unmittelbare Kontrolle über ihre digitale Infrastruktur ausüben. Bei Bürosoftware sowie Arbeitsplatz- und Serverbetriebssystemen zeigte eine Marktanalyse 2019, dass 96 % der in Bundesbehörden eingesetzten Büro-Softwarelösungen von nur einem Anbieter stammen – ähnlich starke Abhängigkeiten gibt es auch im Bereich Cloud oder Virtualisierung.[1] Diese Monokultur der öffentlichen IT-Landschaft führt zu Lock-in-Effekten, erschwert den Anbieterwechsel und macht es schwierig für die Verwaltung, IT-Systeme eigenständig weiterzuentwickeln oder an spezifische eigene Anforderungen anzupassen.[2]

ZenDiS Zentrum Digitale Souveränität

Der verstärkte Einsatz cloudbasierter Software-as-a-Service-(SaaS-)Lösungen verlagert darüber hinaus Kontrolle über Software und Daten zunehmend an externe Anbieter. Gleichzeitig verändern sich Kostenstrukturen, da einmalige Investitionen um laufende Lizenz- und Nutzungsgebühren im Abomodell ergänzt werden. Das reduziert langfristig nicht nur die technische, sondern – gerade vor dem Hintergrund mangelnden Wettbewerbs in vielen Bereichen – auch die wirtschaftliche Steuerungsfähigkeit der öffentlichen Verwaltung. Hinzu kommen veränderte geopolitische Rahmenbedingungen: Weniger verlässliche internationale Partnerschaften lassen einen potenziellen Zugriff auf europäische Daten und Infrastruktur – beispielsweise durch den US Cloud Act – zunehmend realistisch erscheinen. Die Debatte um gesperrte E-Mail-Accounts und andere Online-Dienste von Mitarbeitenden des Internationalen Strafgerichtshofs (IStGH) im Rahmen von US-Sanktionen machte dieses Risiko 2025 deutlich sichtbar.[3]

Vor diesem Hintergrund hat der Begriff der Digitalen Souveränität enorm an Bedeutung gewonnen – und wird zunehmend inflationär verwendet: Hyperscaler verwenden den Begriff gern im Kontext ihrer Cloud-Angebote. Sie verweisen dabei auf Maßnahmen wie europäische Serverstandorte oder technisch isolierte Systeme und präsentieren ihre Angebote damit als souverän. Realität ist aber: Solche Ansätze adressieren einzelne Aspekte Digitaler Souveränität, greifen jedoch zu kurz, solange andere (beispielsweise rechtliche oder organisatorische) Abhängigkeiten bestehen bleiben. Belastbare Aussagen über Digitale Souveränität erfordern daher eine messbare Grundlage. Dabei geht es nicht nur um die Bewertung einzelner Softwarelösungen, sondern um die Frage, in welchem Umfang öffentliche Institutionen insgesamt ihre IT-Infrastruktur wählen und ihren Anforderungen entsprechend (mit)gestalten können.

Was Digitale Souveränität (nicht) ist

Infolge der Marktanalyse des Bundes-Stacks von 2019 entwickelte der IT-Planungsrat (IT-PLR) eine Strategie, um die langfristige Handlungsfähigkeit der öffentlichen Verwaltung zu sichern. Die Digitale Souveränität soll dabei in drei Dimensionen gestärkt werden: Wechselmöglichkeit, Gestaltungsfähigkeit und Einfluss auf IT-Anbieter.[4] Ziel ist, dass die öffentliche Verwaltung IT-Lösungen und -Anbieter flexibel wählen und mit vertretbarem Aufwand wechseln kann. Darüber hinaus soll sie in der Lage sein, IT-Lösungen aktiv mitzugestalten. Dafür sind sowohl technisches und organisatorisches Know-how innerhalb der Verwaltung als auch offene und anpassbare Technologien erforderlich. Darüber hinaus soll die öffentliche Verwaltung ihre Anforderungen gegenüber IT-Anbietern wirksam durchsetzen können, etwa in Bezug auf Vertragsgestaltung, Sicherheitsanforderungen oder Betriebsmodelle. Das Zentrum Digitale Souveränität (ZenDiS) wurde vom IT-PLR gegründet, um die öffentliche Verwaltung in genau diesen Bereichen zu stärken: indem Plattform, Produkte und Dienste bereitgestellt werden, die Wechselmöglichkeiten und Mitgestaltung fördern, sowie durch den Aufbau von Kompetenzen in der öffentlichen Verwaltung, die eine effektive Durchsetzung der eigenen Interessen ermöglichen.

Das Prinzip Digitale Souveränität ist dabei als Antwort auf kritische Abhängigkeiten in der öffentlichen Verwaltung zu verstehen, nicht aber im Sinne einer Abschottung von anderen. Autarkie ist nicht das Ziel, sondern es geht vielmehr darum, eine diverse IT-Landschaft zu schaffen, mit offenen, interoperablen Lösungen, die möglichst unabhängig von einzelnen Anbietern entwickelt und betrieben werden können. Voraussetzung ist, dass diese Anwendungen durch ein kompetentes Dienstleister-Ökosystem unterstützt werden, das zuverlässigen Support bietet und die öffentliche Verwaltung bei Betrieb und Weiterentwicklung unterstützen kann. Qualitäts- und sicherheitsgeprüfte Open-Source-Software bietet dazu *per default* die besten Voraussetzungen und ist ein zentrales Element der Strategie des IT-PLR und des ZenDiS.

Digitale Souveränität messbar machen

Derzeit fehlt eine belastbare Grundlage, um die Digitale Souveränität der öffentlichen Verwaltung systematisch zu bewerten. Mit dem *Cloud Sovereignty Framework* der Europäischen Union liegen zwar erste Kriterien zur Einordnung von Cloud-Diensten vor, für die Digitale Souveränität der Verwaltung auf Organisationsebene existiert jedoch bislang kein vergleichbarer Kriterienrahmen. Sie lässt sich daher derzeit weder verlässlich messen noch vergleichen oder gezielt steuern. Es braucht klar definierte, pra-

xisfähige Kriterien für Digitale Souveränität, um die Frage nach der Handlungsfähigkeit von öffentlichen Institutionen als Ganzes zu beantworten – einschließlich ihrer IT-Infrastruktur und der darauf aufbauenden digitalen Dienste. Nur durch eine solche organisationale Betrachtung kann Digitale Souveränität als Gesamtfähigkeit der jeweiligen Einrichtung erfasst werden. Eine Betrachtung einzelner Anwendungen würde die Wechselwirkungen und das Zusammenspiel der eingesetzten IT-Services – sowie Kompetenzen oder Beschaffungsprozesse – nicht ausreichend berücksichtigen. Auf Grundlage der strategischen Ziele des IT-PLR für Digitale Souveränität hat das ZenDiS Kriterien abgeleitet, anhand derer sich Behörden systematisch bewerten und vergleichen lassen.

Vorschlag für einen Kriterienkatalog

Der hier vorgeschlagene Kriterienkatalog des ZenDiS basiert auf den strategischen Zielen des IT-PLR und entspricht dem Stand von April 2026. Die Kriterien wurden bis Mitte Mai 2026 im Rahmen eines offenen Konsultationsprozesses durch das ZenDiS auf der Plattform *openCode (opencode.de)* zur Diskussion gestellt. Informationen zum bisherigen und weiteren Vorgehen sind auf souveränitätscheck.de zu finden.

A. Organisation und Fähigkeiten

Der Fokus dieser Kategorie liegt auf der Management- und Steuerungsfähigkeit der Organisation hinsichtlich der Anforderungen an digital souveräne Dienste. Ausgehend von der Organisation werden die Fähigkeiten zur Bewertung und Umsetzung Digitaler Souveränität für die genutzten digitalen Dienste eingeordnet. Hierzu werden folgende Bereiche betrachtet: Strategie, IT-Governance und Management, Risikomanagement, Beschaffung und Vergabe, Auftraggeberfähigkeit sowie Kompetenzen als Voraussetzung der Einflussnahme auf Anbieter.

B. Digitale Anwendungen und Dienste

Diese Kategorie schaut auf die Gestalt- und Austauschbarkeit von – sowie Kontrolle über – Anwendungen und Diensten. Die Kriterien überprüfen die Eigenschaften der Anwendung bzw. des digitalen Dienstes auf den Erfüllungsgrad der beschriebenen strategischen Ziele. Betrachtete Bereiche sind: Transparenz und Dokumentation, Nachvollziehbarkeit und Sicherheit der Lieferkette, Anwendungsarchitektur und Modularität, Standards und Schnittstellen, Abhängigkeiten auf Software-Ebene.

C. Informationen und Daten

Diese Kategorie prüft, inwieweit regulatorische, technische und betriebliche Bedingungen Datenhoheit und Datensouveränität gewährleisten. Hier werden die folgenden Bereiche betrachtet: Datenlokation, Datensicherheit, Datenschutz, Datenstrukturen.

D. Betrieb und Infrastruktur

Diese Kategorie bewertet die Rahmenbedingungen und die Durchführung des Betriebs. Folgende Bereiche werden betrachtet: Abhängigkeit auf Betriebs- bzw. Provider-Ebene, Kundenverhältnis, Exit-Fähigkeit, Resilienz und Business Continuity, Sicherheit und Compliance im Betrieb.

Strategische Ziele

- ● **Gestaltungsfähigkeit** = Fähigkeit, IT-Infrastruktur und digitale Dienste aktiv mitzugestalten und nach Bedarf anzupassen
- ■ **Wechselmöglichkeit** = Möglichkeit, IT-Lösungen, Komponenten und Anbieter flexibel auszuwählen und bei Bedarf mit vertretbarem Aufwand zu wechseln
- ◆ **Einflussnahme auf IT-Anbieter** = Fähigkeit, Anforderungen gegenüber Technologieanbietern wirksam zu vertreten

Kriterien zur Messung Digitaler Souveränität			
A	Organisation und Fähigkeiten		Ziel
A1	Strategie	Ist Digitale Souveränität in der Digitalstrategie und den übergeordneten Leitlinien der Organisation verankert?	● ◆
A2	IT-Governance & Management	Sind Verantwortlichkeiten, Prozesse und Steuerungsstrukturen im IT-Betrieb definiert und umgesetzt?	● ◆
A3	Risikomanagement	Werden technologische, organisatorische und strategische Risiken im Hinblick auf Abhängigkeiten erfasst und gesteuert?	● ■ ◆
A4	Beschaffung und Vergabe	Werden Beschaffungsprozesse so gestaltet, dass Wettbewerb, Offenheit und Alternativen berücksichtigt werden?	● ■ ◆
A5	Auftraggeberfähigkeit	Ist die Organisation in der Lage, IT-Projekte eigenständig zu steuern und Anbieter wirksam zu kontrollieren?	● ◆
A6	Kompetenzen	Verfügt die Organisation über die nötigen (IT-)Kenntnisse, Fachkräfte und Wissensbestände, um souverän handeln zu können?	● ■ ◆
B	Digitale Anwendungen und Dienste		Ziel
B1	Transparenz/ Dokumentation	Ist eine umfassende Dokumentation von Anwendungen hinsichtlich der Funktionalität, der Schnittstellen und der Datenstrukturen sowie des Zusammenspiels der Komponenten im Systemkontext mit anderen Anwendungen oder Diensten zum Zwecke der Nutzung, Auditierung, der Wartung und der Inbetriebnahme vorhanden?	● ■
B2	Nachvollziehbarkeit und Sicherheit der Lieferkette	Ist die Herkunft von Hardware- und Software-Komponenten der Organisation – einschließlich Herstellungsorte, beteiligter Länder, Anbieter außerhalb der EU und Transparenz der gesamten Lieferkette – bekannt und überprüfbar?	● ■
B3	Anwendungsarchitektur/ Modularität	Sind Anwendungen portabel und modular aufgebaut und technisch entkoppelbar?	● ■
B4	Standards	Nutzen Anwendungen offene Schnittstellen und etablierte Standards, um Austauschbarkeit und Integration zu ermöglichen?	● ■
B5	Abhängigkeit auf Software-Ebene	In welchem Umfang bestehen Lock-in-Risiken durch proprietäre Software oder fehlende Alternativen?	■ ◆

Kriterien zur Messung Digitaler Souveränität			
C	Daten		Ziel
C1	Datenlokation	Wo werden Daten gespeichert und verarbeitet (lokal, EU, Drittstaaten) und wie ist dies zu kontrollieren?	■ ◆
C2	Datensicherheit	Werden Daten umfassend verschlüsselt und gibt es entsprechende Konzepte sowie technische und organisatorische Maßnahmen, welche die Datensicherheit Ende-zu-Ende gewährleisten?	●
C3	Datenschutz	Werden rechtliche Vorgaben (z. B. DSGVO) eingehalten und durch technische sowie organisatorische Maßnahmen abgesichert?	● ◆
C4	Datenstrukturen	Sind Daten in offenen, interoperablen Formaten abgelegt, sodass Portabilität und Wiederverwendbarkeit gesichert sind?	● ■
D	Betrieb und Infrastruktur		Ziel
D1	Abhängigkeit auf Betriebs-/ Provider-Ebene	Wie stark ist die Bindung an einzelne Betreiber, Dienstleister oder Cloud-Anbieter und sind diese durch EU-Recht kontrollierbar?	■ ◆
D2	Kundenverhältnis	Erlaubt das Kundenverhältnis eine Einflussnahme auf Software-Entwicklung und digitale Dienste, beispielsweise durch eine transparente Release-Planung und aktivem Anforderungsmanagement?	● ◆
D3	Exit-Fähigkeit	Ist ein Anbieterwechsel oder Rückführung in Eigenbetrieb realistisch und erprobt?	■
D4	Resilienz & Business Continuity	Wie robust sind die Systeme gegenüber Ausfällen, Krisen oder Angriffen und wie schnell ist ein Wiederanlauf möglich?	●
D5	Sicherheit und Compliance im Betrieb	Werden regulatorische und organisatorische (EU-)Anforderungen im laufenden Betrieb durchgängig überprüft und eingehalten?	● ◆

Ausführliche Übersicht der Kriterien zur Messung digitaler Souveränität.

Eine risikobasierte Anwendung der Kriterien

Nicht jede IT-Komponente oder jeder Einsatzbereich bringt dieselben Risiken mit sich, daher ist eine risikobasierte Bewertung sinnvoll. Die Bewertung richtet sich beispielsweise nach dem konkreten Beschaffungsbedarf oder der Schutzbedarfsanalyse der betroffenen Daten. Dabei sollten insbesondere folgende Aspekte betrachtet werden:[5]

- Anforderungen an Vertraulichkeit, Integrität und Verfügbarkeit der Daten, die von der IT-Infrastruktur verarbeitet werden
- Einzuhaltende regulatorische Vorgaben, beispielsweise zum Datenschutz
- Grad der Abhängigkeit von einzelnen Anbietern oder proprietären Lösungen sowie die Möglichkeit einer Rückmigration zur Vermeidung von Lock-in-Effekten
- Technische und organisatorische Schutzmaßnahmen zur Sicherheit, bestehende Schwachstellen und Reifegrad der Sicherheitskontrollen
- Art, Umfang und Kritikalität der Prozesse, die auf die IT-Infrastruktur der Organisation angewiesen sind
- Stabilität und Integrität der Lieferkette

Souveränitätscheck

Die vorgeschlagenen Kriterien und Risikoaspekte dienen als Basis für einen Souveränitätscheck auf Behördenebene. Jedes Kriterium wird dabei über konkrete Prüffragen adressiert, sodass eine strukturierte Bewertung der Digitalen Souveränität möglich ist – etwa durch Fragen wie: „Sind Souveränitätsprinzipien fest in den Organisationszielen verankert?“ (Kategorie A) oder „Liegen erprobte Exit-Runbooks vor?“ (Kategorie D). Ergänzend werden zu jedem Kriterium geeignete Nachweise definiert, beispielsweise in Form von Dokumentation, Richtlinien, technischen Prüfberichten oder Zertifizierungen. Auf diese Weise lässt sich nachvollziehen, welche Anforderungen bereits erfüllt sind und an welchen Stellen noch Verbesserungsbedarf besteht. Dieser Souveränitätscheck wird aktuell auf Basis der Konsultation auf openCode durch das ZenDiS entwickelt (siehe souveränitätscheck.de), um ein anwendungsorientiertes Werkzeug bereitzustellen, mit dem sich die Digitale Souveränität in der Verwaltung fundiert bewerten lässt.

Anmerkungen

1 *PwC Strategy& (Germany) GmbH. (2019). Strategische Marktanalyse zur Reduzierung von Abhängigkeiten von einzelnen Software-Anbietern: Eine Studie im Auftrag des Bundesministeriums des Innern, für Bau und Heimat. Berlin.*

2 *Ibid.*

3 *Laaff, M. (2025, 23. Juli). Diese E-Mail ist unzustellbar: Was, wenn Donald Trump Big Tech zwingt, die Dienste in Europa abzuschalten? Lange war das Theorie. Dann ging eine wichtige Mailadresse am Strafgerichtshof nicht mehr. Die Zeit. https://www.zeit.de/digital/internet/2025-07/microsoft-email-sperre-karim-khan-donald-trump-istgh, zuletzt abgerufen am 19.03.2026.*

4 *Bundesministerium des Innern, für Bau und Heimat (BMI). (2021, Januar). Beschluss 2021/09: Strategie zur Stärkung der digitalen Souveränität für die IT der öffentlichen Verwaltung. Berlin. IT Planungsrat. https://www.it-planungsrat.de/fileadmin/beschluesse/2021/Beschluss2021-09_Strategie_zur_Staerkung_der_digitalen_Souveraenitaet.pdf*

5 *Bundesministerium des Innern und für Heimat. (2024). Anforderungen an Technologieanbieter und -lösungen(Beschluss Nr. 2024/01). https://www.cio.bund.de/SharedDocs/downloads/Webs/CIO/DE/cio-bund/steuerung-it-bund/beschluesse_cio-board/2024_01_Beschluss_CIO_Board_Technologieanbieter_Anlage.pdf*

Lea Beiermann

Lea Beiermann ist Partnership Lead im *Zentrum Digitale Souveränität* und verantwortet den strategischen Aufbau und die Pflege von Partnerschaften zwischen der öffentlichen Verwaltung und dem Open-Source-Ökosystem in Deutschland und Europa. Sie promovierte an der Universität Maastricht in Technikgeschichte und verfügt über umfassende Erfahrung in der Erwachsenenbildung, Unternehmens- und Technikkommunikation sowie im Community- und Partnermanagement.

Thilo Weichert, ***Digitalcourage e. V., DVD e. V.***

Wie souverän sind wir bei unseren Finanzdaten?

Während die Diskussion über digitale Souveränität generell in Europa langsam Fahrt aufnimmt, ist das Bewusstsein über die Abhängigkeit und Verletzlichkeit unseres Finanzsystems von US-Anbietern noch unterentwickelt. Diese Anbieter sind nicht nur Instrument der US-Regierung, um politischen Einfluss zu nehmen, sie ignorieren in großem Maße europäisches Datenschutzrecht. Die Entwicklung und verstärkte Nutzung rechtskonformer europäischer Alternativen muss auf die Tagesordnung.

US-Sanktionen gegen Verteidigende des Rechts

Donald Trump war zum zweiten Mal nicht einmal einen Monat im Amt des US-Präsidenten, als er Anfang Februar 2025 Sanktionen gegen den Internationalen Strafgerichtshof (IStGH) anordnete. Dieser hatte u. a. Haftbefehle gegen Israels Premier Benjamin Netanjahu und Ex-Verteidigungsminister Joav Gallant vor dem Hintergrund des völkerrechtlich unzulässigen israelischen Vorgehens im Gaza-Streifen erlassen. Trump wirft dem IStGH „bösartiges Verhalten" und „Machtmissbrauch" vor. Sein Dekret sanktioniert Führungskräfte, Angestellte und Mitarbeitende des IStGH sowie deren Familienangehörige. Alle Vermögenswerte, die diese Personen in den USA besitzen, wurden eingefroren. Ihnen wurde die Einreise in die USA untersagt. Der französische IStGH-Richter Nicolas Guillon, Mitunterzeichner des Haftbefehls gegen Netanyahu, berichtet: „Diese Sanktionen betreffen alle Bereiche meines täglichen Lebens." Er verlor seine Konten bei Amazon, Airbnb und PayPal; Expedia stornierte seine Reservierung für ein Hotelzimmer. Er kann nicht mehr mit American Express, Visa oder Mastercard bezahlen und nicht nur das: „Es gibt Banken, die, obwohl sie nicht amerikanisch sind, die Konten von sanktionierten Personen schließen." Schon September 2020 hatte Trump in seiner ersten Amtszeit gegen die damalige IStGH-Chefanklägerin Fatou Bensouda Sanktionen verhängt, weil das Gericht mutmaßliche Kriegsverbrechen von US-Soldaten in Afghanistan untersucht hatte.[1]

Die Sanktionen haben System: Kurz vor Weihnachten 2025 verhängte die Trump-Administration Sanktionen gegen „Ideologen in Europa". Betroffen sind der Ex-EU-Kommissar Thierry Breton sowie vier Aktivisten gegen Hassrede: die Geschäftsführerinnen der gemeinnützigen Organisation HateAid Anna-Lena Hodenberg und Josephine Ballon, die Gründerin des britischen Global Disinformation Index (GDI) Clare Melford und der in den USA und Großbritannien tätige Aktivist des Center for Countering Digital Hate (CCDH) Imram Ahmed. Breton wird zum Vorwurf gemacht, federführend für den EU-Digital-Services-Act gewesen zu sein, mit dem gegen illegale Inhalte von US-Internet-Plattformen wie Meta, Google oder X vorgegangen werden kann. Neben der Einreisesperre in die USA stehen Finanzsanktionen im Vordergrund einschließlich der Sperrung von Bankkonten sowie Kreditkarten von US-Finanzdienstdienstleistern wie Visa oder Mastercard. Das Online-Banking der Betroffenen ist massiv eingeschränkt, da sie auch von Banken, die nicht direkt in US-Besitz sind, abgewiesen werden. Ein Betroffener stellte fest, dass er „faktisch auf einer schwarzen Liste des weltweiten Bankensystems" steht. Man könne kaum noch etwas online bestellen, „da man nicht wisse, ob das Paket, in dem das Produkt verpackt ist, aus den USA stammt".[2]

Schon im Juli 2025 hatte die US-Regierung dem brasilianischen Richter Alexandre de Moraes das Visum entzogen und finanzielle Sanktionen nach dem Global Magnitsky Act verhängt. Dieses Gesetz soll sich eigentlich gegen Personen richten, die schwere Menschenrechtsverletzungen begangen haben. Das Vergehen von de Moraes bestand darin, ein Strafverfahren gegen den Trump-Verbündeten und früheren brasilianischen Präsidenten Jair Bolsonaro wegen dessen Putschversuchs geführt zu haben.[3]

Beim Streben nach digitaler Souveränität kann es also nicht nur um die Befreiung der Abhängigkeiten von den US-Clouds der AWS & Co., von Microsofts Verwaltungs-Software, von Amazons Online-Marktplatz, von Apples und Googles Smartphone-Betriebssystemen gehen. Unsere Abhängigkeit von US-Zahlungsdiensten ist noch nicht ins öffentliche Bewusstsein gedrungen.

Platzhirsch *PayPal*

Das Zahlen mit dem Smartphone wird bei uns vom US-amerikanischen PayPal dominiert. In Deutschland bieten 92 % der Akzeptanzstellen PayPal als digitale Zahlungsmöglichkeit an. Beim Umsatz im Online-Handel liegt PayPal mit ca. 30 % klar an der Spitze. Die europäischen Verbraucher- und Datenschützer, die seit Jahrzehnten Gefechte mit den US-IT-Konzernen bei Social Media und Bürokommunikation ausfechten und inzwischen vor Gericht austragen, haben sich bisher wenig um diese US-Dominanz beim digitalen Bezahlen gekümmert. Einen Schrecken bekamen sie, als August 2025 Millionen PayPal-Nutzerdaten im Darknet zum Verkauf standen und kurz danach von PayPal initiierte Lastschriften wegen Betrugs- und Missbrauchsverdacht im zweistelligen Milliarden-Euro-Bereich gestoppt werden mussten.[4]

Wieder kurz danach veröffentlichte das Netzwerk Datenschutzexpertise ein 50-seitiges Gutachten zum Datenschutz bei PayPal, das zu wenig schmeichelhaften Ergebnissen kommt: „Die Information der Betroffenen über Zwecke, Rechtsgrundlagen, Datenempfänger und über die genutzten automatisierten Entscheidungsverfahren ist ungenügend und verstößt gegen Artikel 13 DSGVO. Der konzerninterne Datenaustausch ist intransparent; die rechtlichen Grundlagen hierfür sind nicht ersichtlich. PayPal verleugnet entgegen den Vorgaben der DSGVO seine gemeinsame datenschutzrechtliche Verantwortlichkeit im Hinblick auf die Datenverarbeitung bei den Zahlungsempfängern (Verkäufern), den eingebundenen Banken und Konzernunternehmen. Die nach Artikel 26 DSGVO geforderte Transparenz zu den in gemeinsamer Verantwortlichkeit geführten Verfahren wird nicht hergestellt.

Soweit Einwilligungen eingeholt werden, entsprechen diese nicht den rechtlichen Anforderungen (Artikel 7 DSGVO), schon

gar nicht an eine ausdrückliche Einwilligung. Die ist für die Verarbeitung von sensitiven Daten, für die Cookie-Nutzung und die Nutzung für Marketing- bzw. Werbezwecke nötig. Der Schutz von besonderen Kategorien personenbezogener Daten, etwa von Gesundheitsdaten, sowie von Berufsgeheimnissen ist nicht gewährleistet (Artikel 9 DSGVO, § 203 StGB).“[5]

Die Reaktion PayPals auf diese Gutachtenveröffentlichung beschränkte sich zunächst auf eine pauschale Zurückweisung der Vorwürfe und die Erklärung, das Unternehmen nehme den Datenschutz ernst.[6] Eine Datenschutzdiskussion über PayPal sollte dessen Weihnachtsgeschäft nicht beeinträchtigen. PayPal nahm kurzfristig seine Datenschutzerklärung, auf die sich das Gutachten des Netzwerks Datenschutzexpertise wesentlich berief, von seiner Webseite. Diese wurde erst wieder online gestellt, nachdem sich gezeigt hatte, dass die Tagespresse die Gutachtenveröffentlichung nicht aufgegriffen hatte. Das Unternehmen änderte zudem umgehend eine Voreinstellung bei der Eröffnung eines PayPal-Accounts: Sang- und klanglos verschwand dort die bisher vorangekreuzte Einwilligung in die Werbenutzung. Zu offensichtlich unzulässig war diese – technisch leicht zu beseitigende – Praxis. Mit Datum vom 22. Januar 2026 änderte PayPal dann seine Datenschutzerklärung und bereinigte diese von einigen offensichtlichen Rechtsverstößen, soweit diese sich nicht auf das Geschäftsmodell des Unternehmens auswirken.[7]

Das Wegducken PayPals in Sachen Datenschutz hatte sich abgezeichnet: Ihr im September analog per Post wie digital versandter umfangreicher Fragenkatalog mit 23 Themen blieb weitgehend ohne Antwort: Da die digitale Kontaktaufnahme mit dem bei PayPal zuständigen Datenschützer nur über einen Nutzer-Account angeboten war und deren Umfang begrenzt war, bedurfte es mehrerer hintereinander geschalteter Anfragen, um sämtliche 23 Themen zu adressieren. Die erste Fragerunde wurde innerhalb von wenigen Stunden über den eingerichteten Account beantwortet, enthielt aber faktische und fachliche Fehler. Die Vermutung liegt nahe, dass hier kein Datenschützer aus Fleisch und Blut tätig war, sondern so genannte Künstliche Intelligenz. Die Hoffnung auf weitere Antwort-Brocken erwies sich als unbegründet. Offenbar hatte ein echter Mensch die weitere KI-Beantwortung abgeschaltet. Seitdem herrscht Sendepause.

Trotz dieser offensichtlichen Verstöße blieben die Datenschutzaufsichtsbehörden weitgehend untätig. Für die gemäß der DSGVO federführend zuständige Behörde – die Nationale Kommission für den Datenschutz in Luxemburg (Commission Nationale pour la Protection des Données – CNPD) – ist PayPal kaum ein Thema: In deren jährlichen Tätigkeitsberichten findet sich zu diesem weltweit tätigen Datenverarbeiter nichts. Die Webseite der CNPD weist lediglich darauf hin, dass sie die Binding Corporate Rules (BCR) des Konzerns genehmigt habe. Diese BCRs sollen global anwendbar sein und europäischen Datenschutz nicht nur in den USA, sondern z. B. auch in der Volksrepublik China garantieren. Sie enthalten nichts anderes als eine formale Paraphrasierung von DSGVO-Vorgaben, ohne dass wirksame Mechanismen zu deren Umsetzung etabliert sind.[8]

In Deutschland hatte PayPal bisher seinen Sitz in Brandenburg, seit Anfang 2026 liegt dieser in Berlin. Die Landesbeauftragte für Datenschutz in Brandenburg teilte mit, dass sich die Zahl der Eingaben zu dem Unternehmen jährlich im mittleren zweistelligen Bereich bewegt. Diese werden nach Luxemburg zur weiteren Bearbeitung weitergegeben. Dieses Schicksal ereilt nun auch das Gutachten des Netzwerks Datenschutzexpertise. Rückmeldungen über Datenschutzaktivitäten von der Luxemburger Datenschutzbehörde blieben bisher aus.

Sensible Finanzdaten

Während die Datenschutzaufsicht die Augen verschließt vor der Grundrechtsmissachtung durch PayPal, sprechen die Fakten ihre eigene Sprache. Das weltweit tätige Unternehmen mit 434 Millionen Nutzenden, das mit über 100 unterschiedlichen Währungen hantiert und dabei im Jahr 2024 1,68 Billionen US-Dollar umgesetzt hat, schert sich nicht um den Datenschutz seiner Kunden und nicht um die europäischen rechtlichen Vorgaben. Zwar widmet PayPal dem Datenschutz viel Text. Darin genehmigt sich das Unternehmen aber alles, was Profit bringt und Verluste vermeidet. Der Katalog der erfassten Daten umfasst alles, was im Rahmen der Finanztransaktionen anfallen könnte, nicht nur Zahlung und Zahlungsempfänger, sondern das erworbene Produkt und was sonst zum Kunden in Erfahrung gebracht werden kann, vom Standort über Gerätedaten bis hin zu Konsum- und Bonitätsprofilen.

Zwecks Abwicklung seiner Geschäfte lässt sich PayPal den weltweiten Datenaustausch mit sämtlichen Konzernunternehmen genehmigen, ohne offenzulegen, um welche es sich handelt, natürlich auch mit Banken, technischen Dienstleistern und Kreditschutzunternehmen. Zu den Datenempfängern gehören aber auch Facebook, Google und sonstige Datenvermarkter. Welche Daten des Kunden wo für welche Zwecke landen – darum geht es bei informationeller Selbstbestimmung – bestimmt PayPal und behält es für sich. Dafür erteilt sich das Unternehmen im Kleingedruckten und dort gut verteilt „ausdrückliche Einwilligungen“. Auch in den Kontoeinstellungen sind diese gut versteckt und bleiben ein Rätsel: Wofür die schwarz bzw. grau gefärbten Schieber-Einstellungen stehen, ist unklar und mehr Glücksspiel als Datenschutz. Besonders brisant ist die unbeantwortete Frage, welche Daten wie zweckfremd genutzt werden.

Digitale Zahlungen verdrängen immer mehr das anonyme Bargeld. Dadurch erhalten die eingeschalteten Zahlungsdienstleister ein präzises Bild frei Haus davon geliefert, wo sich Menschen wann aufgehalten haben und für was sie wieviel bezahlt haben. Spenden für politische Parteien, die Beschaffung von erotischem Spielzeug, der Erwerb von Arzneimitteln wie der von Büchern oder frischen Brötchen …: alles wird langfristig gespeichert. Für die Abwicklung der finanziellen Transaktionen ist einiges kurzfristig in Ordnung; die jahrelange Aufbewahrung dieser Daten und Nutzung für Werbezwecke oder gar für die an die Zahlungsfähigkeit angepasste individuelle Preisgestaltung aber definitiv nicht.

Digitale Finanztransaktionsdaten – Spielball für US-Dienste

Das Gutachten des Netzwerks Datenschutzexpertise entstand auf Anregung der Nichtregierungsorganisation Finanzwende, die im Juni 2024 eine umfassendere Kampagne zu Big-Techs im

Finanzwesen startete.[9] Ziel der Kampagne ist es, auf die Über- und Vormachtstellung der Big-Tech-Unternehmen und die damit verbundenen Risiken, die mit der Einführung von Finanzdienstleistungen verbunden sind, hinzuweisen, um deren unkontrollierten Machtzuwachs zu verhindern. Gefördert wird dieser Machtzuwachs durch unzureichende staatliche Aufsicht und Lücken bei der Regulierung. Nach Ansicht von Finanzwende ist eine enge Kooperation der Behörden aus der Wettbewerbs-, der Datenschutz- und der Finanzaufsicht sowie die Schaffung öffentlicher Alternativen nötig. Regulativ wird eine strikte Trennung der Finanzsparte von sonstigen operativen Geschäften gefordert.

Tatsächlich findet keine Kooperation der europäischen Datenschutzbehörden mit der Finanz- und Wettbewerbsaufsicht statt. Die US-Plattformen – ähnlich auch chinesische Anbieter – versuchen, sich erfolgreich dem Zugriff der europäischen Aufsicht zu entziehen. Ihr Geschäftsmodell basiert auf Rechtsverstößen und Gesetzeslücken, die sich in der Schnittmenge der Aufsichtszuständigkeiten abspielen.

PayPal ist insofern nur ein Beispiel. Google (Alphabet), Apple, Amazon, Meta und jüngst das chinesische Alibaba etablieren sich auf unserem Finanzmarkt und koppeln ihre Datenerfahrungen aus dem Bereich der Online-Geschäfte mit erlangten Finanzdaten. PayPal geht den umgekehrten Weg und nutzt seine Finanztransaktionsdaten für Werbezwecke. Die US-Kreditkartenunternehmen Visa oder Mastercard haben die gleiche Richtung eingeschlagen. Über diese beiden Unternehmen werden rund 60 % aller bargeldlosen Zahlungen in Europa abgewickelt. Auch deren Datenschutzinformationen sind Allgemeinplätze, die ihnen – ohne jegliche Transparenz – weitgehend freie Hand lassen bei der Datennutzung. Die tatsächlich bestehende rechtliche Hürde, die Forderung nach einer „ausdrücklichen Einwilligung" wird durch die Einholung von Pauschalerlaubnissen umschifft.

Die Gefahren der Datenmacht der Unternehmen werden massiv verstärkt durch den potenziellen Zugriff auf deren Datenschatz durch US-Behörden. Das Office of Foreign Assets Control (OFAC), das dem US-Finanzminister Scott Bessent untersteht, kann mit der Behauptung, US-Sicherheitsinteressen seien bedroht, Vermögen blockieren und Überweisungen verbieten, um Terroristen, Drogenkartelle oder ganze Länder vom US-Finanzsystem abzuschneiden.

Die weltweiten Banktransaktionen erfolgen über den in Belgien beheimateten Dienstleister Society for Worldwide Interbank Financial Telecommunication (SWIFT). Sämtliche globalen Transaktionsdaten liefen lange Zeit über ein in den USA befindliches Rechenzentrum, auf das US-Sicherheitsbehörden nach den Terroranschlägen am 11. September 2001 direkten Zugriff nahmen. Als dies bekannt wurde, verlegte SWIFT sein Spiegelrechenzentrum von den USA in die Schweiz, der US-Rechner wird weiterhin für den lokalen, nicht mehr für den innereuropäischen Datenverkehr genutzt. Dessen ungeachtet verpflichteten sich die EU-Staaten im Gegenzug in einem Terrorist Finance Tracking Programme (TFTP), dem US-Finanzministerium auf Anfrage Banktransaktionsdaten von in Europa ansässigen Finanzdienstleistern zu liefern, ohne dass adäquate Datenschutzvorkehrungen bestehen.[10]

Zugriffe auf Finanzdaten durch US-Behörden erfolgen bisher in einer Blackbox. Mit dem Cloud Act besteht ein US-Gesetz, das US-Konzerne verpflichtet, US-Behörden auf Verlangen Kundendaten auszuhändigen, auch wenn diese außerhalb der Vereinigten Staaten verarbeitet und gespeichert werden. Ein Whistleblower, der hierzu etwas Licht ins Dunkel bringen könnte, ist bisher nicht in Sicht. Was mit diesen Daten möglich ist, das lassen die jüngsten Aktionen der Trump-Administration erahnen. Dass diese Regierung keine ethischen oder rechtlichen Grenzen sieht, hat sie – bzgl. der Datennutzung innerhalb des Landes – durch das Zulassen des ungehinderten Treibens der DOGE-Abrissbirne unter Führung von Elon Musk gezeigt.[11]

Fehlendes Problembewusstsein

Dass hinsichtlich des Umgangs mit Finanztransaktionsdaten in Europa und insbesondere in Deutschland kein Problembewusstsein besteht, mag auf ein traditionelles, weit verbreitetes Vertrauen in die Finanzwirtschaft zurückgehen: Solange die Finanzdaten in den Tresoren der einheimischen Banken und Sparkassen verwahrt sind, meinen die Menschen diese seien in vertrauenswürdigen – vom Bankgeheimnis geschützten – Händen. Dabei ranken um dieses Bankgeheimnis vor allem Mythen: Beim „Bankgeheimnis" handelt es sich nicht, wie z. B. beim ärztlichen Patientengeheimnis, um ein gesetzliches strafbewehrtes Datennutzungsverbot. Vielmehr ist es nichts anderes als ein vertragliches Vertraulichkeitsversprechen der Geldinstitute, an das sich diese aber weitgehend auch gebunden fühlen.[12]

Die Digitalisierung des Zahlungsverkehrs im Internet sowie vor Ort am Point of Sale und die Einschaltung von Intermediären hat schon längst zu einem Systemwechsel geführt. Der deutsche und der europäische Gesetzgeber haben dem Rechnung getragen mit der inzwischen grundlegend überarbeiteten Payment-Service-Direktive 2 (PSD 2) und deren Umsetzung im Zahlungsdiensteaufsichtsgesetz (ZAG). Danach ist eine Zweckänderung von Finanztransaktionsdaten nur per ausdrücklicher Zustimmung/Einwilligung erlaubt.[13] Die Gesetzgeber hatten aber nicht im Blick, mit welcher Dreistigkeit Big Techs „Einwilligungen" einholen und mit welcher Unbekümmertheit Betroffene diese erteilen.

Naives Vertrauen scheint nicht nur bei der Öffentlichkeit allgemein zu bestehen, sondern auch in der Finanzbranche, bei der Aufsicht und in der Politik. Nicht anders zu erklären ist, dass für die meisten Finanzjuristen Datenschutz ein Fremdwort ist, dass der Finanzsektor in der Datenschutzaufsicht praktisch nicht vorkommt und dass von Seiten der politischen Verantwortlichen das Problem der finanziellen Datensouveränität nur allmählich in den Blick gerät.

Es tut sich doch etwas in Sachen Souveränität

Es ist insbesondere Trump und seiner Administration zu verdanken, dass sowohl die Finanzwirtschaft als auch die europäische Politik die Notwendigkeit zu erkennen beginnen, sich von US-Finanzdienstleistern unabhängig zu machen. Ein erster Bewusstwerdungsschub entstand 2019 mit Metas Libra-Projekt, also dem Versuch des Facebook-Konzerns, eine weltweite pri-

vate digitale Parallel-/Kryptowährung einzuführen. Nachdem dieses Projekt 2022 begraben wurde[14], versandete die Diskussion um Finanzsouveränität. US-Wirtschaft und -Regierung betreiben weiterhin eine weltweite imperiale Finanzpolitik. Ein Bestandteil davon ist Trumps Kryptopolitik, mit der dieser nicht nur eine weltweite staatliche, an den US-Dollar anknüpfende Parallelwährung von Stablecoins ins Spiel bringt, sondern sich darüber zugleich persönlich bereichert.[15]

Ein Ansatzpunkt für eine europäische Antwort ist die konkrete Planung der EU-Kommission für die Einführung eines digitalen Euro. Mit ihm soll per Karte oder Smartphone online bezahlt werden können und im gesamten Euroraum in gleicher Weise wie mit Bargeld am Point of Sale. Der digitale Euro, neben dem das analoge Geld vollständig erhalten bleiben soll, muss den europäischen Datenschutzvorgaben entsprechen; grundsätzlich soll auch damit anonymes Zahlen möglich sein. Gemäß der Projektleiterin in der Europäischen Zentralbank (EZB) Evelien Witlox könnte der digitale Euro Ende 2028/Anfang 2029 Wirklichkeit werden.[16] Siehe dazu aktuell die Kampagne „Unabhängigkeit von Trump und Co. Unbezahlbar!“[17]

Die Finanzwirtschaft hat die 2020 gegründete European Payment Initiative mit dem institutsübergreifenden Angebot von Wero damit begonnen, bei den Alltagstransaktionen eine europäische Alternative zu den US-Anbietern auf den Markt zu bringen. In Belgien, Frankreich und Deutschland können Wero-Banken-App-Nutzende seit 2024 in Sekundenschnelle einander Geld hin- und herschicken. Der Einsatz im Online-Handel und generell im E-Commerce steht kurz vor der Einführung und kann PayPal Konkurrenz machen.[18] Doch auch bei der Wero-Alternative hält sich die Souveränität in Grenzen, da Wero das europäische Angebot des Amazon-Cloudanbieters AWS nutzt, auf das im Bedarfsfall über den CLOUD-Act US-Behörden Zugriff haben.[19] Die in einzelnen europäischen Ländern erfolgreichen nationalen Lösungen genügen nicht für einen einheitlichen europäischen Markt und als Antwort auf die Gefahren von Übersee.[20]

Aufsicht und Verbraucherorganisationen sollten damit beginnen, die bestehenden Regeln der DSGVO und der PSD 2 bzw. des ZAG durchzusetzen. Dabei muss ein Ansatz verfolgt werden, der das Finanz-, das Wettbewerbs- und das Datenschutzrecht zusammenbringt. Auch die Gesetzgebung bleibt gefordert: Angesichts der Sensibilität sind Finanzdaten einer strengeren Zweckbindung zu unterwerfen; Finanzabwicklung und sonstige digitale Aktivitäten müssen strikt voneinander getrennt werden.

Auch den Verbraucherinnen und Verbrauchern, wenn sie schon digital bezahlen wollen, sollte Souveränität ein Anliegen sein, nicht zuletzt um zu verhindern, dass ihre Daten im Einflussbereich von Trump oder Xi landen. Mit der Nutzung europäischer Alternativen tun die Verbraucher nicht nur sich selbst einen Gefallen, indem sie sich ihre digitale Souveränität über ihre Finanzdaten zumindest teilweise zurückholen. Sie handeln auch im Interesse der Händler, deren Gebühren – bei PayPal z. B. mit ca. 2,5 % des Umsatzes – exorbitant hoch sind. Wero und erste recht der digitale Euro sollen für die Akzeptanzstellen erheblich kostengünstiger sein. Finanzsouveränität in einem rechtsstaatlichen Raum, den die Europäische Union (hoffentlich langfristig) darstellt, ist Voraussetzung, dass der Gesellschaft wie auch den Einzelnen nicht das digitale Finanznetz abgeschaltet wird oder zur Totalüberwachung genutzt wird. Nicht nur ökonomische Gründe, sondern auch die Wahrung von Freiheit, Demokratie und Rechtsstaatlichkeit sprechen dafür, dass die Kontrolle über die eigene Finanzdatenverarbeitung sichergestellt wird.

Anmerkungen

1 *Trump ordnet Sanktionen gegen Strafgerichtshof an, https://www.tagesschau.de 07.02.2025; USA verhängen Sanktionen gegen IStGH-Chefankläger Khan, https://www.spiegel.de 14.02.2025; Bartz u. a.: „Dann gehen hier die Lichter aus“, Der Spiegel 4/2026 v.16.01.2026, S. 11.*

2 *USA verhängen Visa-Sperren gegen Hassrede-Gegner, https://www.dw.com 24.12.2025; Prantl: „In Acht und Bann“, Süddeutsche Zeitung 02.01.2026, 6.; Protest gegen Einreiseverbote der USA, Süddeutsche Zeitung 27./28.12.2025.*

3 *Wiedmann-Schmidt: „Auf amerikanischem Boden unerwünscht“, Der Spiegel 2/2026 v. 02.01.2026, 29.*

4 *Heck: „Mail von Paypal? Nein!“, Süddeutsche Zeitung 26.08.2025, 13; Heck: „Millionen PayPal-Daten zu verkaufen“, Süddeutsche Zeitung 21.08.2025, S. 13; Heck/Schreiber/Zydra: „Banken stoppen Paypal-Zahlungen“, Süddeutsche Zeitung 28.08.2025, 1; Heck/Nezig/Schreiber: „Der dominante Kumpel aus den USA“, Süddeutsche Zeitung 30./31.08.2025, 21.*

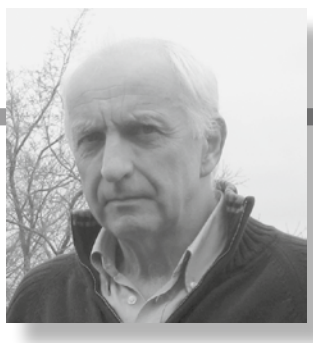
5 *Schuler/Weichert: „Datenschutz bei PayPal“, 10.12.2025, https://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2025_12_paypal.pdf.*

6 *Koch: „Gutachten bescheinigt Paypal Datenschutzverstöße, Paypal weist Vorwürfe zurück“, 11.12,2025, Update 19.12.2025, https://www.heise.de/-11111140.*

7 *PayPal-Datenschutzerklärung, https://www.paypal.com/de/legalhub/paypal/privcay-full.*

8 *The CNPD approves the BCR of PayPal, 09.02.2018, Dernière mise à jour 05/06/2025, https://cnpd.public.lu/en/actualites/national/2018/02/bcr-paypal.html; https://www.paypal.com/de/legalhub/paypal/bcr?locale.x=de_DE.*

9 *Melches/Peters: „Mehr Geld, mehr Macht: Big-Techs im Finanzwesen“, Juni 2024, https://www.finanzwende-recherche.de/wp-content/*



Thilo Weichert

Dr. **Thilo Weichert** war von 2004 bis 2015 *Landesbeauftragter für Datenschutz Schleswig-Holstein* und damit Leiter des *Unabhängigen Landeszentrums für Datenschutz* in Kiel. Er ist Mitglied des *Netzwerks Datenschutzexpertise*, Vorstandsmitglied der *Deutschen Vereinigung für Datenschutz e. V.* (DVD) sowie von *Digitalcourage e. V.*

uploads/Mehr_Geld_mehr_Macht_Big_Techs_im_Finanzwesen.pdf; Melches/Peters: „Die Finanzdienste von Apple, Google und Co.: Ein gefährlich guter Deal", März 2025, https://www.finanzwende-recherche.de/wp-content/uploads/Studie_Big_Tech_Die-Finanzdienste-von-Apple-Google-und-Co.pdf.

10 *Weichert: „SWIFT: Europa „befreit" Banktransaktionsdaten vom Grundrecht auf Datenschutz", Grundrechte-Report 2010, Hrsg. Müller-Heidelberg u.s., S. 35 ff.*

11 *Weichert: „Trump und der Datenschutz", DANA 2/2025, 73; „Musk nutzt Daten-Vollzugriff auf sämtliche Staatsausgaben", DANA 2/2025, 99.*

12 *Heinson in Specht/Mantz: Handbuch Europäisches und deutsches Datenschutzrecht, 2019, § 14 Rn. 4 ff. (S. 392 ff.).*

13 *Art. 94 Abs. 2 PSD 2; § 59 Abs. 2 ZAG.*

14 *Beer: „Metas Stablecoin Diem – vormals Libra – angeblich vor dem Aus", 26.01.2022, https://heise.de/-6338511.*

15 *Muth: „Die Finanzwelt zittert vor Stablecoins", SZ 04.11.2025, 15.*

16 *Schreiber/Zydra: „Niemand wird zum Umstieg gezwungen", Süddeutsche Zeitung 26.01.2026, 14.*

17 *https://www.finanzwende.de/kampagnen/unabhaengigkeit-von-trump-und-co-unbezahlbar*

18 *Bartz: „Kann Europa PayPal?", Der Spiegel Nr. 38/2025 v.12.09.2025, 63; Heck: Online bezahlen – aber bitte europäisch, Süddeutsche Zeitung 21.08.2025, 13; Heck: „Online-Händler schalten Wero frei", Süddeutsche Zeitung 09.10.2025, 15.*

19 *Leisegang: „Uneingelöstes Versprechen auf digitale Souveränität: Europäischer Bezahldienst Wero nutzt Amazon-Server", 21.04.2026, https://netzpolitik.org/2026/uneingeloestes-versprechen-auf-digitale-souveraenitaet-europaeischer-bezahldienst-wero-nutzt-amazon-server/*

20 *Bizum in Spanien, Sibs in Portugal, Bancomat in Italien, iDEAL in den Niederlanden, Twist in der Schweiz, MobilePay in Dänemark, Norwegen und Finnland, Swish in Schweden.*

Lisa Seifert, ***Forum SCS-Standards der OSBA***

Sovereign Cloud Stack – Baustein Digitaler Souveränität jenseits von Big Tech

Die zunehmende Abhängigkeit von wenigen globalen Cloud-Anbietern stellt Bund, Unternehmen und Zivilgesellschaft vor grundlegende Fragen der digitalen Selbstbestimmung. Während Hyperscaler wie AWS, Microsoft oder Google zentrale Teile der digitalen Infrastruktur kontrollieren, wächst der Wunsch nach Alternativen, die Transparenz, Kontrolle und Interoperabilität stärker berücksichtigen. Sovereign Cloud Stack (SCS) setzt genau hier an: mit einem offenen, transparenten und anbieterneutralen Cloud-Ökosystem aus Europa für Europa.

Was ist Sovereign Cloud Stack?

Sovereign Cloud Stack (SCS) ist eine europäische Initiative, die ein offenes, transparentes und anbieterneutrales Cloud-Ökosystem schafft, welches Souveränität gewährleistet. Im Fokus steht echte Wahlfreiheit. Die Grundlage von SCS bilden zertifizierbare Standards, ein modularer Software-Stack sowie praxisnaher Wissenstransfer. Diese Grundlage soll sicherstellen, dass Cloud-Dienste interoperabel, transparent und unabhängig betreibbar sind.

Ein zentrales Anliegen von SCS besteht darin, technologische Abhängigkeiten zu reduzieren, offene Schnittstellen zu etablieren und damit langfristig die Handlungsfähigkeit von Organisationen im digitalen Raum zu sichern. SCS adressiert damit nicht nur technische, sondern auch strategische Fragestellungen moderner IT-Infrastrukturen.

Die Initiative wurde von der *Open Source Business Alliance e. V.* (OSBA)[1] ins Leben gerufen und in den Jahren 2021 bis 2024 durch das Bundesministerium für Wirtschaft und Klimaschutz gefördert. Inhaltlich ist es eng mit europäischen Initiativen wie Gaia-X[2] verbunden und folgt deren Leitbild, vertrauenswürdige, vernetzte und föderierte digitale Ökosysteme aufzubauen.

Nach dem Ende der Förderphase wird die Weiterentwicklung der Standards durch das *Forum SCS-Standards* organisiert, das ebenfalls in der OSBA angesiedelt ist. Dieses Forum schafft einen neutralen Rahmen, in dem Anbieter:innen, Integratoren:innen und Anwender:innen gemeinsam an der Evolution der Standards arbeiten. Dadurch entsteht ein dynamisches Ökosystem, das nicht von einzelnen Akteuren dominiert wird, sondern durch die Beiträge vieler Beteiligter wächst.

Sovereign Cloud Stack

Diese Governance-Struktur ist kein Zufall, sondern Ausdruck eines grundlegenden Prinzips: Digitale Souveränität soll nicht durch proprietäre Plattformen oder einzelne Marktteilnehmer definiert werden, sondern durch offene Verfahren, nachvollziehbare Entscheidungsprozesse und gemeinschaftlich entwickelte Normen.

Wenn Souveränität technisch wird

Kaum ein Begriff prägt die aktuelle Cloud-Debatte so stark wie Digitale Souveränität. Gleichzeitig bleibt häufig unklar, woran sich diese konkret festmachen lässt. Schlagworte wie „Hosting in Europa" oder „DSGVO-konform" greifen zu kurz, wenn es darum geht, tatsächliche Abhängigkeiten, Wechselmöglichkeiten oder die Kontrolle über den eigenen Betrieb zu bewerten.

Die Unsicherheit liegt dabei weniger in fehlenden Technologien als vielmehr in der Schwierigkeit, komplexe Cloud-Systeme systematisch zu beurteilen. Plattformsoftware, Schnittstellen, Betriebsprozesse und organisatorische Rahmenbedingungen grei-

Anja Voß (DigitalHub.SH, links) moderiert bereits zum zweiten Mal den Summit 2026 *und begrüßt gemeinsam mit Lisa Seifert (Projektleiterin im Forum SCS-Standards, OSBA) das Publikum in Berlin. Foto: @SCS@social.osb-alliance.de*

fen ineinander – und genau daraus ergibt sich die zentrale Frage für viele IT-Verantwortliche: Nach welchen Kriterien lässt sich Souveränität belastbar einschätzen?

Dabei ist Digitale Souveränität keineswegs ein undefinierter Begriff. Sowohl auf nationaler als auch auf europäischer Ebene existieren klare Beschreibungen, etwa durch den IT-Planungsrat[3] oder das Zentrum für Digitale Souveränität der Öffentlichen Verwaltung[4] (ZenDiS). Problematisch wird es jedoch, wenn diese Konzepte verkürzt werden. Wird Souveränität allein über den Standort einer Cloud definiert, entsteht ein trügerisches Bild. Solche Vereinfachungen – häufig als „Souveränitäts-Washing" bezeichnet – blenden bestehende technische, rechtliche und operative Abhängigkeiten aus und erschweren fundierte Entscheidungen. Veröffentlichungen wie das *Cloud Sovereignty Framework* der EU[5] oder der Souveränitätscheck der Stadt München[6] helfen, den Begriff greifbarer werden zu lassen, und machen deutlich, dass ein belastbares Verständnis Digitaler Souveränität deutlich weiter geht. Es umfasst die Fähigkeit, Cloud-Lösungen rechtssicher zu betreiben, Abhängigkeiten von einzelnen Anbietern zu vermeiden und Systeme auch bei Störungen oder Anbieterwechseln unter eigener Kontrolle zu halten. Ebenso gehören Transparenz – etwa durch die Nutzung und die offene Dokumentation von Open Source Software – sowie die Möglichkeit zur technischen Anpassung und Weiterentwicklung dazu.

Entscheidend ist dabei, dass diese Eigenschaften nicht isoliert betrachtet werden können: Cloud-Infrastrukturen bestehen aus vielen miteinander verzahnten Ebenen, von der zugrunde liegenden Infrastruktur über Plattformdienste und Schnittstellen bis hin zu Betriebsprozessen und organisatorischem Know-how. Abhängigkeiten können auf jeder dieser Ebenen entstehen und müssen entsprechend ganzheitlich adressiert werden.

Von der Definition zur Umsetzung

Sovereign Cloud Stack setzt genau an diesem Punkt an und überführt den Begriff der Digitalen Souveränität in konkrete, überprüfbare Anforderungen. Statt abstrakter Zielbilder beschreibt SCS, wie Cloud-Infrastrukturen gestaltet sein müssen, um langfristig kontrollierbar und anpassbar zu bleiben. Dabei steht nicht ein einzelnes Produkt im Mittelpunkt, sondern eben offene Standards für Architektur, Betrieb und Schnittstellen.

Diese Aspekte werden im SCS systematisch aufgegriffen und in klar abgegrenzte Handlungsfelder überführt. Dazu zählen rechtliche Verlässlichkeit, tatsächliche Wahlfreiheit zwischen Anbietern, die Möglichkeit zur technischen Weiterentwicklung sowie nachvollziehbare und beherrschbare Betriebsprozesse. Sie bilden die konzeptionelle Grundlage, aus der konkrete Anforderungen abgeleitet werden.

Im nächsten Schritt werden diese Leitlinien in strukturierte Vorgaben überführt: durch definierte Standards und darauf aufbauende Zertifizierungsstufen, die sowohl technische als auch organisatorische Kriterien abbilden. Auf diese Weise wird Digitale Souveränität nicht nur beschrieben, sondern in messbare und überprüfbare Eigenschaften übersetzt. Die Standards[7] werden gemeinschaftlich in der SCS-Community sowie im Forum SCS-Standards entwickelt und bilden zugleich die Grundlage für entsprechende Zertifizierungen.

Digitale Souveränität wird damit zu einer praktischen Entscheidungsfrage: Sie zeigt sich nicht in einzelnen Eigenschaften, sondern im Zusammenspiel von Recht, Technik und Organisation – und in der Fähigkeit, diese Faktoren aktiv zu gestalten.

Offene Standards als Grundlage der Interoperabilität

Die Frage, ob Cloud-Infrastrukturen dauerhaft digital souverän nutzbar sind, entscheidet sich weniger an einzelnen Features als an ihrer strukturellen Offenheit. Wo Schnittstellen proprietär bleiben, Erweiterungen nur innerhalb eines Anbieter-Ökosystems funktionieren und Betriebsmodelle nicht übertragbar sind, entstehen langfristige Abhängigkeiten. Ein späterer Wechsel wird dadurch technisch aufwendig oder wirtschaftlich unattraktiv.

Sovereign Cloud Stack begegnet diesem Problem, indem Interoperabilität nicht als Nebenbedingung, sondern als zentrales Designziel verstanden wird. Im Fokus stehen dabei keine einzelnen Produkte, sondern klar definierte Standards[8] für die grundlegenden Bausteine moderner Cloud-Architekturen. Dazu zählen etwa Infrastrukturressourcen, containerbasierte Plattformdienste, Identitäts- und Zugriffsmechanismen sowie organisatorische Betriebsprozesse.

Durch diesen Ansatz entsteht eine gemeinsame technische Basis, auf der unterschiedliche Cloud-Angebote kompatibel betrieben werden können. Anwendungen lassen sich zwischen entsprechenden Umgebungen verschieben oder verteilt betreiben, ohne dass grundlegende Anpassungen an der Architektur notwendig werden. Interoperabilität wird damit zum entscheidenden Mittel, um Abhängigkeiten zu vermeiden und Handlungsspielräume zu erhalten.

Aktuell konzentrieren sich die SCS-Standards auf die *Infrastructure-as-a-Service* (IaaS) und *Kubernetes-as-a-Service* (KaaS)-Ebene.

Für Anwender:innen eröffnet sich dadurch ein breites Spektrum an Handlungsmöglichkeiten. Bestehende Cloud-Infrastrukturen können systematisch anhand der definierten Standards analysiert, bewertet und schrittweise weiterentwickelt werden, ohne bestehende Systeme vollständig ablösen zu müssen. Gleichzeitig bieten die Standards eine verlässliche Grundlage, um neue Cloud-Umgebungen von Beginn an interoperabel und zukunftsfähig zu konzipieren. Darüber hinaus erleichtern sie die Auswahl geeigneter Anbieter: Organisationen können gezielt nach Cloud-Diensten suchen, die die definierten Anforderungen erfüllen und dies durch entsprechende Zertifizierungen nachweisen. Die Standards fungieren damit nicht nur als technischer Leitfaden, sondern auch als Orientierungshilfe für strategische Entscheidungen im Cloud-Bezug.

Die SCS-Zertifizierungen – Interoperabilität messbar machen

Ein zentrales Instrument des Sovereign Cloud Stack ist das Zertifizierungsmodell. SCS übersetzt die SCS-Standards in überprüfbare Kriterien und schafft damit eine Grundlage, um Interoperabilität nachweisbar zu machen und Cloud-Angebote entsprechend zu kennzeichnen.

Dazu gehört auf der Infrastrukturebene die Bestätigung, dass das Cloud-Angebot definierte Anforderungen an Computer-, Storage- und Netzwerkschnittstellen erfüllt und zugleich Aspekte wie Betrieb, Sicherheit und Governance berücksichtigt. Ergänzend dazu wird auch die Kompetenz von Dienstleistern geprüft: Integrator:innen können nachweisen, dass sie in der Lage sind, Cloud-Umgebungen gemäß den SCS-Vorgaben aufzubauen und zu betreiben.

Perspektivisch soll das Zertifizierungsmodell erweitert werden, etwa um Plattformdienste auf Basis von Kubernetes.

Sovereign Cloud Stack liefert damit erstmals einen strukturierten Ansatz, um Aspekte Digitaler Souveränität systematisch zu erfassen. Der derzeitige Fokus zeigt klar: Interoperabilität ist kein technisches Nebenprodukt, sondern die Voraussetzung dafür, Wechselfähigkeit in der Cloud überhaupt zu ermöglichen.

Technische Bausteine im SCS-Ökosystem

Die Umsetzung der SCS-Standards erfolgt nicht nur auf konzeptioneller Ebene, sondern wird durch konkrete Werkzeuge und einen modularen Software Stack unterstützt. Sie bilden die technischen Bausteine, mit denen sich interoperable und standardkonforme Cloud-Infrastrukturen praktisch realisieren und betreiben lassen. Ein zentraler Aspekt ist die Automatisierung des Cloud-Betriebs. Neben dem laufenden Betrieb spielt jedoch das Lifecycle-Management beim Betrieb von komplexen Cloud-Infrastrukturen auch eine zentrale Rolle. Für Infrastructure-as-a-Service (IaaS) Umgebungen existieren im SCS Ökosystem verschiedene Ansätze.

Mit Yaook[9], *Yet another OpenStack on Kubernetes*, steht ein System zur Verfügung, das den Betrieb von OpenStack auf Basis von Kubernetes weitgehend automatisiert. Es folgt einem deklarativen Ansatz: Der gewünschte Zustand der Infrastruktur wird beschrieben, während das System kontinuierlich dafür sorgt, dass dieser Zustand eingehalten wird. Änderungen an der Konfiguration – etwa die Zuordnung von Diensten zu bestimmten Knoten – lassen sich so gezielt steuern und werden automatisiert umgesetzt. Auch im laufenden Betrieb unterstützt Yaook durch Mechanismen wie automatisierte Reaktionen auf Störungen oder die Verlagerung von Workloads, wodurch Stabilität und Verfügbarkeit erhöht werden. Neben dem vom ALASCA e. V. entwickelten Yaook gibt es mit *OSISM* ein Integrations- und Betriebsframework für OpenStack-basierte Umgebungen. Neben den Installations-, Update- und Wartungsprozessen rund um OpenStack können mit OSISM auch jede Menge weiterführende Komponenten wie beispielsweise Ceph als Software-Defined-Storage verwaltet werden. Es diente im SCS-Förderprojekt-Kontext als Grundlage für die IaaS-Referenzimplementierung und bündelte verschiedene Werkzeuge zu einem integrierten Ansatz für den Betrieb. Für die Bereitstellung der Cloud-Dienste greift OSISM unter anderem auf etablierte Open-Source-Projekte wie Kolla[10] zurück. Diese stellen containerisierte OpenStack-Komponenten sowie Werkzeuge für deren Deployment und Betrieb bereit und haben sich über Jahre im produktiven Einsatz bewährt. Vergleichbare Ansätze finden sich auch in anderen OpenStack-basierten Plattformen und Distributionen.

In ihrer Gesamtheit zeigen diese Bausteine, dass Sovereign Cloud Stack nicht nur einen normativen Rahmen vorgibt, sondern auch konkrete technische Ansätze bereitstellt, um Digitale Souveränität praktisch umzusetzen.

Fazit: Souveränität ist kein Produkt

Sovereign Cloud Stack ist kein singuläres Produkt, sondern ein Ökosystem welches Bausteine für einen Transformationsprozess liefert. Alternativen zu den dominierenden Cloud-Modellen sind möglich – es ist jedoch deutlich, dass diese Alternativen nicht von selbst entstehen. Sie erfordern bewusste Entscheidungen, Investitionen und die Bereitschaft zur gemeinsamen Gestaltung.

Lisa Seifert

Lisa Seifert ist seit Juni 2025 Projektleiterin im *Forum SCS-Standards* der *Open Source Business Alliance e. V.* (OSBA). In dieser Rolle arbeitet sie an der Weiterentwicklung der Standards und bringt Akteur:innen aus Wirtschaft, öffentlicher Hand und Open-Source-Community zusammen. Seit 2024 ist sie aktives Mitglied der OSBA, war Teil des geschäftsführenden Vorstands und ist heute im erweiterten Vorstand aktiv.

Im Spannungsfeld zwischen globalen Plattformkonzernen und staatlicher Kontrolle bietet SCS keinen einfachen Ausweg, sondern einen dritten Ansatz. Weder die Abhängigkeit von wenigen marktbeherrschenden Anbietern noch die Verlagerung von Kontrolle in zentralisierte staatliche Strukturen lösen das Problem Digitaler Souveränität nachhaltig. Beide Modelle bergen Risiken – sei es durch ökonomische Machtkonzentration oder durch potenzielle Überwachung und politische Einflussnahme.

Sovereign Cloud Stack setzt stattdessen auf Offenheit und zertifizierbare Standards. Ein Perspektivwechsel findet statt: weg von der Frage, welchem Anbieter man vertraut, hin zu der Frage, unter welchen strukturellen Bedingungen Vertrauen überhaupt gerechtfertigt ist. Souveränität wird damit nicht delegiert, sondern gestaltet.

Gerade in Europa liegt hierin eine strategische Chance. Initiativen wie SCS können dazu beitragen, digitale Infrastruktur als gemeinschaftliche Aufgabe zu begreifen – jenseits von Plattformabhängigkeit und zentralisierter Kontrolle.

SCS ist damit weniger eine fertige Lösung als vielmehr ein Angebot: Digitale Souveränität nicht als Schlagwort zu behandeln, sondern als konkrete Gestaltungsaufgabe ernst zu nehmen.

Anmerkungen

1 *https://osb-alliance.de/*
2 *https://gaia-x.eu/*
3 *https://www.it-planungsrat.de/fileadmin/beschluesse/2021/Beschluss2021-09_Strategie_zur_Staerkung_der_digitalen_Souveraenitaet.pdf*
4 *https://www.zendis.de/media/pages/newsroom/publikationen/souveraenitaets-washing/87412539a0-1755243871/zendis-whitepaper-souveraenitaets-washing.pdf*
5 *https://sovereigncloudstack.org/das-cloud-sovereignty-framework-der-eu-kommission/*
6 *https://stadt.muenchen.de/news/digitale-souveraenitaet-messbar.html*
7 *https://docs.scs.community/standards/standards/overview*
8 *https://docs.scs.community/standards*
9 *https://yaook.cloud/*
10 *https://docs.openstack.org/kolla/latest/*

Maria Vaquero, Daniel Gerber, *ALASCA e. V.*

Vertrauen ist gut, Open Source ist besser: Wie ALASCA Digitale Souveränität durch Open Source schafft

Im Zeitalter von Cloud Computing, datengetriebener Innovation und geopolitischen Spannungen gibt es kaum ein Thema, das so wichtig und aktuell ist wie die digitale Souveränität. Die Fähigkeit, die eigene Technologie, Infrastruktur und Datenströme zu kontrollieren und anzupassen, ist zum Lackmustest für die digitale Zukunft und den Erfolg Europas geworden. Wer diese Fähigkeit in Zukunft nicht besitzt oder entwickelt, macht sich nicht nur abhängig, sondern auch erpressbar. Vor diesem Hintergrund ist der ALASCA e. V. gegründet worden.

Ob Erhöhung der Preise für digitale Dienstleistungen, Abschaltung des E-Mail-Postfachs oder Kündigung des Bankkontos: Digitalpolitik ist zu Machtpolitik geworden. Dabei besteht nicht nur das Problem, dass die US-amerikanischen Big-Tech-Unternehmen diese Machtpolitik versuchen auf die Europäische Union auszuweiten und sich deren Forderungen zum Beispiel im Digital Omnibus Paket der EU wiederfinden, sie greifen auch Daten der Synergy Research Group[1] zufolge sämtliches Umsatzwachstum des europäischen Cloud-Marktes ab.

In diesem Spannungsfeld, in dem technologische Kontrolle und geopolitische Interessen immer stärker verflochten sind, haben sich mehrere Akteure in Dresden zusammengeschlossen. Sie wollten nicht nur auf die Herausforderungen der digitalen Souveränität reagieren, sondern aktiv die eigene Zukunft gestalten und auch andere unterstützen, dies zu tun. Wer nicht gestaltet, wird gestaltet! So wurde im September 2022 der gemeinnützige Verein ALASCA e. V. gegründet, dessen klare Mission es ist, die digitale Souveränität Europas durch Open-Source-Zusammenarbeit zu stärken.

Eine Mission, die auf Offenheit und Unabhängigkeit gründet

Die Mission von ALASCA ist sowohl zukunfts- als auch praxisorientiert: Entwicklung, Unterstützung und Förderung von

ALASCA Gründungsversammlung

Open-Source-Technologien, die es Organisationen ermöglichen, ihre eigenen Cloud-Infrastrukturen effizient und sicher aufzubauen und zu betreiben. Die Mitglieder von ALASCA und die breitere Community sind der Überzeugung, dass Cloud-Infrastrukturen nicht von einer Handvoll globaler Anbieter kontrolliert werden sollten, sondern eine Governancestruktur innerhalb der europäischen Jurisdiktion, ganz ohne Cloud Act und Foreign Intelligence Surveillance Act (FISA), benötigen. Sie stellen sich eine Zukunft vor und arbeiten täglich daran, sie Realität werden zu lassen, in der Unternehmen, öffentliche Einrichtungen, Privatpersonen und alle, die es möchten, ihre eigenen

Cloud-Umgebungen betreiben, die als Freie Software entwickelt werden und auf der Basis transparenter Open-Source-Technologien beruhen.

Zu diesem Zweck dient ALASCA als Heimat für Open-Source-Projekte in verschiedenen Reifestadien. Der Verband unterstützt zudem den Übergang von zuvor geschlossenen oder proprietären Technologien zu Open-Source. Im Mittelpunkt all dessen steht ein Leitprinzip: Betriebsbereitschaft. Das Ziel von ALASCA ist es, Tools bereitzustellen, die für den Einsatz in realen Anwendungsfällen bereit sind.

Von Yaook bis ALASCA: Die Geschichte des Vereins

Im Mittelpunkt der Entstehungsgeschichte von ALASCA steht das Open-Source-Projekt Yaook. Das Projekt begann im Juni 2020, als zwei Unternehmen, Cloud&Heat Technologies und STACKIT, erkannten, dass sie vor dem gleichen Problem stehen: das äußerst manuelle und fehleranfällige Lebenszyklusmanagement ihrer OpenStack-Infrastrukturen. Sie beschlossen dafür eine gemeinsame Lösung zu entwickeln. Damit war der Startschuss für Yaook, ein auf Kubernetes aufsetzendes Open-Source-Tool für das Lebenszyklusmanagement von OpenStack-basierten Cloud-Infrastrukturen, das die Bereitstellung, Updates, Monitoring und den Betrieb automatisiert, gefallen.

Als die Community und die Bekanntheit von Yaook stiegen, entstand der starke Wunsch, das Projekt von den beiden Unternehmen zu entkoppeln und eine unabhängigere Struktur aufzubauen, um eigenständig und unternehmensunabhängig zu agieren. So legte Yaook den Grundstein für ALASCA. Mit der Dynamik von Yaook und der wachsenden Erkenntnis, wie wichtig Open-Source-Cloud-Infrastrukturen sind, entschieden sich sieben Gründungsmitglieder im September 2022 zur Gründung von ALASCA.

Zahlreiche Open-Source-Projekte, eine Vision

ALASCA beherbergt derzeit sieben Open-Source-Projekte, von denen jedes in seiner Disziplin einen wertvollen Beitrag zu offenen, transparenten Cloud-Infrastrukturen leistet:

Yaook: Das Projekt, das den Anstoß für ALASCA gab, ist ein Werkzeug für automatisiertes Lifecycle-Management von OpenStack-Clouds auf Basis von Kubernetes. Es vereinfacht Deployment, Betrieb und Wartung, indem es Konfiguration, Skalierung und Betriebsprozesse automatisiert und so DevOps-Teams entlastet sowie den Aufbau souveräner Cloud-Infrastrukturen erleichtert.

Krake: Krake ist ein Open-Source-basierter Workload-Manager für verteilte Infrastrukturen. Er orchestriert die effiziente Verteilung virtualisierter und containerisierter Workloads über Multi-Cloud-, Private-Cloud- und On-Premise-Umgebungen und wählt Zielsysteme anhand frei definierbarer ökologischer, technischer oder wirtschaftlicher Metriken.

ALASCA Hackathon

Yake: Yake ist ein GitOps-basiertes Tool zur Installation und zum Lifecycle-Management von Gardener. Es ermöglicht schnelle, zuverlässige Deployments sowie einfache Updates und Wartung. Basierend auf Flux wird der Systemzustand kontinuierlich mit der deklarativen Git-Konfiguration abgeglichen und bietet somit volle Kontrolle über die Konfiguration und den Betriebszustand der Gardener-Installation.

Tarook: Tarook, als *Certified-Kubernetes*-Distribution der *Cloud Native Computing Foundation* (CNCF), ermöglicht als ganzheitliches Lebenszyklus-Management-Tool die einfache Bereitstellung, Verwaltung und Skalierung von Kubernetes Clustern – ob auf Bare Metal oder in OpenStack. Unabhängig vom Einsatzbereich bietet es eine flexible, automatisierte Lösung für das vollständige Lifecycle-Management und sorgt so für einen effizienten Betrieb.

Arko: Arko ist eine standardisierte Plattform zur Überwachung hybrider Cloud-Infrastrukturen. Sie bietet einen Überblick über den Zustand von Systemen und Anwendungen über private und öffentliche Umgebungen hinweg und ermöglicht durch Drilldown-Analysen eine schnelle Fehleridentifikation sowie effizienteres Monitoring und Troubleshooting.

Ixpect: Ixpect ist ein Open-Source-Tool zur kontinuierlichen Überwachung von IXP-Peering-LANs. Es analysiert BUM-Traffic zur Erkennung von Fehlkonfigurationen und Angriffen, integriert bestehende Router-Konfigurationsdaten und meldet erkannte Probleme zentral zur weiteren Analyse und schnellen Behebung.

Seconlay: Seconlay ist ein in Rust entwickeltes Infrastructure-as-a-Service-Tool (IaaS) für sichere Mandantentrennung. Es reduziert die Komplexität der Infrastruktur durch eine kleine Trusted Computing Base, trennt strikt Control- und Data-Plane und ermöglicht einen stabilen, nachvollziehbaren Betrieb von IaaS-Umgebungen.

Zusammen verdeutlichen diese Projekte den ganzheitlichen Ansatz von ALASCA: Es geht nicht nur darum, Software zu entwickeln, sondern ein ganzes Ökosystem für Installation und den Betrieb offener Infrastrukturen zu schaffen und zu fördern.

Eine Kultur des Bewusstseins schaffen

Die Mission von ALASCA ist allerdings nicht einfach auf den Code fokussiert: Der Verband spielt eine zentrale Rolle bei der Aufklärung und Mobilisierung der Community hinsichtlich der Bedeutung digitaler Souveränität – und der Rolle, die Open-Source dabei spielt. So wurde zu diesem Zweck der „Aufbau einer offenen und inklusiven Community zum Austausch von Wissen, Erfahrungen und Informationen zwischen Entwicklern und weiteren Akteuren im Bereich Open-Source" in der Satzung des Vereins verankert.

Zur Erreichung dieses Ziels veranstaltet der Verband seit 2024 jährlichen seinen ALASCA Summit. Im nunmehr dritten Jahr kommen am 3. und 4. November 2026 voraussichtlich rund 300 Teilnehmende aus ganz Europa unter dem Motto „With C – as in Community. Breaking down technical silos united for a digitally sovereign Europe." zu Vorträgen, Workshops und Diskussionen rund um Open-Source-Cloud-Infrastruktur in Dresden zusammen. Das Community-Event bietet ein hochkarätiges Treffen, bei dem Entwickler, Open-Source-Enthusiasten, Cloud-Nutzer, aber auch Politiker und Verwaltungsangestellte zusammenkommen, um gemeinsam die Zukunft der digitalen Souveränität zu gestalten und Erfahrungen auszutauschen. Die Anmeldung zum Summit[2] ist kostenfrei und der Call-for-Participation ist noch bis zum 31. Juli 2026 offen für Beiträge.

Eine weitere Initiative, um der Allgemeinheit gesammeltes Wissen zur Verfügung zu stellen, sind die ALASCA Tech-Talks. Sie sind ein monatliches Online-Format, bei dem Experten aus Industrie, Wissenschaft und der Open-Source-Community in mittlerweile 34 Ausgaben Anwendungsfälle aus der Praxis und Open-Source-basierte Lösungen vorstellen, um die Autonomie und Widerstandsfähigkeit der Cloud zu stärken.

Der Verband veranstaltet zudem *Round-table*-Gespräche, bei denen Vertreter aus der Zivilgesellschaft, Wirtschaft und Politik zusammenkommen, um ihre Vision von digitaler Souveränität zu teilen und zu erörtern, wie verschiedene Technologien, Initiativen und Strategien dazu beitragen. Er bringt sich ebenfalls in die politische Willensbildung ein und hat bei Beteiligungsverfahren für große Digitalprojekte wie den *Deutschlandstack* der Bundesregierung und der *European Open Digital Ecosystem Strategy* der EU Kommission Stellungnahmen zur Stärkung des Open-Source-Ökosystems abgegeben.

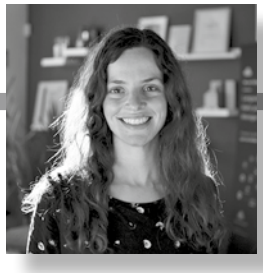
Durch diese Veranstaltungen und Initiativen schafft ALASCA mehr als nur Open-Source-Technologie – es baut eine Gemeinschaft auf und schärft das Bewusstsein für die Erreichung digitaler Souveränität. So wird sichergestellt, dass die Botschaft einer offenen, souveränen Infrastruktur Entscheidungsträger, Entwickler und Cloud-Nutzer gleichermaßen erreicht.

Förderung der Zusammenarbeit, Schaffung von Steuerungsstrukturen und Stärkung der Neutralität

Von Anfang an war sich ALASCA bewusst, dass Zusammenarbeit unerlässlich ist. Seine Mitglieder vereinen eine vielfältige Mischung aus Fachwissen und Stärken. Der Verband arbeitet zudem eng mit bedeutenden Open-Source-Initiativen wie der OpenInfra Foundation und der Open Source Business Alliance zusammen und stellt so sicher, dass seine Arbeit mit dem übergeordneten Open-Source-Ökosystem im Einklang steht.

In den vergangenen Jahren verzeichnete der Verein ein stetiges Wachstum – nicht nur durch die Gewinnung neuer Mitglieder und die Einführung weiterer Open-Source-Projekte, sondern auch durch bedeutende Schritte in Richtung Reife. Ein Technischer Lenkungsausschuss legt nun die technische Roadmap fest, während sich die laufenden Bemühungen auf die Verbesserung der Governance-Modelle sowohl für den Verein als auch für seine Projekte konzentrieren. Es ist ebenfalls ein Onboarding-Prozess (inkl. Logo und Landingpage) definiert und eine Guideline für Projekte definiert worden, um von Snowflake zu einem Glacier-Projekt zu reifen.

Die Entwicklung von ALASCA wurde durch die finanzielle Unterstützung des Freistaates Sachsen weiter gefördert, wodurch der Verein seine Open-Source-Arbeit im Rahmen der Free and *Open Cloud Initiative Saxony* (FOCIS) ausweiten konnte. Diese



Maria Vaquero und Daniel Gerber

Dr. **Maria Vaquero** ist Teamleiterin für Geschäftsentwicklung und Marketing bei *Cloud & Heat Technologies*, einem Gründungsmitglied von ALASCA. Sie unterstützt die Weiterentwicklung des Vereins und dessen Kommunikation, etwa durch Community-Events wie den *ALASCA Summit* und hat zur Sicherung der Finanzierung der Verbandsaktivitäten beigetragen. Sie hat einen ingenieurwissenschaftlichen Hintergrund und promovierte an der TU Dresden im Innovationsmanagement.

Dr. **Daniel Gerber** ist promovierter Informatiker. Als CTO bei der *Targomo GmbH* verantwortete er globale IT-Dienstleistungen, bevor er 2019 als Abgeordneter in den Sächsischen Landtag einzog und dort für digitale Souveränität stritt. Seit 2025 setzt er sein Engagement für freie Software beim ALASCA e. V. und als stellvertretender Geschäftsführer der *Open Source Business Alliance* fort.

Förderung unterstützt die Open-Source-Entwicklung, die fortlaufende Ausrichtung der ALASCA-Projekte auf gemeinschaftsgetriebene Standards wie den *Sovereign Cloud Stack* (SCS)[3] und die Erprobung des Technologie-Stacks in realen Anwendungsfällen. Sie hat es ALASCA zudem ermöglicht, ein engagiertes Team aus Open-Source-Spezialist:innen und Softwareentwickler:innen einzustellen. Dies hat die Fähigkeit des Vereins signifikant gestärkt, unabhängig zu agieren und Innovationen innerhalb der Open-Source-Community voranzutreiben.

Eine gemeinsame Vision für die digitale Zukunft Europas

In weniger als vier Jahren seit seiner Gründung hat sich ALASCA zu einer unverwechselbaren Stimme in der europäischen Technologielandschaft entwickelt, die technische Innovation mit gesellschaftlichem Engagement verbindet. Durch die Förderung offener Zusammenarbeit und praxisorientierter Innovation trägt ALASCA dazu bei, eine digitale Welt zu gestalten, in der Transparenz fest in den Grundpfeilern der Cloud verankert ist. Von Dresden bis hin zur europäischen Bühne beweist der Verband, dass Open-Source ein Weg ist, um sicherzustellen, dass wir die Kontrolle über unsere digitale Zukunft behalten. Bringen Sie gern Ihre Perspektive ein und werden Sie Teil dieser gemeinsamen Entwicklung.

ALASCA

Verband für betriebsfähige, offene Cloud-Infrastrukturen e.V.

Anmerkungen

1 *https://www.srgresearch.com/articles/european-cloud-providers-local-market-share-now-holds-steady-at-15*
2 *https://alasca.cloud/alasca-summit-2026/*
3 *https://sovereigncloudstack.org/*

Oliver Radfelder, ***Hochschule Bremerhaven, Informatik***

Jenseits des Jargons der Souveränität

Ein Plädoyer für robuste Architekturen und eine kritische Informatiklehre

Digitale Souveränität ist zum politischen Leitbegriff avanciert, droht aber ohne fachliche Kompetenz zur bloßen Worthülse zu verkommen. Während moderne Cloud-Metaphern oft neue Abhängigkeiten hinter einer ‚Abstraktions-Bürokratie' verschleiern, plädiert dieser Beitrag für eine Rückbesinnung auf ein solides ingenieur:innenwissenschaftliches Fundament und handwerkliche Redlichkeit.

Wir leben in einer Zeit tiefgreifender Veränderungen. Tiefgreifender in kurzer Zeit vielleicht als jemals in der Geschichte, in jedem Fall aber tiefgreifender als in den vergangenen Jahrzehnten.

Der Themenkomplex *Souveränität*, speziell *digitale Souveränität*, vermengt mit *nationaler* und *europäischer* Souveränität, treibt die öffentliche Debatte. In kurzer Zeit werden unter hohem Druck staatliche Entscheidungen als Ergebnis von Aushandlungen diverser Akteur:innen, denen *Souveränität* gewiss ein Anliegen ist, getroffen.

Dass die Forderung nach digitaler Souveränität oft ohne scharfe Konturen bleibt, unterstreichen auch Pohle und Thiel (2020) in ihren Arbeiten am Weizenbaum-Institut. Sie zeigen auf, wie der Begriff diskursiv eingesetzt wird, um sehr unterschiedliche, teils widersprüchliche Maßnahmen politisch zu legitimieren.

Als Lehrende in der Informatik bereiten wir Studierende auf eine ungewisse Zukunft vor, in der sie in der Lage sein sollen, sich gegen übermächtige Institutionen individuell und in kollektiven Strukturen gegen Vereinnahmungen zu behaupten mit ihrem Wissen, ihrem Denken, ihrer Sprache und ihrer Ethik.

Was also geben wir den Studierenden mit auf den Weg, sich unter dieser Maßgabe selbst zu verorten?

Informatik als Ingenieur:innendisziplin

Wenn Souveränität nicht als bloßer Rechtsbegriff herhalten soll oder als Diskursvoraussetzung, sondern *auch* als ingenieur:innenwissenschaftliche Kategorie und als notwendige Voraussetzung für ethisches Handeln in der Informationstechnik, dann braucht ein radikaler Souveränitätsbegriff die Bedeutung von Determinismus und Verifizierbarkeit.

Politische Souveränitätsansprüche sind wertlos, wenn die Komplexität der technischen Systeme ihre Überprüfbarkeit unmöglich macht. Ein herrschaftsfreier Diskurs ist spätestens dann zum Scheitern verurteilt, wenn die Diskursteilnehmer:innen keinen sachverständigen Bezugspunkt mehr finden. Ohne tiefes technisches Verständnis bleibt Souveränität ein Schlagwort. Der Versuch, durch unangemessene Abstraktionen die existierende Komplexität zu verwalten anstatt sie wieder auf ein Maß der Beherrschbarkeit zu reduzieren, verursacht selbst wieder soviel Indirektion und Verwaltungskomplexität, dass kognitive Souveränität weder vom Individuum noch von kleinen Gruppen erreicht werden kann.

Kognitive Souveränität

Es existiert fraglos *inhärente Komplexität* in der modernen IT. Informatik als Wissenschaft und Ingenieur:innendisziplin begriffen, tritt dazu an, diese *inhärente* von *zufälliger*, achtlos auf-

summierter Komplexität zu trennen und Prinzipien und Umsetzungsstrategien zu schaffen, um die eine zu erkennen und die andere zu meiden.

Es ist jener Punkt zu finden, ab dem ein technisches System noch im Krisenfall von Einzelnen oder einer fokussierten kleinen Gruppe mit einem adäquaten gemeinsamen, inneren Modell insofern beherrscht werden kann, dass die Kausalität von der Handlung des Tippens eines Kommandos bis hin zu den Auswirkungen auf eine Schar entfernter Maschinen folgerichtig vorhersehbar ist.

Die US-Hyperscaler haben durchaus die Komplexität ihrer Großsysteme im Griff. Es sollte aber nicht übersehen werden, dass sie durch ihre Systematik einen Teil der Komplexität externalisieren und ihren Kund:innen in die Hand legen. Das Zusammenspiel der verfügbaren Komponenten so auszuwählen, dass die eigenen Ziele effizient, verlässlich und nachhaltig umsetzbar sind, hat eine eigene Branche hervorgebracht, die diese am Ende möglicherweise doch nicht so zufällige Komplexität wieder einhegen soll.

Kognitive Souveränität zu erlangen, bedeutet für Studierende die tägliche Praxis an der Kommandozeile in einer Umgebung, die keine Beherrschbarkeit suggeriert, wo sie nicht gegeben ist. Je mehr Indirektionen zwischen Aktion und Wirkung liegen, desto schwieriger wird es, ein Modell des eigenen Handelns zu entwickeln.

Technische Souveränität braucht sprachliche Souveränität

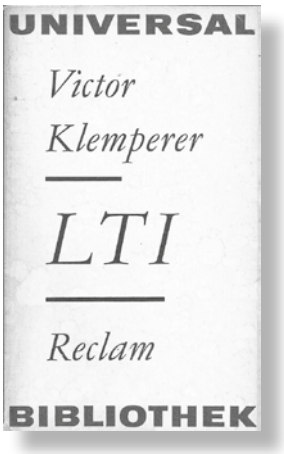
Sprache ist das Instrument, mit dem Werte, Ziele und Lösungen ausgehandelt werden. Es bedarf der Übung, anspruchsvolle Abwägungen zum Ausdruck zu bringen.

Einen Satz zu zerlegen, der zwar hübsch aufbereitet, in der Bedeutung aber leer ist – oder der, nur einen kleinen Schritt weitergedacht, autoritärem Denken geradezu das Wort redet –, muss auch für Informatiker:innen eine Kernkompetenz sein. Es gilt, Grammatik, Bedeutungsnuancen und die Anschlussfähigkeit der Argumentation kritisch zu prüfen.

Sprachliche Wendungen haben eine Geschichte; Sprecher:innen positionieren sich durch Wortwahl und Rhetorik. Wenn angehende Informatikingenieur:innen nicht erkennen, welcher Tradition sich ihr Gegenüber verpflichtet fühlt – wie soll dann fundiert über „europäische Werte“ diskutiert werden? Diese Werte sind keine bloßen Listen; sie sind entstanden, um nach den Katastrophen der ersten Hälfte des letzten Jahrhunderts ein anderes Europa zu errichten.

Die geistigen Strömungen von der Frankfurter Schule über den kritischen Rationalismus und den Poststrukturalismus bis hin zu feministischer Theorie und Funktionalismus haben dieses Europa und seine Werte geprägt.

Wer sich als Ingenieur:in erkenntnistheoretisch auf Popper (1935/2005) bezieht, aber die Positionsbestimmung im Streit um die positivistische Deutung der Welt nicht einzuordnen vermag (Adorno et al. 1969), läuft Gefahr, auch bei Habermas (2022) nur noch „gedrechselte Sprache“ zu hören, wenn von „deliberativer“ Demokratie die Rede ist. Wer sich nie an der Dekonstruktion von Subjekt und Macht versucht hat, kann kaum systematisch hinterfragen, wer was wann mit *Souveränität* meint. Technik ist in dieser Perspektive niemals neutral, sondern formt und zementiert stets spezifische Identitäten und Machtverhältnisse (Haraway 1985).



Victor Klemperer: LTI – Notizbuch eines Philologen, 1947

Und wer Victor Klemperer (1947/2010) gelesen hat, weiß, wie sich die „kleinen Arsendosen“ in der Sprache wieder vermehrt breitmachen.

Dabei darf die Forderung nach Klarheit nicht mit dem Ruf nach einer trivialisierenden Vereinfachung verwechselt werden. Wenn eine anspruchsvolle Sprache gefordert wird, dann nicht, um eine neue ‚Bildungs-Magie‘ zu begründen oder damit sich Eliten hinter einer Mauer aus Begriffen verschanzen. Im Gegenteil: Im Sinne Adornos (1964) ist die Schärfe des Begriffs die beste Notwehr gegen den Jargon, der in der IT-Industrie heute als Marketing-Sprech die Sicht auf die tatsächlichen Machtverhältnisse vernebelt.

Eine ‚demokratische‘ Sprache in der Informatik ist nicht diejenige, die komplexe Sachverhalte auf bunte Icons reduziert, sondern diejenige, die das Subjekt befähigt, die Mechanismen der Abstraktion zu durchschauen. Es ist ein modern gedachtes humboldtsches Bildungsideal: Souveränität entsteht nicht durch die bloße Anwendung von Werkzeugen, sondern durch das Verstehen und die Aneignung ihrer inneren Logik. Bildung ist hier nicht nur als Erwerb eines technologischen ‚Skill-Sets‘ zu verstehen, sondern als die Fähigkeit zur eigenständigen Urteilskraft und Orientierung in einer komplexen Welt (Nida-Rümelin 2013).

Präzision in der Sprache ermöglicht jene kognitive Tiefe, die notwendig ist, um Technik wieder als gestaltbares Medium menschlicher Praxis begreifbar zu machen.

Was heißt das für Studierende der Informatik? Technikfolgenabschätzung bedeutet – wenn auch nur in kleinem Umfang – zu erleben, welche Texte angehende Geistes-, Kultur- und Gesellschaftswissenschaftler:innen lesen. Studierende der Informatik und Wirtschaftsinformatik werden mit ihnen gemeinsam für eine Welt streiten müssen, in der nicht die Mächtigen die Deutungshoheit darüber haben, was wir unter *digitaler Souveränität* verstehen.

Hier bedarf es sicherlich der Übung, eine oft fremd anmutende Sprache zu verstehen, die versucht, die Komplexität der Wirklichkeit und des Sozialen einzufangen und diskutierbar zu machen, und nicht reflexhaft eine Einfachheit in der Sprache einzufordern, die der Sache nicht gerecht wird.

Denk- und Sprachspiele

Dichotomien – die Setzung von Gegensatzpaaren – als rhetorisches Mittel einzusetzen, ist ein im Alltag, Politik und Verkaufsgesprächen mächtiges Instrument, Diskussionen zu lenken. Mit der Anfangssetzung wird eine Einteilung vorgenommen, bei der schon vorab die Stimmung und Richtung der Diskussion festgelegt wird.

Um sich auch als Ingenieur:in zu wappnen gegen verführerische Manipulationen, sind Sprach- und Rhetorikspiele ein solides Fundament. Redliche Ingenieur:innen sollten in der Lage sein, die eigenen Grundannahmen über Kategorien, gedankliche Strukturen und Gegensatzpaare beständig zu hinterfragen. Wer darin geübt ist, ist besser geschützt davor, bei Bewegungen mitzulaufen, deren Annahmen zunächst plausibel klingen mögen, deren Konsequenzen aber nicht mehr mit dem eigenen Anspruch zu vereinbaren sind. Wer vom Simpson-Paradoxon über das Ziegenproblem bis hin zum Gerrymandering geschult, Taktiken und Strategien von Verführenden und Scharlatanen systematisch argumentativ zu zerlegen gewohnt ist, kann sich zumindest gelegentlich der Dichotomisierung und Verführung erwehren.

Was heißt das für Studierende der Informatik? Denkspiele und Sprachspiele sollten zum Studium als Ergänzung zu Ethikdiskursen gehören. Etwas weniger den Fokus auf das Übernehmen fremdgedachter Kategorien, die scheinbar die Wirklichkeit abbilden, zu legen, und stattdessen die Pfadabhängigkeit von gelenkten Argumentationen am eigenen Geist zu erfahren, schärft das Denken.

Die *Pets-vs.-Cattle*-Dichotomie

Der vermeintliche Wechsel vom *Pet* – als liebevoll gepflegte Einzelmaschine – zum *Cattle* – als verwaltete, namenlose Herde – steckt in nahezu jeder Erzählung zu *DevOps* und *Cloud Native*. Gerade die *Cattle*-Metapher entstammt der verführerischen Sprache der Cloud-Verkäufer:innen (Humble & Farley 2010). Als wären *Automatisierung, Redundanz* und *Skalierbarkeit* mit der Cloud in die Welt gekommen. Die herablassende Verniedlichung des auf Basis von *Posix* arbeitenden, traditionsbewussten *Systems-Engineering* zur Haustier-Hätschelei hat doch vor allem den Zweck, die erfahrenen Sysadmins, die oft das angemessenere Ergebnis mit standardisierten und gut beherrschten Werkzeugen erreichen, selbst zum jederzeit austauschbaren und mit Nummern versehenen *Cattle* zu degradieren.

Wer eine Maschine gut im Griff hat, für die:den ist es nur ein kleiner Schritt, wenn es um 10, 100 oder 1000 Maschinen geht, die gleich oder mit Abweichungen gebaut sind, solange Automatisierung durch ein sorgfältiges, nach Prinzipien des Engineerings im Repository verwaltetes und in der Pipeline geprüftes Verfahren erreicht wird.

Was heißt das für Studierende der Informatik? Der systematische Aufbau konkreter Systeme, bei denen alles Überflüssige weggelassen wird als eine Ganzheit von der Serverinfrastruktur über die Webanwendung hin zum Browser, lässt sich praktisch einüben. Weder muss dabei der Rechner selbst zusammengelötet werden, noch der Browser, das Betriebssystem, die Virtualisierung, die Datenbankengine oder der Webserver selbst programmiert werden. All diese Komponenten interagieren über etablierte Standards miteinander: Http, TCP, Ethernet, Java, TLS, EcmaScript, Posix, SQL!

Das Erfahren von Selbstwirksamkeit in einem anspruchsvollen, aber beherrschbaren Stack schafft nicht nur ein *Gefühl* von den eigenen kognitiven Grenzen und den physikalischen Grenzen technischer Systeme, sondern ein *Wissen* darum.

Der Deutschland-Stack

Der Deutschland-Stack ist vom IT-Planungsrat zum Standard erkoren worden (Bundesministerium für Digitales und Staatsmodernisierung [BMDS] 2026, 19. März). Was aber dieser Stack genau sein soll, wird auch oder gerade bei näherem Hinsehen nicht klar.

In der Beschreibung auf der Webseite (BMDS o. D.) heißt es: „Der Deutschland-Stack ist die nationale souveräne Technologie-Plattform für die Digitalvorhaben in Deutschland. Er beinhaltet sowohl die technologische Basis, die strategischen und organisatorischen Rahmenbedingungen als auch die Umsetzungsvorhaben und Produkte“ (Absatz 1).

Hier liegt eines der zentralen Probleme mit dem Deutschland-Stack-Beschluss: Der Stack soll zu viele unterschiedliche Dinge umfassen, als dass er an irgendeiner Stelle konkret fassbar wäre.

Die Formulierung ist wohlgemerkt: „beinhaltet“ – nicht „tangiert“ oder „beeinflusst“. Der Stack *beinhaltet* von der *technologischen Basis* über *Umsetzungsvorhaben* und *Rahmenbedingungen* bis zu *Produkten* wirklich alles, was irgendwie mit IT zu tun haben könnte. Wenn das ein Stack ist, ist das Bild eines Stapels völlig verfehlt und bleibt eine leere Worthülse.

Ein *digitales Ökosystem* als *Betriebssystem der Staatsmodernisierung*

Das *digitale Ökosystem* – wahlweise nur *Ökosystem* – als Metapher für *naturgegeben* oder einfach, weil Menschen eben Ökosysteme mögen, zieht sich bei den staatlichen Akteur:innen vom IT-Planungsrat (IT-Planungsrat 2026a) bis zum BMDS (BMDS 2026, 29. Januar) durch.

Den Deutschland-Stack dann noch als das *Betriebssystem der Staatsmodernisierung* (IT-Planungsrat 2026b) zu bezeichnen, ist im Sinne Klemperers eine kleine Arsendosis. Das Wort *Betriebssystem* hat in der Informatik eine Bedeutung.

Es gibt viel solide Kritik am Deutschland-Stack. „Wir würden uns mehr Klarheit darüber wünschen, was das BMDS als zentrales Ziel hinter dem Deutschland-Stack sieht.“ (Burmeister & Kaufmann 2025: 2) – eine vorsichtige Forderung. Dass hier aber nun gerade die Organisationen AlgorithmWatch, Gesellschaft für Freiheitsrechte, Open Knowledge Foundation, Reporter ohne Grenzen und Wikimedia Deutschland gemeinsam eine *Weiterentwicklung zu einem Demokratie- und Gesellschafts-*

Stack einfordern (Burmeister & Kaufmann 2025: 8), ist unachtsam. Der sich einschleichende Gebrauch des Wortes Stack für vieles, was nur peripher mit Technik zu tun hat, es aber nicht ist, zieht Kreise.

In keinem auch nur ansatzweise sinnvollen Verständnis des Wortes kann das, was Deutschland-Stack genannt wird, ein *Stack* sein.

Die Open Source Business Alliance [OSBA] fordert eine stärkere Ausrichtung auf offene Standards und befürchtet, der Deutschland-Stack könne zu einem Vehikel für *Souveränitäts-Washing* (Ganten, zitiert nach move – moderne verwaltung, 2025, Absatz 3) werden.

Sovereign Cloud Stack

Dass als Teil dieses *Betriebssystems für die Staatsmodernisierung* nun auch ein zumindest etwas konkreteres technisches Konzept mit *OpenStack* bzw. *Sovereign Cloud Stack* zum Standard für die Verwaltung erhoben wurde, ist, was zusätzlich nachdenklich stimmen sollte.

Hier wird zu einem verbindlichen Standard für die Verwaltung erhoben, was möglicherweise um Größenordnungen zu komplex ist, an der falschen Stelle ansetzt und lediglich die gewohnten Nutzungserfahrungen innerhalb der Cloud-Stacks der großen Hyperscaler reproduziert.

Was heißt das für Studierende der Informatik? Sie müssen lernen einzuordnen, wer mit wem mit welchen Interessen über wen spricht.

Souveränität, Selbstbestimmung, Autarkie, Unabhängigkeit, Handlungsfähigkeit, Hoheit, Gelassenheit, Abgeklärtheit, Mündigkeit, Eigenverantwortlichkeit – die Verengung auf die reflexhafte Nutzung des einen Wortes in unterschiedlichen Bedeutungsnuancen trägt zu dessen Instrumentalisierbarkeit bei.

Manchmal ist der erste Schritt zur Sprach- und Ideologiekritik, sich über Synonyme und vollständige – durchaus eingeübte – längere Sätze selbst zu verdeutlichen, was alles mit Phrasen wie *digitale Souveränität*, *Stack* oder *digitales Ökosystem* ausgedrückt werden kann und nach Ausdrucksalternativen zu suchen. Zumindest dann, wenn gewollt ist, dass sich zukünftige Absolvent:innen mit Sprachgefühl, Wissen und Handlungskompetenz in die Diskussionen einschalten können.

Architekturen für technische, kognitive und emanzipatorische Handlungsfähigkeit

Auch wenn es sich zunächst eigenartig anhören mag: Eine Sammlung von Standards zu einem Standard zu erheben ist keine gute Idee aus informatischer Sicht. Technische Standards sind gerade dazu da, Austauschbarkeit und Interoperabiliät zu ermöglichen. Bei der Erhebung des *Sovereign Cloud Stacks* zum Standard wird implizit eine ganze technische Architektur miteinander und mit Spezifikation, Referenzimplementierung und Zertifizierbarkeit verdrahtet.

Drang zur Komplexitätsexplosion

Architekturen für die tatsächlichen Anwendungen werden unter dem Druck, kompatibel zu den profitabelsten Arbeitsweisen der Hyperscaler zu sein, durch *Microservices*, *Pets vs. Cattle*, *eventual consistency, self healing, observability, immutability* und *serverless* so komplex, weil sie die eine Eigenschaft für Verlässlichkeit, nämlich *Zustand*, nicht mehr haben sollen.

Eine Webanwendung, die innerhalb einer Hyperscaler-Infrastruktur läuft, muss so gebaut sein, dass sie jederzeit ohne explizite, schrittige Zustandsübergänge wegen Wartungsarbeiten oder zum Zweck der Lastverteilung gestoppt, verschoben oder neu gestartet werden kann, weil das zum Arbeitsprinzip der flüchtigen Maschinen gehört.

Jeder Zustand wird notwendigerweise an einen weiteren gemanagten Dienst externalisiert. Das geht so weit, dass jeglicher lokale Zustand als Anti-Pattern diskreditiert wird mit dem vielfach wiederholten Argument der *horizontalen Skalierbarkeit*.

Dass es tatsächlich um die *Wegwerfmentalität* von Pods und VMs geht, verbunden mit der Nötigung, die anbieterspezifischen *Managed Services* zu nutzen, ist kaum mehr einfach zu erkennen. Damit geht eine überbordende Technik-Bürokratie einher, bei der sich Anwendungsentwickler:innen kaum mehr mit der fachlichen Logik beschäftigen können.

Weder Verwaltung noch Mittelstand können so noch gradlinige, robuste, redundante und nachhaltige Anwendungen nach etablierten Prinzipien entwickeln.

Ein Plädoyer für Robustheit und Beherrschbarkeit

Wer sich gar nicht erst auf die Dichotomie von *Bastellösung* (Pets) vs. vermeintlicher *High-End-Hyperscaler-Architektur* (Cattle) einlässt, muss nicht den einfachen Kompromiss im Mittelweg suchen.

In der Informatik finden sich erstaunlich langlebige, deterministische, robuste, redundante und nachhaltige Architekturen auf Basis von etablierten offenen Standards und Verfahren. Die notwendigen Werkzeuge und Systeme *setzen Standards um* und sind nicht zugleich Standards. Diese Architekturen sind bewusst so aufgebaut, dass sie nicht jeden *Zustand* in einen *Managed Service* externalisieren, wo sofort mit der Komplexität von verteilten Systemen gekämpft werden muss. Wie Kleppmann (2017) darlegt, ist das Arbeiten in verteilten Systemen inhärent hochgradig anspruchsvoll. Die Verteilung von Zustand auf getrennte Dienste, und seien sie auch noch so gemanaged, könnte sich als der Kardinalfehler der ganzen Cloud-Bewegung herausstellen.

Kleppmann (2015) stellt die provokante These auf: *„Every sufficiently complex and large deployment of microservices contains an ad-hoc, informally-specified, bug-ridden, slow implementation of half of transactions“* (34:40).

Nicht jede Verteilung lässt sich vermeiden. Skalierbarkeit erfordert Verteilung genauso wie lückenlose Persistenz für auditier-

bare Systeme und Anwendungen. Letztlich ist schon das Verhältnis Browser und Anwendungsserver ein verteiltes. Aber es muss nicht mehr Verteilung eingeführt werden als unbedingt nötig, wenn sie am Ende doch wieder eingehegt werden muss.

Der zur Zeit viel gepriesene Einsatz von JWT-Tokens zur Befreiung vom *Zustand* verlagert ihn lediglich in die verteilte Infrastruktur: Die konsistente Validierung und der sichere Widerruf werden in verteilten Architekturen zur großen Herausforderung. Was als Vereinfachung verkauft wird, endet oft in noch komplexerer Infrastruktur für Zustandssynchronisierung durch *eventual consistency*, kompliziertes Key-Management und Blocking.

All das, um Zustandslosigkeit in dem Code zu erlangen, der die Fachlichkeit letztlich umsetzt, und damit genau dieser Code jederzeit nach Belieben gestoppt, verschoben und neu gestartet werden kann.

Wenn das tatsächlich so in den standardisierten technischen Stacks in Deutschland und Europa nachgebaut wird, wie es für die bisherigen Hyperscaler profitabel ist, ist zu befürchten, dass weder die Anwendungsentwicklung beherrschbarer wird, noch dass der Ressourcenhunger eingedämmt oder Sicherheit und Verlässlichkeit überprüfbar wird.

Schlusswort

Die Forderung nach handwerklicher Beherrschung und tiefem Systemverständnis ist kein Plädoyer für einen neuen Elitarismus.

Im Gegenteil: Elitarismus findet sich dort, wo sich eine ‚Kaste der Magier' hinter Bergen von Abstraktionen und unverständlichem Jargon verschanzt. Diese künstliche Komplexität schließt Menschen aus und entzieht Technik der demokratischen Kontrolle.

Ein emanzipatorischer Ansatz hingegen begreift das tiefe Durchdringen von Systemen nicht als Distinktionsmerkmal, sondern als Voraussetzung für Redlichkeit. Nur wer die Mechanik der digitalen Welt wirklich beherrscht, anstatt sie lediglich zu konsumieren, kann sie auch verständlich vermitteln.

Wenn wir als Informatiker:innen unser Fach wirklich beherrschen, agieren wir nicht als abgehobene Expert:innen. Vielmehr können wir aus fundierter, nachprüfbarer Kompetenz heraus die Basis für eine herrschaftsärmere Verständigung schaffen und als Teil der Gesellschaft gemeinsam mit allen Menschen um soziale Gerechtigkeit und Teilhabe ringen.

Bildung schafft keine Barrieren, sie baut sie ab.

Oliver Radfelder

Referenzen

Adorno TW (1964) Jargon der Eigentlichkeit: Zur deutschen Ideologie. Suhrkamp.

Adorno TW, Dahrendorf R, Pilot H, Albert H, Habermas J, Popper KR (1969) Der Positivismusstreit in der deutschen Soziologie. Luchterhand.

Bundesministerium für Digitales und Staatsmodernisierung (2026, 29. Januar) Deutschland-Stack: Sachstand [Präsentationsfolien]. https://bmds.bund.de/fileadmin/BMDS/Dokumente/260129_Deutschland-Stack_Standard_barrierefrei.pdf

Bundesministerium für Digitales und Staatsmodernisierung (2026, 19. März) D-Stack im IT-Planungsrat – Bund und Länder einigen sich auf gemeinsame Umsetzung des Deutschland-Stacks [Aktuelle Meldung]. https://bmds.bund.de/aktuelles/aktuelle-meldungen/detail/gemeinsame-umsetzung-des-deutschland-stacks

Bundesministerium für Digitales und Staatsmodernisierung (o. D.) Der Deutschland-Stack. Abgerufen am 3. Mai 2026 von https://deutschland-stack.gov.de/

Burmeister C, Kaufmann S (2025, 28. November) Stellungnahme zum Deutschland-Stack – Bündnis F5. https://buendnis-f5.de/assets/data/251128_Stellungnahme%20D-Stack%20F5.pdf

Habermas J (1994) Faktizität und Geltung (4. Aufl.). Suhrkamp.

Habermas J (2022) Ein neuer Strukturwandel der Öffentlichkeit und die deliberative Politik. Suhrkamp.

Haraway DJ (1985) A cyborg manifesto: Science, technology, and socialist-feminism in the late twentieth century. Socialist Review, 15(80), 65–108.

Horkheimer M, Adorno TW (1969) Dialektik der Aufklärung: Philosophische Fragmente. Fischer.

Humble J, Farley D (2010) Continuous delivery: Reliable software releases through build, test, and deployment automation. Addison-Wesley.

IT-Planungsrat (2026a, 18. März) Deutschland-Stack (Beschluss B-2026/03-IT). https://www.it-planungsrat.de/beschluss/b-2026-03-it

IT-Planungsrat (2026b, 18. März) Anlage Portfolio zum Beschlussvorschlag (Beschluss 2026/03). https://www.it-planungsrat.de/fileadmin/beschluesse/2026/Beschluss_2026_03_Deutschland-Stack_Portfolio.pdf

Klemperer V (2010) LTI. Notizbuch eines Philologen (24. Aufl.). Reclam. (Originalwerk veröffentlicht 1947)

Kleppmann M (2015, 27. September) „Transactions: myths, surprises and opportunities" by Martin Kleppmann [Video]. YouTube. https://www.youtube.com/watch?v=5ZjhNTM8XU8

Kleppmann M (2017) Designing data-intensive applications: The big ideas behind reliable, scalable, and maintainable systems. O'Reilly Media.

Nida-Rümelin J (2013) Philosophie einer humanen Bildung. Körber-Stiftung.

Pohle J,Thiel T (2020) Digital sovereignty. Internet Policy Review, 9(4). https://doi.org/10.14763/2020.4.1532

Popper KR (2005) Logik der Forschung (11. Aufl.). Mohr Siebeck. (Originalwerk veröffentlicht 1935)

Prof. Dr.-Ing. **Oliver Radfelder** ist seit 2016 Professor im Studienbereich Informatik der Hochschule Bremerhaven. Im Bereich Software Engineering liegt sein Schwerpunkt auf dem durchdringenden Verstehen von nachhaltigen System- und Software-Architekturen. Im Rahmen seiner Lehrveranstaltung hat er sich gemeinsam mit den Studierenden intensiv mit SCS und der Referenzimplementierung auseinandergesetzt.

Joseph P. De Veaugh-Geiss, *KDE Eco*

Mit *Opt Green* und *End of 10* zu längerer Hardware-Lebensdauer und Nutzungsautonomie

Software spielt eine entscheidende Rolle für die ökologische Nachhaltigkeit. Das Projekt Opt Green *von KDE Eco macht die Öffentlichkeit seit 2024 auf das Problem der vorzeitigen Hardware-Veralterung aufmerksam. Zu den Aktivitäten des Projekts gehört die Kampagne* End of 10*, deren Ziel es ist, Endgeräte auf Freie Open Source Software (FOSS) umzustellen, um ihre Lebensdauer zu verlängern und zu verhindern, dass sie auf der Mülldeponie landen. Zudem ermöglicht FOSS Transparenz und Benutzungsautonomie. Dieser Artikel gibt einen kurzen Überblick über die durch Software verursachten Umweltschäden und darüber, wie das Projekt und die Kampagne dagegen vorgehen.*

Wie würden Sie diesen Satz vervollständigen: Das nachhaltigste Gerät ist …? Behalten Sie Ihre Antwort im Hinterkopf – wir kommen gleich darauf zurück.

Digitale Technologie wird oft (und fälschlicherweise) mit Immaterialität in Verbindung gebracht. Doch die Digitalisierung hat einen sehr realen, sehr materiellen Aspekt, der nicht nur unsere physischen Geräte wie Smartphones und Laptops umfasst, sondern auch die Verarbeitungsanlagen für die abgebauten Metalle, die für deren Betrieb notwendig sind, Containerschiffe, die massenproduzierte Hardware transportieren, sowie Kabel und Rechenzentren, die sie mit globalen Netzwerken verbinden.

Zwar können digitale Geräte bestimmte Arten von Abfall reduzieren, doch um die tatsächlichen Umweltauswirkungen digitaler Technologien abzuschätzen, muss der gesamte Lebenszyklus eines Produkts berücksichtigt werden. Dazu gehören die Kosten für die Herstellung und den Transport digitaler Geräte (zum und vom Geschäft sowie zur Deponie), die Kosten für deren Nutzung und die Kosten für die Beseitigung der durch Elektroschrott verursachten Umweltschäden. Dies gilt insbesondere, wenn man den gesamten CO_2-Fußabdruck unserer digitalen Technologien betrachtet, da in manchen Fällen die Herstellung eines Geräts mehr Treibhausgasemissionen verursacht als die Nutzung des Geräts über seine gesamte Betriebsdauer.

Insbesondere der in Produkten enthaltene Kohlenstoff spielt eine entscheidende Rolle, wenn es um den CO_2-Fußabdruck unserer IT-Nutzung geht. Betrachten wir zwei gängige Endgeräte: Laptops und Desktop-Computer. Vergleicht man die während der Nutzung entstehenden Emissionen mit den in den Produkten enthaltenen Emissionen (*produktionsbedingten CO_2-Emissionen*), so macht allein die Herstellung bis zu 80 % (manchmal sogar mehr) der Gesamtemissionen über die gesamte Lebensdauer dieser Geräte aus (Logic 2024). Ein vom Umweltbundesamt veröffentlichter Bericht aus dem Jahr 2012 schätzt, dass man angesichts der sehr hohen Produktionskosten einen Laptop *Jahrzehnte* lang nutzen müsste, bevor sich die Effizienzgewinne neu produzierter Geräte rechtfertigen würden (Prakash et al. 2012). Der Bericht stellt fest (Hervorhebung hinzugefügt):

> *Die Analyse der Amortisationszeiten hat belegt, dass der Umweltaufwand bei der Herstellung eines Notebooks so hoch ist, dass er sich durch eine erhöhte Energieeffizienz in der Nutzung nicht in realisierbaren Zeiträumen amortisieren lässt. Bei einer 10 %igen Energieeffizienzsteigerung des neuen Notebooks im Vergleich zum alten liegen die Amortisationszeiten* zwischen 33 und 89 Jahre*.*

Kehren wir vor diesem Hintergrund zu dem Satz zurück, mit dem dieser Abschnitt eingeleitet wurde. Wie haben Sie diesen Satz vervollständigt: „Das nachhaltigste Gerät ist …"?

Die Antwort des Projekts „Opt Green": *Das nachhaltigste Gerät ist das, das Sie bereits besitzen!*

Opt Green

Inspiriert von den Erfolgen des Projekts *Blauer Engel für FOSS* (BE4FOSS[1]) und der *Sustainable-Software*[2]-Zielsetzung der KDE Gemeinschaft startete KDE Eco[3] im Jahr 2024 die Initiative *Opt Green: Nachhaltige Software für nachhaltige Hardware.*[4] Das Projekt konzentriert sich auf die entscheidende Rolle, die Software für die Langlebigkeit von Hardware spielt: Laptops, Smartphones und andere Geräte sind schnell aufgrund von Software veraltet. In manchen Fällen kann es vorkommen, dass Sie bereits 3-5 Jahre nach dem Kauf eines Geräts eine Warnmeldung erhalten, dass Sie ein neues Gerät kaufen müssen, da die Hardware die Mindestanforderungen der Software nicht mehr erfüllt. Oder dass die App, die Sie installieren möchten, ein Update erfordert, das Sie nicht installieren können. Das Gerät selbst funktioniert eigentlich immer noch. Das ist frustrierend für die Nutzenden.

Abbildung 1: Slogan der KDE-Eco-Initiative Opt Green[5],

Viele Menschen nutzen ihr Gerät auch noch, nachdem der Software-Support abgelaufen ist. Ein oft übersehener Punkt ist, dass die Verwendung nicht unterstützter Software eine tickende Zeitbombe ist. Alle Software hat Programmfehler, sogenannte Bugs, viele noch unentdeckt. Sobald sie entdeckt wurden, sind Updates der beste Weg, sie zu reparieren. Nach dem Ende der Sicherheitsupdates bleiben kritische Fehler unrepariert und Nutzende bleiben in Gefahr. Nicht unterstützte Software setzt Sie einer Vielzahl von Bedrohungen aus wie Viren, Ransomware, Trojanern, Spyware, Kryptojacking usw. Ein Problem mit Ihrer Software kann diese verbreiten und andere der gleichen Gefahr aussetzen. Aus diesem Grund veröffentlichen Regierungsbehörden wie das *Bundesamt für Sicherheit in der Informationstechnik (BSI)* Warnungen nach dem Ende des Supports von Software wie Windows 10 (BSI 2025). Updates sind nicht nur für einzelne Nutzende, sondern auch für die breitere Gesellschaft wichtig.

Software kann ein funktionierendes Gerät unbrauchbar machen und mehr Elektroschrott schaffen. Elektroschrott ist der am schnellsten wachsende Abfallstrom weltweit (World Economic Forum 2019). Elektroschrott ist giftig und schädlich für die Menschen und die Umwelt, in der sie leben. Schlimmer noch, ein funktionierendes Gerät wegzuwerfen, bedeutet, ein neues zu produzieren. Die Produktion hat oft auch enorme soziale Kosten unter miserablen Arbeitsbedingungen. Einige sind illegal, wie der Einsatz von Kinderarbeit in Kobaltminen.

Freie Open Source Software garantiert von Grund auf Transparenz und Nutzungsautonomie[6]. Dadurch erhalten *Sie* als Nutzende die Kontrolle über *Ihre* Hardware, da unnötige Abhängigkeiten von Herstellern beseitigt werden. Mit Freier Open Source Software können Sie Ihre Geräte so nutzen, wie Sie wollen, und so lange, wie Sie sie brauchen. Es gibt keine Bloatware und Sie können unerwünschter Datennutzung und Werbung (Uijttewaal et al. 2021), die den Energieverbrauch in die Höhe treiben und Ihr Gerät verlangsamen – und gleichzeitig unerwünschtem Schnüffeln in Ihrem Privatleben, einen Riegel vorschieben. Mit Software, die auf Ihre Bedürfnisse zugeschnitten ist und nicht auf die der Hersteller, können Sie Anwendungen wählen, die für die Hardware entwickelt wurden, die Sie bereits besitzen.

Für die Konsumenten sind die Umweltschäden vielleicht *aus den Augen, aus dem Sinn*. Doch die Umwelt spürt die Auswirkungen: vom CO_2, das in die Atmosphäre gepumpt wird, über die Deponien, auf denen unsere ausgedienten Geräte am Ende ihrer Lebensdauer landen, bis hin zur Luft, dem Boden und den Gewässern in ihrer Umgebung – ganz zu schweigen von den Menschen und Tieren. Die *End-of-10*-Kampagne *(https://endof10.org)*, die 2024 vom Opt-Green-Projekt ins Leben gerufen wurde, hatte zum Ziel, Endnutzende weltweit für die Umweltschäden zu sensibilisieren, die durch das Auslaufen des Supports für Windows 10 im Jahr 2025 verursacht werden.

End of 10

Am 14. Oktober 2025 wollte Microsoft den Support für Windows 10 einstellen. Seit Beginn der Kampagne hat Microsoft das Ende des Supports um ein Jahr bis zum 13. Oktober 2026 verlängert. Zu diesem Zeitpunkt wird Microsoft keine Updates mehr für das System bereitstellen, was schätzungsweise 200 bis 400 Millionen Laptops und Computer weltweit zu Sicherheitsrisiken oder stark umweltbelastendem Elektroschrott machen wird (Caddy & Jessop 2023).

Abbildung 2: Skulptur „Wertgigant" von HA Schult, die auf den in Haushalten anfallenden Elektroschrott aufmerksam macht. Foto: Axel Hindemith, CC BY-SA 3.0

Aus der Perspektive des durchschnittlichen Nutzenden gibt es zwei Optionen: entweder die weitere Nutzung eines nicht mehr unterstützten Betriebssystems mit den damit verbundenen Sicherheitsrisiken oder der Kauf eines neuen Computers. Und Microsoft möchte wirklich, dass Windows-10-Nutzende neue Hardware kaufen. Tatsächlich hat das Unternehmen Vollbild-Benachrichtigungen auf den Bildschirmen der Nutzenden eingeblendet (Cunningham 2024), um sie genau dazu zu ermutigen – selbst bei Computern, die auf Windows 11 aktualisiert werden können.

Die Installation eines neuen Betriebssystems erscheint den meisten Menschen schwierig, doch die Community hinter *End of 10* wollte dabei helfen. In Städten und Gemeinden rund um den Globus standen und stehen Menschen und Organisationen bereit, um bei der Installation zu helfen oder sogar Linux für andere zu installieren. Das war das Hauptziel von *End of 10*: normale Nutzende mit fachkundigen Helfenden zu verbinden, ganz gleich, wo sie wohnen. Seit Mai 2025 wurden über 1000 Orte und Veranstaltungen von Freiwilligen aus Reparaturkollektiven, MakerSpaces, FabLabs, Linux-User-Groups und unabhängigen Computerläden im *End-of-10*-Verzeichnis gelistet. Jede Woche kommen weitere hinzu.

Wer sich für Linux entscheidet, erhält ein aufgerüstetes System für den täglichen Gebrauch, und derselbe Rechner kann noch jahrzehntelang funktionieren. Die meisten Bedenken gegenüber Linux sind mittlerweile überholt oder unbegründet – und mit ein wenig Hilfe bleiben die Geräte der Nutzenden auch weit über das Ende von Windows 10 hinaus sicher, oft ohne Kosten. Neben der Verringerung der Umweltbelastung hat die End-of-10-Kampagne fünf Gründe für ein Upgrade auf Linux aufgezeigt:

1. *Keine neue Hardware, keine Lizenzgebühren:* Ein neuer Laptop kostet viel Geld, aber die meisten Linux-Betriebssysteme stehen gratis zur Verfügung. Software-Aktualisierungen sind ebenfalls kostenlos – für immer.

2. *Verbesserte Privatsphäre:* Windows kommt mit viel Werbung und Spyware. Dies verlangsamt Ihren Computer, ermöglicht es Unternehmen Sie auszuspionieren und erhöht Ihre Stromrechnung.

3. *Gut für unseren Planeten:* Ein funktionierendes Gerät länger zu behalten, ist eine sehr wirksame Methode, um Emissionen zu verringern.

4. *Gemeinschaftliche & professionelle Unterstützung:* Lokale Repair Cafés, unabhängige professionelle Angebote und Computergeschäfte stehen bereit, um Sie zu unterstützen. Auch in Online-Foren gibt es Hilfe.

5. *Mehr Kontrolle für die Nutzenden:* Linux gibt Ihnen die vier Software-Freiheiten: Sie können Programme nutzen, untersuchen, teilen und verbessern, so lange Sie möchten. Sie haben die Kontrolle über Ihr Gerät.

Gamer und Gamerinnen fragen sich vielleicht auch: Können sie ihre Spiele unter Linux spielen? Ja, das können sie, und es war noch nie so einfach. Tausende beliebter AAA-Spiele laufen mittlerweile reibungslos unter Linux, und in vielen Fällen ist die Leistung genauso gut oder sogar besser als unter Windows, insbesondere auf älterer Hardware.

Einige Nutzende haben bereits einen neuen Computer mit vorinstalliertem Windows gekauft, wollten aber stattdessen Linux darauf installieren. Wussten Sie, dass Sie, wenn Sie Linux oder ein anderes Betriebssystem bevorzugen, dennoch für Windows bezahlen, auch wenn Sie es gar nicht nutzen? Das ist unfair und in den meisten Fällen intransparent. *Refund4Freedom* ist eine Initiative der Free Software Foundation Europe, die das Recht der Konsumenten verteidigt, ihr Betriebssystem frei zu wählen und Rückerstattungen für ungenutzte vorinstallierte Software – insbesondere Microsoft Windows – auf neuen Computern zu erhalten. Die im Mai 2025 gestartete Initiative konzentrierte sich zunächst auf den italienischen Markt, wird aber auf andere Regionen ausgeweitet. Erfahren Sie hier mehr: *https://refund4freedom.org/*.

Wir sollten für eine Zukunft kämpfen, in der Nutzende jede beliebige Software auf jeder beliebigen Hardware installieren können. Es ist schließlich unsere Hardware! *Device Neutrality*, eine ebenfalls von der Free Software Foundation Europe ins Leben gerufene Initiative, zielt darauf ab, Nutzenden zu ermöglichen, *Gatekeeper* zu umgehen, um Software – einschließlich Freier Open Source Software – auf ihren Geräten diskriminierungsfrei nutzen zu können. Erfahren Sie hier mehr: *https://fsfe.org/activities/deviceneutrality/index*.

Abbildung 3: KDE-Developer-Maskottchen[7]

Mehrere Organisationen aus den Bereichen Freie Open Source Software sowie Reparaturdienste haben die *End-of-10*-Kampagne unterstützt, darunter: anstiftung.de, iFixit, Repair Cafe International, Right To Repair Europe, Runder Tisch Reparatur, Computertruhe e. V., Free Software Foundation Europe, Software Freedom Conservancy, und viele mehr. Natürlich auch FIfF e. V.! Möchten Sie mitmachen? Die Kampagne lebt von Menschen wie Ihnen. Weitere Informationen finden Sie unter „Beitragen“ auf der Website der Kampagne: *https://endof10.org/de/contribute/*.

In Kürze werden wir ein Handbuch des KDE-Eco-Projekts zur Rolle von Software für ökologische Nachhaltigkeit sowie eine Anleitung veröffentlichen, wie Freie Open Source Software für alle Nutzenden zugänglich gemacht werden kann. Behalten Sie die folgende Seite im Auge: *https://eco.kde.org/grow-green/*.

Joseph P. De Veaugh-Geiss

Joseph P. De Veaugh-Geiss ist der Community-Manager des *KDE-Eco-Projekts*. Das Ziel von KDE Eco ist es, Nachhaltigkeitsziele im Rahmen der Entwicklung und Einführung Freier Open Source Software zu stärken.

Über KDE Eco

Wer steckt hinter der KDE Eco Initiative? Der Freie Open Source Software Verein KDE e. V.! KDE ist eine globale Gemeinschaft von Softwareentwickelnden, Kunstschaffenden, Übersetzenden und Kreativen, die sich der Entwicklung von Freier Open Source Software verschrieben haben. Wir sind eine kooperative Organisation. Wir arbeiten zusammen, um die weltweit beste Freie Open Source Software zu entwickeln. Jeder Mensch ist willkommen, mitzumachen und zu KDE beizutragen – auch Sie. Erfahren Sie hier mehr: *https://community.kde.org/Get_Involved*

Das Opt-Green-Projekt wurde gefördert durch das Umweltbundesamt und das Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz. Die Mittelbereitstellung erfolgt auf Beschluss des Deutschen Bundestages. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Autorinnen und Autoren.

Referenzen

Bundesamt für Sicherheit in der Informationstechnik (BSI) (2025): „BSI empfiehlt Upgrade oder Wechsel des Betriebssystems nach Supportende von Windows 10“: https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2025/250414_Windows10_Ende.html [abgerufen am 8.4.2026]

Caddy, Ben, Kieren Jessop (2023): „The end of Windows 10 support could turn 240 million PCs into e-waste“, Canalys Insights: https://web.archive.org/web/20250820092334/https://www.canalys.com/insights/end-of-windows-10-support-could-turn-240-million-pcs-into-e-waste [abgerufen am 20.8.2025]

Cunningham, Andrew (2024): „Microsoft pushes full-screen ads for Copilot+ PCs on Windows 10 users“, Ars Technica: https://arstechnica.com/gadgets/2024/11/microsoft-pushes-full-screen-ads-for-copilot-pcs-on-windows-10-users/ [abgerufen am 8.4.2026]

Logic, Scott (2024): „Hardware Life Cycle Emissions“, Technology Carbon Standard: https://www.techcarbonstandard.org/technology-categories/lifecycle [abgerufen am 8.4.2026]

Prakash, Siddharth, Ran Liu, Karsten Schischke, Dr. Lutz Stobbe (2012): „Zeitlich optimierter Einsatz eines Notebooks unter ökologischen Gesichtspunkten“, Heidrun Moser, Maike Janßen, Marina Köhn (Hrsg.), Dessau-Roßlau: Umweltbundesamt.: https://www.oeko.de/oekodoc/1583/2012-439-de.pdf

Uijttewaal, Meis, Geert Bergsma, Thijs Scholten (2021): „Carbon footprint of unwanted data-use by smartphones: An analysis for the EU“, Delft: CE Delft: https://groenlinks.nl/sites/groenlinks/files/2021-09/CE_Delft_210166_Carbon_footprint_unwanted_data-use_smartphones.pdf

World Economic Forum (2019): „A New Circular Vision for Electronics, Time for a Global Reboot“: http://www3.weforum.org/docs/WEF_A_New_Circular_Vision_for_Electronics.pdf

Anmerkungen

1 *https://eco.kde.org/de/blog/2022-01-25-resource-efficient-software-and-blauer-engel-eco-certification/*
2 *https://community.kde.org/Goals/Sustainable_Software*
3 *https://eco.kde.org*
4 *https://www.umweltbundesamt.de/das-uba/was-wir-tun/foerdern-beraten/verbaendefoerderung/projektfoerderungen-projekttraeger/opt-green-nachhaltige-software-fuer-nachhaltige*
5 *Bild von Karanjot Singh, veröffentlicht unter einer CC BY 4.0 Lizenz. Quelle: https://eco.kde.org/de/blog/2024-05-29_introducing-ns4nh/*
6 *https://fsfe.org/freesoftware/index.de.html*
7 *Quelle: https://community.kde.org/File:Mascot_konqi-app-dev.png*

Anton Ballmeier, Philip Engelbutzeder, *Foodsharing & IISI, Uni Siegen*

Digitale Souveränität von unten: Selbstorganisation digitaler Räume

Die meisten digitalen Räume, in denen wir viel Zeit verbringen, haben eins gemeinsam: Über die Gestaltung der Plattform entscheiden einige wenige, denen diese Plattformen gehören. Am Beispiel der ehrenamtlich betriebenen Online-Plattform foodsharing.de *zeigt sich, was digitale Souveränität in selbstorganisierten Gruppen bedeuten kann – und was das mit unserer Demokratie zu tun hat.*

Digitale Souveränität ist in aller Munde. Deutschland investiert massiv in neue Rechenzentren (Bundesregierung 2026). Staatliche Akteure beginnen zu verstehen, dass die öffentliche Verwaltung nicht von Software abhängen darf, die von einzelnen Tech-Giganten jederzeit entzogen werden kann (IT-Planungsrat 2021). Unternehmen (zumindest die, die selbst nicht groß genug sind, um Teil des Problems zu sein) versuchen sich mit mittelmäßigem Erfolg von SaaS (Software as a Service)[1] und Vendor Lock-ins[2] zu verabschieden. Und immer mal wieder führt dieses gesteigerte Bewusstsein dazu, dass Privatpersonen, der Gewohnheit und Netzwerkeffekten[3] zum Trotz, WhatsApp und Windows zugunsten von Signal und Linux hinter sich lassen.

Warum erfährt digitale Souveränität gerade jetzt einen solchen Zuspruch? Die Abhängigkeit von Big Tech und ihre Marktkonzentration waren auch vor 10 Jahren schon ein großes Problem. Ebenso die bedenklichen Datenschutzpraktiken und Überwachung im Netz. Und dass die meisten Nutzer:innen *das Internet* immer weniger als pluralistischen Haufen kleinerer Webseiten erleben, sondern als Oligopol weniger gigantischer Plattformen, an denen man aufgrund von Netzwerkeffekten kaum vorbei kann, ist als Entwicklung auch nicht gerade neu.

Sind *unsere* digitalen Räume antidemokratisch?

Vielleicht brauchten wir drastischere Weckrufe. Spätestens, seitdem sich bei Trumps zweitem Amtsantritt die gesamte Riege US-amerikanischer Tech-Milliardäre (bewusst ohne *:innen*) hinter ihn gestellt hat (wörtlich und im übertragenen Sinne), ist ziemlich offensichtlich, dass Big-Tech jedenfalls nicht die Demokratie gegen neofaschistische Strömungen verteidigen wird. Seitdem hat Microsoft durch eine Sperrung von E-Mail-Konten den Internationalen Strafgerichtshof behindert (etes 2025), Meta Faktenchecks abgeschafft (Deutschlandfunk 2025), und Elon Musk einfach ganz offen einen Hitlergruß gezeigt, nachdem er Nazis und Verschwörungstheoretiker:innen zurück auf Twitter (jetzt X) willkommen heißt (*netzpolitik.org* 2022).

Ob nun am Beispiel von Facebook oder X, es wird deutlich, dass die Macht über die Regeln einer Plattform nicht nur wirtschaftlich sondern auch politisch ausgenutzt werden kann. Die digitalen Räume, die nach wie vor an Bedeutung gewinnen, und in denen wir immer mehr Zeit verbringen, sind also nicht neutral. Sie sind geprägt durch die Regeln, die von den Besitzer:innen dieser Räume festgelegt werden. Und diese Regeln sind kaum die einer freiheitlich-demokratischen Gesellschaft.

Brauchen wir also einfach neue, bessere Plattformen, auf denen andere Regeln herrschen — und Problem gelöst? Wir fürchten nein. Denn auch bevor die *Enshittification*[4] großer Plattformen so richtig Fahrt aufgenommen hat, und auch vor den riesigen Desinformationskampagnen auf Facebook zur US-Wahl 2016 (Spiegel 2017), hatten beinahe alle größeren Plattformen eins gemeinsam: Sie sind im Kern undemokratisch! Denn anders, als wir es in einer demokratischen Gesellschaft gewohnt sind (oder zumindest sein sollten), hatten und haben wir in diesen digitalen Räumen kein strukturell verankertes Mitspracherecht. Weder darüber, welche Regeln dort gelten, wer welche Berechtigungen (d. h. Macht) hat, und wie mit unseren Ressourcen (d. h. persönlichen Daten) umgegangen wird.
Ständig müssen wir AGB- oder Datenschutz-Updates zustimmen, ohne eine echte Wahl zu haben. Und jedes Mal werden wir mehr daran gewöhnt, dass digitale Räume und demokratische Mitbestimmung nicht zusammengehören.

Aber wie sähe eine digital souveräne, demokratische Gemeinschaft aus? Wie würde sie ihre Regeln festlegen, ihre Infrastruktur pflegen, welche Daten würde sie erheben und wie damit umgehen, …?

Nun, bevor ihr euch zu viele Hoffnungen macht: Wir wissen es nicht. Was wir aber wissen, ist, wie eine Plattform aussieht, die seit knapp 15 Jahren von ihrer Community selbst betrieben, weiterentwickelt und mit Leben gefüllt wird. Eine Plattform, die viele, wenn vielleicht auch nicht alle Kriterien digitaler Souveränität erfüllt, und die uns als Praxisbeispiel dienen kann, was demokratische Mitbestimmung in digitalen Räumen bedeuten kann — und wo sie auf Schwierigkeiten stößt.

Eine Bewegung, die ihre Plattform selbst betreibt

Die Plattform, von der wir schreiben, ist *foodsharing.de*. Und obwohl Anton als einer ihrer Entwickler sie sehr oft aus einer technischen Perspektive betrachtet, ist zunächst mal wichtig klarzustellen, dass foodsharing keine Organisation ist, die sich vorwiegend mit Digital- und IT-Fragen beschäftigt. Bei foodsharing geht es – wie der Name vermuten lässt – darum, Lebensmittel zu teilen, die andernfalls von unserem Ernährungssystem verschwendet worden wären. In Deutschland, Österreich und der Schweiz sind dazu Hunderttausende komplett ehrenamtlich als *Foodsaver:innen* aktiv geworden, indem sie überschüssige Lebensmittel aus Bäckereien, Supermärkten, Kantinen usw. abholen und sicherstellen, dass sie gegessen werden, statt im Müll zu landen.

Dabei setzt foodsharing nicht auf zentrale Strukturen, wie eigene Lagerhäuser oder Lieferwagen, sondern koordiniert sich dezentral. So kümmert sich ein eigenes Team möglichst ortsansässiger Lebensmittelretter:innen um die Abholungen jedes Kooperationsbetriebs.

Neben all den logistischen Herausforderungen, welche allein die Organisation von mehreren Millionen jährlichen Lebensmittelrettungen mit sich bringt, arbeiten Aktive auch daran, die Ursachen der Lebensmittelverschwendung einzudämmen. Es werden also nicht nur bereits überproduzierte Lebensmittel verwendet, sondern verschiedene Arbeitsgruppen organisieren politische Kampagnen, Öffentlichkeits- oder Bildungsarbeit.

Das, was diese riesige, dezentrale Bewegung zusammenhält, der (digitale) Raum, wo sich all diese Menschen versammeln, ist die online-Plattform foodsharing.de. Betrieben wird diese Plattform seit foodsharings Gründung 2012 *von der Community selbst*. Die Organisation ist damit *unabhängig* und schafft sich ihren digitalen Raum selbst. Entsprechend ist foodsharing also *digital souverän*. Oder?

Nun ja, ganz so einfach ist es wohl nicht. Denn was bedeutet es überhaupt, dass eine Plattform *von der Community* betrieben wird? Gibt es nicht doch *Abhängigkeiten*, wenn auch gegebenenfalls innerhalb der Gemeinschaft? Und vor allem: was bedeutet *digitale Souveränität* überhaupt für eine gemeinnützige Organisation?

Digitale Souveränität jenseits von Individuum, Markt und Staat

Wie so oft bei viel verwendeten *buzz words* bleibt die Begriffsdefinition etwas unscharf. Denn je nach Handlungsebene bzw. Akteur:in meint das Konzept etwas anderes. Oft werden daher drei Ebenen digitaler Souveränität betrachtet – Staat, Wirtschaft & Individuum (Pohle 2021). Foodsharing passt aber in keine dieser Kategorien. Selbstorganisierte Gruppen, deren gemeinsames Ziel etwas anderes ist als ökonomische Gewinnmaximierung, finden in klassischen Definitionen digitaler Souveränität keinen Platz.

Dabei könnten gerade dort einige Aspekte digitaler Souveränität und Selbstbestimmung besonders greifbar werden: Denn wo weder Marktanreize noch staatliche Regulierung die Gestaltung digitaler Infrastruktur dominieren, müssen Fragen von Kontrolle, Abhängigkeit und Verantwortung unmittelbar von der Gemeinschaft selbst beantwortet werden – im Unterschied zu isolierten Individuen, die für sich genommen digitale Infrastrukturen überhaupt nicht wesentlich mitzugestalten vermögen.

Lasst uns also einen Blick darauf werfen, wie die digitale Infrastruktur hinter foodsharing entworfen, umgesetzt und instandgehalten wird, und welche Hürden sich dabei in den Weg stellen.

Community-getriebene Plattformentwicklung – zwischen Mitgestaltung und Konsument:innenmentalität

Zurück also zur Frage, was eigentlich damit gemeint ist, wenn wir schreiben, die foodsharing-Plattform werde *von der Community selbst* betrieben.

Die Software hinter foodsharing.de wird schon lange als Open-Source-Projekt ehrenamtlich weiterentwickelt. Wer die entsprechenden Fähigkeiten hat, kann sich also daran beteiligen, den gemeinsamen digitalen Raum zu formen. Ein paar *Maintainer:innen* achten zwar darauf, dass technische und rechtliche Standards eingehalten werden, und neue Entwicklungen nicht den Grundwerten der Organisation widersprechen, darüber hinaus sind Entwickler:innen aber recht frei darin zu entscheiden, welche Themen sie bearbeiten.

Gleichzeitig kann natürlich ein sehr großer Teil der Community nicht selbst programmieren, soll aber von der Mitgestaltung der Plattform nicht ausgeschlossen werden. Hierfür gibt es das überregionale *Produktteam*, eine Arbeitsgruppe, die quasi als kollektiver *Product Owner* fungiert. Hier werden Ideen eingebracht, diskutiert, abgestimmt und priorisiert. Auch wenn die Entscheidungen des Produktteams genau genommen nicht bindend für die Entwickler:innen sind, sind sie ganz maßgeblich dafür, was tatsächlich umgesetzt wird. Für die Nutzer:innen interessante, also nicht rein technische Änderungen, werden mittlerweile immer im Produktteam besprochen und ausgearbeitet.

Nutzer:innen haben also nicht nur die Möglichkeit, direkt am Code mitzuarbeiten, sie haben auch niedrigschwellige Gestaltungsmöglichkeiten, für die kein technisches Fachwissen notwendig ist.

Entsteht dadurch eine digital mündige, souveräne Gemeinschaft? Nun, wir halten es für eine notwendige, aber keine hinreichende Bedingung. Denn nach wie vor sind die meisten gewohnt, Software nur zu konsumieren. Wir stören uns zwar an bestimmten Design-Entscheidungen, vermissen Funktionen oder finden *Bugs*, kommen aber gar nicht auf die Idee, dass wir selbst daran etwas ändern könnten.

Erst, wenn wir die Konsument:innenmentalität in Bezug auf digitale Räume hinter uns lassen, und diese Räume stattdessen als Gegenstand kollektiver Mitgestaltung begreifen, kann die Bewegung digital souverän werden. Denn andernfalls liegen Entscheidungen über die Gestaltung und Regeln der digitalen Räume trotzdem bei wenigen Personen, von denen die Community dann abhängig wäre. Erst durch *Governance*, Vermittlungsarbeit, *Onboarding* und Wissensweitergabe wird aus technischer Offenheit also reale Souveränität.

Die unsichtbare Arbeit hinter digitalen Infrastrukturen

Eine Plattform zu betreiben heißt natürlich nicht nur, neue Funktionen zu entwickeln. Damit die Software überhaupt läuft, braucht es Infrastruktur: Ein Server, auf dem sie betrieben wird, Fehlerbehebungen, regelmäßige Backups, Updates, um Sicherheitslücken zu schließen, sowie Optimierungen, wenn steigende Nutzer:innenzahlen das bestehende System an seine Grenzen bringen. All diese Aufgaben sind essenziell, um die Plattform auf Dauer betreiben zu können. Gleichzeitig bleiben solche Instandhaltungsaufgaben meist unsichtbar und erfahren wenig Wertschätzung.

In klassischen Unternehmen ist das kein strukturelles Problem. Wartung und Betrieb werden schlicht als notwendige Kosten eingeplant, und es gibt bezahlte Stellen, die sich darum kümmern. In einer weitgehend geldfrei organisierten Bewegung wie foodsharing ist das keine Option. Hier konkurriert die unsichtbare Pflegearbeit mit der Programmierung neuer Funktionen. Letztere bietet Entwickler:innen nicht nur mehr Gestaltungsspielräume, sondern erfährt auch sehr viel mehr Wertschätzung aus der Community.

Wenn sich dadurch zu wenige Personen um Betrieb und Wartung kümmern, entstehen Überlastung, Wissenskonzentration bei einzelnen Personen, und vor allem Unzufriedenheit. Und auch wenn foodsharing in seiner sehr weitreichenden Geldfreiheit doch eine Ausnahme darstellen dürfte, entstehen vergleichbare Situationen leicht auch in anderen nicht-kommerziell betriebenen IT-Projekten. Die größten Bedrohungen digitaler Souveränität liegen also nicht unbedingt nur im Einfluss von außen, sondern in der inneren Prekarität. Um so wichtiger ist es, solche Aufgaben auf viele Schultern zu verteilen und Strukturen zu schaffen, in denen aufkommende Frustration gehört und bearbeitet werden kann. Nicht zuletzt muss aber auch die Community über die Wichtigkeit dieser Aufgaben aufgeklärt werden, um eine gesteigerte Anerkennung von Pflegearbeit zu erreichen.

Die Geldfreiheit der Plattform bringt aber nicht nur Schwierigkeiten mit sich, sondern eröffnet auch neue Möglichkeiten, die von kommerziellen Plattformbetreiber:innen wohl kaum in Betracht gezogen werden. Zunächst gibt es auf foodsharing keine Werbung. Wenn aber keine Werbefläche verkauft wird, gibt es erstmal auch kein Interesse daran, Nutzer:innenverhalten zu tracken und auszuwerten, um Werbung besser personalisieren zu können. Auch ist es hier kein Ziel, die Aufmerksamkeit der Nutzer:innen möglichst lange zu binden. Im Gegenteil: Ziel ist es, Menschen zu motivieren, im analogen Raum aktiv zu werden, statt sie länger als nötig auf der Plattform zu halten.

Diese Logik hat direkte technische Konsequenzen. Eine Plattform, die keine datenintensiven Geschäftsmodelle verfolgt, kommt mit deutlich weniger Hardware aus. Die komplette foodsharing-Plattform läuft auf einem Server, der vergleichbar ist mit dem recht durchschnittlichen Laptop, auf dem wir diesen Text hier tippen. Und wenn die Serverkapazitäten doch mal knapp werden, wird eben die Software aufgeräumt und optimiert (während die nächste KI-Firma gleich ein neues Rechenzentrum baut).

Effizienz, Datensparsamkeit, Werbefreiheit und der Verzicht auf Profiling sind hier nicht nur Fragen des Datenschutzes oder der digitalen Souveränität im engeren Sinne. Sie sind Ausdruck einer alternativen politischen Ökonomie digitaler Infrastruktur – einer, die nicht auf Wachstum und Extraktion setzt, sondern auf gemeinschaftliche Nutzung und bewusste Begrenzung.

Digitale Souveränität in selbstorganisierten Gruppen

Was also ist nun digitale Souveränität in selbstorganisierten Gruppen? Für uns bedeutet sie vor allem infrastrukturelle Selbstregierung. Die Fähigkeit, (digitale) Kommunikations-, Koordinations- und Entscheidungsinfrastrukturen selbstbestimmt zu gestalten. Sie bedeutet, digitale Infrastrukturen durch demokratische Mitgestaltung so zu formen und aufrechtzuerhalten, dass sie den normativen Zielen der Gemeinschaft entsprechen. Open Source ist dabei zwar ein wichtiger Baustein, aber bei weitem nicht hinreichend. Erst durch Governance, Vermittlungsarbeit, Onboarding, Wissensweitergabe und die Anerkennung von Pflegearbeit kann aus technischer Offenheit reale Souveränität werden. Denn digitale Souveränität entsteht nicht primär durch Besitz, Kontrolle oder Regulierung digitaler Technologien, sondern durch tatsächlich von breiten Teilen der Community gelebte Mitgestaltung.

Und mit diesem Bild vor Augen zeigt sich vielleicht auch ein Weg heraus aus der heutigen, von Monopolisten geprägten Tech-Landschaft.

Denn die Alternative zu Big Tech muss nicht bloß bessere, offene Technologie sein, sondern vor allem die Möglichkeit, sie gemeinsam zu gestalten. Digitale Souveränität beginnt dort, wo die Macht von Big Tech endet. Nämlich da, wo Systeme nicht nur genutzt, sondern kollektiv aufrechterhalten und verändert werden können.

Referenzen

Bundesregierung (2026): Rechenzentrumsstrategie der Bundesregierung, Digitalministerium [online]. https://dc-intelligence.com/dci/news/meldungen/Rechenzentrumsstrategie_der_Bundesregierung.php [abgerufen am 9.4.2026].

IT-Planungsrat (2021): Strategie zur Stärkung der digitalen Souveränität für die IT der öffentlichen Verwaltung [online]. https://www.it-planungsrat.de/fileadmin/beschluesse/2021/Beschluss2021-09_Strategie_zur_Staerkung_der_digitalen_Souveraenitaet.pdf [abgerufen am 9.4.2026].

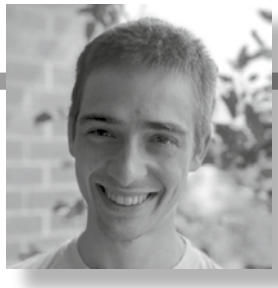
etes (2025): Microsoft E-Mail Sperre am IStGH zeigt digitale Abhängigkeit, etes.de [online]. https://www.etes.de/blog/microsoft-e-mail-sperre-am-istgh-zeigt-digitale-abhaengigkeit [abgerufen am 10.4.2026].

Deutschlandfunk (2025): Meta schafft Faktencheck ab – Vor Trump eingeknickt? [online]. https://www.deutschlandfunk.de/meta-instagram-facebook-zuckerberg-faktencheck-beschraenkungen-100.html [abgerufen am 10.4.2026].

netzpolitik.org (2022): Twitter-Amnestie: Elon Musk holt die Rechtsextremen zurück [online]. https://netzpolitik.org/2022/twitter-amnestie-elon-musk-holt-die-rechtsextremen-zurueck [abgerufen am 10.4.2026].

Spiegel 2017: US-Wahl 2016: Wie soziale Medien Werbung zu Propaganda machten. Spiegel Online [online]. https://www.spiegel.de/netzwelt/web/us-wahl-2016-wie-soziale-medien-werbung-zu-propaganda-machten-a-1175906.html [abgerufen am 9.4.2026].

Pohle, Julia (2021): Digitale Souveränität. Ein neues digitalpolitisches Schlüsselkonzept in Deutschland und Europa? Berlin: Wissenschaftszentrum Berlin für Sozialforschung.



Anton Ballmaier und Philip Engelbutzeder

Anton Ballmaier ist Software- und Organisationsentwickler der gemeinnützigen Initiative *foodsharing*. In der Sozio-Informatik der Universität Siegen forscht er zu Gerechtigkeitsfragen in digitalen Räumen sowie Plattformdesigns zur Unterstützung sozialer Bewegungen.

Dr. **Philip Engelbutzeder** ist Wissenschaftler an der Universität Siegen an der Schnittstelle von Sozio-Informatik und Pluraler Ökonomie und forscht zu alltäglichen, nachhaltigen Lebensmittelpraktiken, insbesondere zur Unterstützung des Rettens und Teilens sowie zur gesellschaftlichen Rolle von Informations- und Kommunikationstechnologien. Als Aktionsforscher arbeitet er seit vielen Jahren mit Graswurzelbewegungen zusammen, sowohl mit Entwickler:innen von Open-Source-Anwendungen als auch mit lokalen Gemeinschaften, die diese nutzen.

Anmerkungen

1 *Software as a Service beschreibt cloudbasierte Software-Lösungen, die als Abonnement bereitgestellt und bezahlt werden. Dabei haben Kund:innen oft mangelnde Kontrolle über ihre Daten und Systeme, da sie beim Anbieter lagern und jederzeit gekündigt oder eingeschränkt werden können.*

2 *Vendor Lock-in bezeichnet die Abhängigkeit von einem einzigen Anbieter, beispielsweise durch proprietäre Standards, Verträge oder Datenformate, die einen Wechsel zu Alternativen technisch, finanziell oder organisatorisch stark erschweren.*

3 *Als Netzwerkeffekt beschreibt man das Phänomen, dass der Nutzen einer Plattform mit der Zahl ihrer Nutzer:innen zunimmt. Ein einfaches Beispiel sind Messenger, die erst durch die Vielzahl andere Nutzer:innen ihren eigentlichen Nutzen bringen können. Dies erschwert den Wechsel zu Alternativen, da Kontakte das gleiche System nutzen müssen, um weiterhin kommunizieren zu können.*

4 *Mit seiner Wortschöpfung Enshittification beschreibt der Autor Cory Doctorow den Qualitätsverfall digitaler Plattformen durch eine Verschiebung der Wertorientierung: Zunächst werden Nutzer:innen durch ein attraktives Angebot gewonnen, anschließend werden zunehmend die Interessen von Geschäftskund:innen – etwa Werbetreibenden – priorisiert, bevor die Plattform schließlich dazu übergeht, den größtmöglichen Wert für sich selbst abzuschöpfen, bis die Plattform nahezu (aber eben nur nahezu) unbrauchbar wird.*

Anne Mollen, ***Kommunikationswissenschaft, Universität Münster***

Das Unbehagen mit der digitalen Souveränität

Digitale Souveränität ist zum Leitbegriff europäischer Digitalpolitik geworden. Doch was bedeutet Souveränität in einer digitalisierten Welt? Zwischen autokratischen Internet-Shutdowns, europäischen Abhängigkeiten von Digitalunternehmen und zivilgesellschaftlichen Gegenentwürfen zeigt sich: Der Begriff kann nützlich sein, birgt aber Gefahren. Er zielt auf staatliche Handlungsfähigkeit, legitimiert aber gleichzeitig Zentralisierung und droht Pluralität zu untergraben. Dieser Beitrag lotet die Grenzen des Souveränitätsbegriffs aus und fragt, was an seine Stelle treten kann.

Der Zeitpunkt des fast vollständigen Shutdowns iranischer Kommunikationsnetzwerke lässt sich exakt beziffern. Daten zum Internet-Traffic zeigen: Am 8. Januar 2026 um 13:50 Uhr deutscher Zeit kam der Datenverkehr aus dem Iran fasst vollständig zum Erliegen (Belson, 2026). Ebenso betroffen: Telefon- und Mobilfunknetze. Die medienvermittelte Kommunikation im Iran wird seit diesem Zeitpunkt in einem bisher beispiellosen Umfang fast vollständig unterbunden – denn auch drei Monate später bleibt der Zugang zum Internet und weiteren Kommunikationskanälen massiv eingeschränkt.

Internet-Shutdowns gehören weltweit flächendeckend zum Repertoire autokratischer Machtstrategien und Menschenrechtsverletzungen (Ryng et al., 2022). Im Fall des Irans trugen sie direkt nach dem 8. Januar dazu bei, die Massaker an der lokalen Bevölkerung mit vermutlich mehreren zehntausenden Toten zu ermöglichen und zu vertuschen.

In dieser verstörenden Situation adressierten Wissenschaftler:innen und Aktivist:innen einen eindringlichen Appell an die Internationale Fernmeldeunion (engl: International Telecommunication Union, ITU):

> *"In the context of internet shutdowns, the debate over digital sovereignty has reached its limits: when states sever connectivity and kill with impunity, the priority can no longer be sovereignty but ensuring that people can remain connected and in control of their communications." (Akbari et al., 2026)*

Der massive Umfang des Shutdowns im Iran war nur möglich, weil das iranische Regime die Kontrolle über das Internet weitgehend institutionell über einen Telekommunikationsdienstleister zentralisiert (Reuter, 2026). Eine Zentralisierung, die die Handlungs- und damit Repressionsfähigkeit des Regimes ermöglicht. Andere autokratische Regime versuchen eine ähnliche Abschottung durchzusetzen und bezeichnen dies als *souveränes Internet* (Litvinenko, 2021).

Nationalstaatliche Souveränität

Diese Vorstellung eines souveränen Internets unterscheidet sich grundlegend von Diskussionen einer digitalen Souveränität, wie sie aktuell in der Europäischen Union und ihren Mitgliedsländern geführt wird. Im Fokus steht hier der Abbau von Abhängigkeiten gegenüber großen Technologieunternehmen, beispielsweise durch einen Wechsel auf Open-Source-Technologien, wie sie in der *Declaration on European Digital Sovereignty (Digital Austria, 2025)* vereinbart wurde. Dennoch: Bereits vor einigen Jahren haben Julia Pohle und Thorsten Thiel darauf hingewiesen, dass sich in der immer nebulöser werdenden Diskussion rund um digitale Souveränität der Fokus auf staatliche Handlungsfähigkeit in einer digitalen Welt durchsetzt, die durch Abhängigkeiten von großen außereuropäischen Technologieunternehmen geprägt ist (Pohle and Thiel, 2020).

Nicht erst seit den erneuten massiven Einschränkungen im Iran wird diese primär nationalstaatliche Perspektive auf digitale Souveränität kritisch diskutiert: Denn der Souveränitätsbegriff scheint fundamental ungeeignet als normative Zielrichtung einer progressiven Digitalpolitik, wenn er ausschließlich auf eine kollektive Souveränitätszuschreibung an einen staatlichen Akteur zielt – und damit die Zentralisierung von Macht und Gewalt sowie deren Missbrauch ermöglicht.

Die Auswirkungen eines nationalstaatlich fokussierten Souveränitätsbegriffs sind in den EU-Mitgliedsstaaten nicht ansatzweise mit den Repressionen autokratischer Regime zu vergleichen. Wenn in Deutschland digitale Souveränität vor allem nationalstaatlich

verstanden wird, können wir daran kritisieren, dass es dem Digitalministerium erlaubt ist, Souveränitätskriterien aufzuweichen, um von AWS betriebene Cloudinfrastrukturen als souverän darstellen zu können, trotz gegenläufiger rechtlicher Einschätzungen.[1] Oder es lässt sich auf dieser Grundlage kritisieren, wenn Landes-Innenminister:innen versuchen, sich aus der Abhängigkeit von Palantir-Software herauszureden, indem sie zukünftig europäische oder deutsche Data-Mining-Anwendungen in der Polizeiarbeit entwickeln und einsetzen wollen (Jeric and Hagen, 2025). Denn natürlich bleibt auch eine deutsche Kopie einer grundrechtswidrigen Software weiterhin grundrechtswidrig.

Souveränität – what else?

Es gibt also fundamentale Unterschiede zwischen den Gefahren eines zentralisierten Internets in einem autokratischen Regime und nationalstaatlich fokussierten Verständnissen von digitaler Souveränität in demokratischen Systemen. Dennoch birgt eine auf staatliche Handlungsfähigkeit ausgerichtete digitale Souveränität auch in demokratischen Staaten fundamentale Gefahren – denn sie postuliert ebenfalls eine zentralisierte Gestaltung von Digitalisierung.

Wenngleich der Souveränitätsbegriff in der Digitalpolitik daher zunehmend aus guten Gründen sehr kritisch diskutiert wird, möchte ich dennoch argumentieren, dass er weiterhin einen Zweck erfüllt. Denn erstens muss ein demokratischer Nationalstaat angesichts steigender autokratischer Tendenzen und geopolitischer Abhängigkeiten handlungsfähig in Fragen der Digitalisierung sein und damit souverän gegenüber Digitalunternehmen. Zweitens bedeutet dies nicht, dass der Staat die einzige oder auch nur primär handlungsfähige Instanz bleiben sollte. Eine staatliche Souveränität schließt die selbstbestimmte und autonome Gestaltung von Digitalisierung durch Organisationen und Individuen nicht grundsätzlich aus. Drittens, stellt der Souveränitätsdiskurs die Frage, wer der Souverän in der Digitalisierung ist. Wenn die Antwortet lautet: „die großen Digitalunternehmen“ oder die „Nationalstaaten“, müssen wir die demokratische Verfasstheit unserer digitalisierten Gesellschaften schützen. Ein kurzer und zugegebenermaßen vereinfachender Blick in die ideengeschichtlichen Hintergründe des Souveränitätsbegriffs hilft uns an dieser Stelle seine Grenzen auszuloten und zu definieren, wann und wofür wir neue Begriffe entwickeln müssen.

Wer ist der Souverän?

Im Kern sollte für eine Souveränitätsdiskussion zunächst die Frage geklärt werden, wer ist der Souverän bzw. wer sollte es sein? In der Staatstheorie lassen sich verschiedene Perspektiven auf diese Frage abgrenzen. Im Kern der Verhandlung um Souveränität wird immer wieder auf das absolutistische Herrschaftsmodell von Thomas Hobbes verwiesen. Im 17. Jahrhundert entwirft dieser die Idee eines Gesellschaftsvertrags: Um den chaotischen und von Gewalt gezeichneten Naturzustand zu überwinden, in dem Menschen sich ohne Staatsform befänden, übertragen alle Menschen ihre Freiheiten, Rechte und Ansprüche auf Selbstbestimmung in einem Gesellschaftsvertrag an einen absoluten Herrscher, den Souverän. Hobbes entwirft zu diesem Zweck das Bild des Leviathans, eines Seeungeheuers aus der jüdisch-christlichen Mythologie, das sinnbildlich für den allmächtigen Staat steht, der Bürger:innen durch Strafen voreinander und den Staat selbst nach außen schützt.

Die Hobbes'sche Vorstellung ist eine denkbar ungünstige Referenz für das Souveränitätsideal einer modernen Digitalpolitik. Sie verdeutlicht vielmehr, warum digitale Souveränität, wie im Appell an die ITU formuliert, kritisiert werden muss, die nicht von den Menschen gedacht wird, sondern von der absoluten Macht staatlicher Akteure. Liberale Staatstheoretiker hielten dem Hobbes'schen Verständnis entsprechend entgegen, dass basale Rechte, wie beispielsweise das Recht auf freie Meinungsäußerung, vor dem Machtmissbrauch des Souveräns gesichert sein müssten. Zudem muss Herrschaft fortlaufend durch den kollektiven Willen des Volkes zugeschrieben werden. Rousseau formuliert hier am explizitesten den Anspruch einer demokratischen Souveränität, die nicht durch das Übertragen von Macht an gewählte Repräsentant:innen, sondern durch partizipative und direkt-demokratische Elemente als Volkswille ausgefüllt werden sollte.

Das Totalitäre im Souveränen

Dieses demokratische und im Volkswillen verortete Souveränitätsverständnis lässt sich am ehesten mit einer Digitalpolitik vereinbaren, die auf Beteiligung vieler verschiedener Akteur:innen baut. Es stellt sich gegen die Dominanz von Digitalunternehmen und Staaten in der Ausgestaltung von Digitalisierung. Stattdessen lassen sich hier partizipative Technologieentwicklung oder offene Daten, Software und Infrastrukturen als Elemente einer partizipativen Souveränität integrieren. Ein Blick auf die Souve-

Gustave Doré, Bibel mit Luther-Text (1867-1870), Leviathan (Jesaja 27,1)

ränitätskritik von Hannah Arendt trübt hingegen den Optimismus. Sie sieht das Souveränitätskonzept als grundlegend totalitär, da selbst der vereinheitlichende Volkswille von Rousseau einen zentralisierenden und damit pluralitätsfeindlichen Charakter hat (Förster, 2013). Nach Arendt gefährdet Souveränität ein Verständnis von Politik als Aushandlung und Konflikt um vielfältige Perspektiven, Meinungen und Wünsche. Demnach impliziert ein einheitlicher Volkswille die Einschränkung von Freiheit und unterbindet Pluralität als Grundbedingung des Politischen (Arendt, 2024, Original 1963). Damit hat Souveränität, laut Arendt, immer das Potenzial totalitär zu wirken.

Eurozentrismus in Souveränitätsdebatte

Die Diagnose von Arendt ist nicht nur eine intellektuelle Spitzfindigkeit in der politischen Theorie. Sie hilft uns aktuelle Diskussionen zur digitalen Souveränität besser zu verstehen. Denn zu Recht kann man der europäischen Diskussion um digitale Souveränität einen eurozentristischen Fokus vorwerfen, wie es im Zuge des iranischen Shutdowns passierte:

> *"(…) the current wave pushing digital sovereignty as the key to ending dependency on American and Chinese technology is negligent of its Eurocentric bias. Despite democratic and people-centred language, such initiatives basically imply one message: our nationalism is better than yours!" (Akbari, 2026)*

Die Diagnose eines Eurozentrismus ist zutreffend – und nicht ungewöhnlich im europäischen Kontext. Auch vielfache Appelle der Europäischen Union, Digitalisierung und KI menschenzentriert zu gestalten (Europäische Kommission, 2018) beziehen sich in der Regel nur auf Europäer:innen und nicht auf Menschen außerhalb Europas, die beispielsweise seltene Erden für Hardware abbauen und anfallenden Elektroschrott entsorgen (Mollen, 2024b). Das gleiche Muster zeigt sich in der europäischen Diskussion zu digitaler Souveränität – die vor allem die Handlungsfähigkeit der EU-Mitgliedsstaaten gegenüber amerikanischen und chinesischen Digitalunternehmen zum Ziel hat. In dieser Problemdiagnose erfüllt der Souveränitätsbegriff jedoch einen sinnvollen Zweck: Digitalunternehmen sollten niemals die Rolle eines Souveräns in einer digitalisierten Welt einnehmen können. Gleichwohl sollten auch Nationalstaaten nicht die alleinige Handlungsmacht in der Digitalisierung halten dürfen. Und auch eine partizipativ gedachte Souveränität mag letztlich auf Vereinheitlichung und Zentralisierung zielen. Der Appell Hannah Arendts sollte hier nachklingen: Pluralität kann als Leitmotiv einer anti-totalitären Digitalisierung dienen, denn Souveränität schränkt potenziell Freiheit ein. Wenn Souveränitätsbestrebungen also Pluralität in der Digitalisierung unterbinden, müssen wir hellhörig werden.

Selbstbestimmung als individuelles und kollektives Recht

Statt Souveränität lassen sich alternative Konzepte denken, um Pluralität in der Digitalisierung zu stärken. Beispielsweise digitale Selbstbestimmung als „dezentrale und partizipative Gestaltungsprozesse einer Vielzahl von individuellen und kollektiven Akteuren" (Mollen, 2024a). Ein solche Perspektive auf die Gestaltbarkeit von Digitalisierung stände im Widerspruch zu einer Zentralisierung von Macht bei den Digitalunternehmen wie auch bei staatlichen Akteur:innen. Sie war handlungsleitend in der Etablierung der ersten Internetangebote überhaupt – und bleibt dies weiterhin in vielen aktuellen Digitalisierungsbewegungen: Unter anderem in der Diskussion zur Nachhaltigkeit und Digitalisierung.

Gegen die Kommodifizierung der Klimakrise

Die Klimakrise ist ein Beispiel, an dem sich die Spannungen zwischen zentralisierten und pluralen Gestaltungsansprüchen in der Digitalisierung konkret beobachten lassen. Große Internetunternehmen versuchen zunehmend, ein datengetriebenes Verständnis von Nachhaltigkeit zu etablieren. Sie positionieren ihre digitalen Infrastrukturen und Anwendungen als Lösung für die sozial-ökologische Transformation, indem sie beispielsweise Nachhaltigkeit primär als ein Effizienz- und Optimierungsproblem definieren: So ließen sich mit umfassenden Datenanalysen und automatisierten Anwendungen beispielsweise ausreichend CO_2-Einsparungen in Produktionsprozessen umsetzen (Laaksonen and Frig, 2026; Sridharan, 2026). Dieses Narrativ pushen die großen Technologieunternehmen massiv auf europäischer Ebene – beispielsweise Google in dem EU-Policy-Papier *The AI Opportunity for Europe's Climate Goals*, das im Kern eine Botschaft transportiert: Die Klimakrise lässt sich durch den massiven Einsatz von KI-Technologien bewältigen, wenn die politischen Rahmenbedingungen stimmen – also wenn der Staat den Weg für die Lösungen der Technologieunternehmen frei macht. Nachhaltigkeit wird so zu einem weiteren Markt, auf dem Digitalunternehmen Deutungshoheit und Infrastrukturmacht beanspruchen – und so Abhängigkeiten schaffen. Über diese Abhängigkeiten wird die Klimakrise zu einem Geschäftsmodell.

Techsolutionismus statt pluraler Gestaltung

Für nationalstaatliche Akteur:innen ist dieser Techsolutionismus attraktiv, weil er sie vermeintlich von einer weitaus anspruchsvolleren Aufgabe entbindet: der politischen Gestaltung komplexer gesellschaftlicher Transformationsprozesse hin zu nachhaltigeren Zukünften. Anstatt extraktivistische Lebens- und Wirtschaftsweisen grundlegend in Frage zu stellen, können Regierungen ihren Bürger:innen signalisieren, dass technologische Innovation den notwendigen Wandel übernimmt – ohne schmerzhafte Veränderungen im Alltag. Digitalisierung wird so nicht zum Werkzeug einer gesellschaftlichen Transformation, sondern zu deren Ersatz. Zugleich läuft der Staat in dieser Konstellation Gefahr, Gestaltungsmacht an dieselben Unternehmen zu übertragen, von denen er sich eigentlich unabhängig machen möchte – ein Widerspruch, der im Souveränitätsdiskurs bisher nicht ausreichend adressiert wird.

Selbstbestimmung für Nachhaltigkeit

Dabei wird eine nachhaltige Digitalisierung durch aktuelle politische Weichenstellungen eher unmöglich gemacht als gefördert. Statt plurale und selbstbestimmte digitale Angebote zu stärken, entstehen flächendeckend neue digitale Abhängigkeiten von großen Anbietenden – und damit genau jene Lock-in-Effekte,

die der Souveränitätsdiskurs eigentlich adressieren sollte. Es sind zivilgesellschaftliche Akteur:innen wie *Bits & Bäume*, die seit Jahren alternative Digitalisierungspfade skizzieren. Sie zeigen, dass eine nachhaltige Digitalisierung auf öffentlichen Infrastrukturen, Dezentralität, Offenheit und bewusster Nicht-Skalierbarkeit aufbauen muss, statt auf der Logik großer Plattformen und zentralisierter staatlicher Steuerung.

Unter dem Leitmotiv der Selbstbestimmung haben wir aus diesem Grund als Teil von *Bits und Bäume NRW* politische Forderungen zur nachhaltigen Gestaltung der Digitalisierung an die Landesregierung NRW gestellt (Bits und Bäume NRW, 2026). Unsere Forderungen stützen den Anspruch auf Pluralität in der Digitalisierung – jene Pluralität, die Hannah Arendt als Gegenpol zu souveräner Vereinheitlichung einfordert. Sie zeigen, dass digitale Selbstbestimmung nicht nur ein abstraktes Konzept ist, sondern in konkreten Praktiken gelebt wird – in offener Software, in gemeinwohlorientierter Infrastruktur, in der Weigerung, die Gestaltung einer nachhaltigen Digitalisierung an Unternehmen oder Staaten zu delegieren. Gerade im Kontext der Klimakrise wird damit deutlich: Weder Digitalunternehmen noch Nationalstaaten sollten definieren, was nachhaltige Digitalisierung bedeutet und wie sie umgesetzt wird. Denn wenn Nachhaltigkeit zum Geschäftsmodell weniger Unternehmen wird und der Staat dies als souveräne Strategie übernimmt, reproduziert sich genau jene Zentralisierung von Macht, die der Souveränitätsdiskurs in anderen Bereichen kritisiert.

Referenzen

Akbari, Azadeh et al. (2026) Iran: When the internet is shut down, gunfire begins. https://docs.google.com/forms/d/e/1FAIpQLSex2DNzJv1nOWXNXpEIIIvvJyd1xZhJRg0y8GcmGOfkqdPd6g/viewform, abgerufen am 26.4.2026.

Akbari, Azadeh. (2026) Iran's Case Should Put an End to Illusions About Digital Sovereignty. TechPolicy.Press, https://www.techpolicy.press/irans-case-should-put-an-end-to-illusions-about-digital-sovereignty/, abgerufen am 26.4.2026.

Arendt, Hannah (2024, Original 1963) Über die Revolution. Erweiterte Neuausgabe, 3. Auflage. München: Piper.

Belson, David (2026) What we know about Iran's Internet shutdown, The Cloudflare Blog, https://blog.cloudflare.com/iran-protests-internet-shutdown/, abgerufen am 26.4.2026.

Bits und Bäume NRW (2026) Für eine selbstbestimmte und gemeinwohlorientierte Digitalisierung in NRW in den planetaren Grenzen. Bits und Bäume. https://bits-und-baeume.org/assets/images/pdfs/260316_B&B_PolitischeForderungen_NRW_barrierefrei_UA.pdf, abgerufen am 26.4.2026.

Digital Austria (2025) Europa unterzeichnet gemeinsame Erklärung zur Europäischen Digitalen Souveränität. https://www.digitalaustria.gv.at/wissenswertes/news/news-77.html, abgerufen am 26.4.2026.

Europäische Kommission (2018) Artificial Intelligence for Europe. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:237:FIN, abgerufen am 26.4.2026.

Förster, Jürgen (2013) Souveränität als Fiktion, in J.S. Wessel, C. Volk, and S. Salzborn (Hrsg.) Ambivalenzen der Ordnung. Wiesbaden: Springer Fachmedien Wiesbaden, pp. 207–231, https://doi.org/10.1007/978-3-531-19829-3_9.

Jeric, Lorenz und Hagen, Lisa Maria (2025) Könnte Palantirs Software ersetzt werden? tagesschau.de, https://www.tagesschau.de/investigativ/ndr/palantir-polizei-daten-software-100.html, abgerufen am 26.04.2026.

Laaksonen, Salla-Maaria und Frig, Meri (2026) Narratives of Indispensability and Infrastructural Solutionism of AI Companies, in A. Mollen et al. (Hrsg.) AI Infrastructures and Sustainability. Palgrave: Basingstoke, pp. 165–188. https://doi.org/10.1007/978-3-032-09748-4_8.

Litvinenko, Anna (2021) Re-Defining Borders Online: Russia's Strategic Narrative on Internet Sovereignty, Media and Communication, 9(4), pp. 5–15, https://doi.org/10.17645/mac.v9i4.4292.

Mollen, Anne (2024a) Infrastrukturen der Automatisierung als Bezugspunkte einer digitalen Selbstbestimmung, UFITA, 88(1), pp. 74–89. https://doi.org/10.5771/2568-9185-2024-1-74.

Mollen, Anne (2024b) Menschenzentrierte KI: Wer zählt als Mensch? #neueRelevanz: Eine Kulturpolitik der Transformation. https://kupoge.de/blog/2024/05/21/menschenzentrierte-ki-wer-zaehlt-als-mensch/ abgerufen am 26.4.2026.

Pohle, Julia und Thiel, Thorsten. (2020) Digital sovereignty, Internet Policy Review, 9(4) https://doi.org/10.14763/2020.4.1532.

Reuter, Markus (2026) So schalten Staaten das Internet aus, netzpolitik.org, https://netzpolitik.org/2026/digitale-unterdrueckung-so-schalten-staaten-das-internet-aus/ abgerufen am 26.4.2026.

Ryng, Julia et al. (2022) Internet Shutdowns: A Human Rights Issue, The RUSI Journal, 167(4–5), pp. 50–63. https://doi.org/10.1080/03071847.2022.2156234.

Sridharan, Hamsini (2026) The Cruel Optimism of the Sustainable Cloud: Fantasies and Futures of Microsoft Azure, in A. Mollen et al. (Hrsg.) AI Infrastructures and Sustainability. Palgrave: Basingstoke, pp. 143–163, https://doi.org/10.1007/978-3-032-09748-4_7.

Anmerkung

1 *https://fragdenstaat.de/dokumente/273689-rechtsgutachten-zur-us-rechtslage-zum-weltweiten-datenzugriff-durch-us-behoerden-bei-nutzung-von-cloud-diensten/*

Anne Mollen

Dr. **Anne Mollen** forscht als Postdoc am Institut für Kommunikationswissenschaft der Universität Münster zu Fragen der sozialen Gerechtigkeit mit Blick auf Automatisierung, Algorithmen und Künstliche Intelligenz. Einer ihrer Forschungspunkte liegt auf der Nachhaltigkeit von KI. Als Expertin für KI und Digitalisierung hat Anne Mollen in der Vergangenheit verschiedene politische Gremien auf nationaler, europäischer und globaler Ebene beraten.

Friederike Hildebrandt, ***Koordinatorin von Bits & Bäume***

Für eine digitale Souveränität ohne Generative KI

Europa diskutiert über digitale Souveränität. Doch statt auf Lösungsvorschläge zu setzen, die einen Fokus auf demokratische Kontrolle, dezentrale und Open-Source-Technologien legen, verstehen die deutsche und europäische Politik Souveränität aktuell insbesondere als Wirtschaftsförderprogramm für generative KI und andere Cloud-Dienste. Dieser Text ist eine Analyse der Debatte und ein Plädoyer für eine nachhaltige und gemeinwohlorientierte digitale Daseinsvorsorge, als Absicherung gegen den Einfluss großer Tech-Konzerne und für eine digitale Zukunft jenseits von generativer KI. Denn: Wenn das Ziel digitaler Souveränität nicht allein Wirtschaftswachstum und die Konkurrenz im Rennen um generative KI ist, dann liegen plötzlich vielfältige Möglichkeiten für selbstbestimmte digitale Infrastrukturen auf dem Tisch.

Dieser Artikel basiert auf den Debatten des Bits & Bäume Netzwerks[1] *zu einer alternativen digitalen Souveränität und ist inspiriert von der* Cables of Resistance Conference *im April 2026.*[2]

Dass Europa und Deutschland digital unabhängig werden müssen, ist spätestens seit der Inauguration von Donald Trump letztes Jahr politischer Konsens. Das Symbolbild der Tech-Milliardäre, die sprichwörtlich hinter der neuen rechten Trump-Regierung stehen, und die digitalpolitische *America-First*-Agenda waren ein Weckruf für die Politik.

Für die digitalpolitische Zivilgesellschaft war dieser Schreck nichts Neues – bereits seit Jahrzehnten kritisieren Hacker:innen, NGOs und Aktivist:innen die Abhängigkeit der Wirtschaft, Konsument:innen und Verwaltung von den großen Tech-Konzernen. Sie entwickeln seit Jahrzehnten eine breite Palette an Open-Source-Alternativen und bilden Communities, die sich für ein datensicheres, unabhängiges und dezentrales digitales Leben einsetzen. Dabei sind bereits viele Synergien mit Wirtschaftswissenschaftler:innen und Umweltverbänden entstanden, die diese Technologie durch ökologische Ansätze und Forderungen nach tiefgreifender Demokratisierung erweitern. (Ein Ort dafür ist beispielsweise das Bits & Bäume-Netzwerk.)

Mit der gemeinwohlorientierten Zivilgesellschaft zusammen hätte ein Zeitalter für diese demokratischen, dezentralen und Open-Source-basierten digitalen Infrastrukturen anbrechen können, weit weg von Elon Musks Hitlergruß und Trumps neuer Digitalpolitik. Viele Alternativen liegen auf dem Tisch, könnten gefördert, ausgeweitet und verbessert werden. Zusätzlich müsste dringend über eine Aneignung und Vergesellschaftung bestehender Infrastrukturen im digitalen Bereich diskutiert werden – mit dem Ziel, eine digitale Grundversorgung aufzubauen, die unabhängig von großen Tech-Konzernen demokratisch kontrolliert wird und informationssicher funktioniert, und das Ganze ohne Datenhehlerei und Sicherheitslücken in Software-Systemen. Die Dominanz von Cloud-Anbietern (63 % des Cloud-Marktes liegen bei Amazon, Google und Microsoft[3]) und ihre (fast) alternativlose Rolle in der Innovationspolitik tragen ein Übriges dazu bei, dass keine digitale Innovation mehr ohne sie stattfinden kann.

Ein erstes Konzept für eine echte Alternative legte bereits 2024 eine Gruppe von Forscher:innen um Cedric Durand und Cecilia Rikap vor mit dem Vorschlag *Reclaiming digital sovereignty: A roadmap to build a digital stack for people and the planet*[4], der seitdem in der Zivilgesellschaft weiterentwickelt und diskutiert wird.

Doch statt sich an diesen Vorschlägen zu orientieren, begreifen die europäischen Regierungen, allen voran das deutsche Digitalministerium, den Begriff der *Digitalen Souveränität* vor allem als Wirtschaftsförderung für deutsche und europäische Unternehmen und insbesondere als ein Argument, im sogenannten *AI-Race* mithalten zu wollen.

Diese Idee von Digitaler Souveränität basiert auf dem sogenannten *Euro-Stack*, der unter anderem von den Denker:innen Francesca Bria und Christina Cafarra vorgeschlagen wurde.[5] Grundidee ist es, die entscheidenden Bausteine der digitalen Infrastrukturen durch europäische Player legen zu lassen, wohlgemerkt ohne den Anspruch, dass diese unter fundamental anderen – ökologischeren oder demokratischeren – Prämissen funktionieren. Es ist ausreichend, dass diese digitalen Infrastrukturen europäischer Regulierung unterliegen und nicht der US-amerikanischen. Ziel ist also keine grundlegend andere digitale Infrastruktur, sondern europäische Äquivalente zu Facebook, Amazon Web Services und Palantir.

Das Digitalministerium bezieht sich zwar ebenfalls auf einen Deutschland-Stack, ist jedoch weniger streng bezüglich der Unabhängigkeit von amerikanischen Konzernen: Es begründet Digitale Souveränität zwar mit Unabhängigkeit, aber fokussiert sich in seinen Vorhaben besonders auf staatliche Investitionen und Aufträge in Wirtschaftsunternehmen, den Aufbau einer *Gigafactory made in Germany*, Rückbau von Umweltvorschriften für Rechenzentren und Staatsmodernisierung, besonders mit Hilfe von KI. Open-Source-Alternativen kommen nur am Rande vor, Nachhaltigkeit und demokratische Kontrolle werden nicht erwähnt.[6] Carsten Wildberger sprach im Bundestag zuletzt stolz von Rechenzentren als „Fabriken des 21. Jahrhunderts" mit denen Deutschland „gestaltet"[7] und bezog sich dann auf Rechenzentrumsprojekte wie das 11 Mrd.-Euro-Projekt der Schwarz-Gruppe in Lübbenau – auf dem aktuell vor allen Dingen amerikanische KI-Modelle wie Gemini oder ChatGPT laufen können[8] – und zwei Microsoft-Rechenzentren, die aktuell im Rheinischen Revier gebaut werden.[9] Diese Projekte haben zwar mit Unabhängigkeit von amerikanischen Tech-Unternehmen wenig zu tun, aber werden als Fortschritt im Wettbewerb um generative KI gewertet.

Das KI-Problem der Digitalen Souveränität

Ein entscheidender Widerspruch in der Debatte um Digitale Souveränität ist also der politische Fokus auf generative KI. Er illustriert klar, dass die politische Priorität auf Wirtschaftswachstum statt auf nachhaltigen, dezentralen und gemeinwohlorientierten Infrastrukturen liegt.

Mit der Einführung von ChatGPT 2022 hat global ein Hype um generative KI-Modelle begonnen. In der Debatte vermischen sich dabei häufig kleine, spezifische Modelle, die schon lange in Wissenschaft und Industrie im Einsatz sind, mit den neueren *general-purpose*-Sprachmodellen, die von den großen Tech-Konzernen eingeführt wurden. In der Debatte zerfließen häufig die sehr sinnvollen Anwendungen von KI – die auch weniger Ressourcen brauchen – mit den großen KI-Modellen. Das mündet in einem vagen wirtschaftspolitischen Versprechen, dass KI ein sehr mächtiges Instrument sei und die nächste Wirtschaftsrevolution herbeiführen werde. Dorothee Bär kündigte letztes Jahr bis zu 10 % Wirtschaftswachstum durch KI an[10], während über ein Drittel des US-amerikanischen BIP-Wachstums aktuell (spekulative) Investitionen in die generativen KI-Unternehmen sind.[11]

Die Logik dabei ist: KI wird zu Wirtschaftswachstum führen => dazu braucht es große Rechenkapazitäten => deswegen müssen Rechenzentren mit Hochleistungschips gebaut werden => die wiederum schnellstmöglichst sehr viel Energie benötigen.

Für die europäischen Regierungschefs ist dabei klar, dass es möglichst viele dieser KI-Rechenzentren in Europa geben soll, selbst wenn sie gar nicht von europäischen Unternehmen betrieben werden. Wie das neue Amazon-Rechenzentrum in Potsdam zeigt.[12]

Die Hoffnung auf das Wirtschaftswachstum ist groß, dabei werden immer mehr Stimmen laut, dass die KI-Modelle sie nicht erfüllen können: Viele Investitionen sind sogenannte *Circular Deals*[13], bei denen Unternehmen gegenseitig ineinander investieren. Immer mehr Wirtschaftsexpert:innen warnen vor einer KI-Blase, die am Ende Staaten und kleine Investoren ausbaden werden, und Studien vom MIT haben bereits ergeben, dass 95 % der Investitionen in KI bisher nicht profitabel sind.[14] Auch die Entwicklungsschritte der Modelle entsprechen nicht den immensen Investitionssummen. Die Modelle werden kaum besser, während Milliarden in ihre Mutterkonzerne investiert werden.

Bohrt man tiefer, wird zudem schnell klar: Das anvisierte Wirtschaftswachstum basiert vor allem auf Automatisierung, also darauf, viele Jobs in Industrie und Tech-Unternehmen überflüssig zu machen. Der Preis für potenzielle Gewinne wären also massive gesamtgesellschaftliche Arbeitsplatzverluste.

Und dabei haben die generativen KI-Modelle wenig zu tun mit digitalen Infrastrukturen, die Nutzer:innen, Verwaltung und Unternehmen von den großen amerikanischen Tech-Konzernen abgrenzen. Die großen Sprachmodelle, wie ChatGPT, sind nicht einfach eine zufällig-brillante Innovation. Sie sind das Ergebnis einer Konzentration an wirtschaftlicher Macht, wie sie nur bei den großen Tech-Konzernen vorliegt. Das Training und der Betrieb der Modelle benötigen: (1) große Datenmengen, (2) sehr viel Rechenkapazität, (3) hundertausende Stunden Arbeit zum Codieren und (4) sehr viel Energie zum Betrieb der Rechenzentren. All das steht nur den größten Tech-Konzernen zur Verfügung und kann auch nur mit systematischer Ausbeutung von Natur und Arbeit geschehen.

Die KI-Rechenzentren sind so energieaufwändig, dass für sie neue Gaskraftwerke gebaut werden und Microsoft sogar das nach einem radioaktiven Zwischenfall abgeschaltete Atomkraftwerk Three Mile Island wieder in Betrieb genommen hat. OpenAI, die Mutterfirma von ChatGPT, kündigte letztes Jahr an, 2030 den Energieverbrauch von Indien zu haben, und die Internationale Energieagentur prognostiziert, dass Rechenzentren bis 2030 bis zu 30 % des globalen Energieverbrauches ausmachen könnten. Zahlen, die mit einer klimagerechten Zukunft nicht vereinbar sind.[15]

Auch die Arbeit, die in die generativen KI-Modelle fließt, ist nur dank ausbeuterischer Lieferketten im globalen Süden möglich und die Daten, die die Modelle speisen, sind zu einem großen Teil ohne oder mit ungeklärten Nutzungsrechten in die Modelle geflossen; neue Daten werden zunehmend aus Nutzer:innendaten von beispielsweise Instagram oder LinkedIn gewonnen.

Die Struktur der generativen KI-Modelle ist folglich weder gemeinwohlorientiert noch nachhaltig und auch nicht problemlos ohne Ausbeutung von Arbeit und enormen Energieverbrauch replizierbar. Deswegen stehen auch Hyperscale-Rechenzentrumsprojekte für die Digitale Souveränität in starkem Kontrast zu regionalen Interessen: Sie werden mit Möglichkeiten regionaler Entwicklung beworben, schaffen aber im Gegensatz zu anderen Industrieanlagen kaum Arbeitsplätze und greifen dafür massiv auf Stromnetze und Wasserversorgung zu. Häufig zahlen sie zudem eine reduzierte Gewerbesteuer – Gewinn fließt also insbesondere aus der Region hinaus, statt in sie hinein.

In den USA lehnen erste Regionen Rechenzentren komplett ab und auch in Deutschland wird die Kritik an den Projekten größer.

Hoffnung macht jedoch: Betrachtet man die Rechenkapazitäten in Deutschland, die nicht auf KI ausgelegt sind, dann sind weder neue Rechenzentren noch zusätzliche Energie erforderlich – die meisten Rechenzentren waren vor dem Hype um generative KI nur zu 30 – 50 % ausgelastet[16].

Friederike Hildebrandt

Friederike Hildebrandt ist Ökonomin und Aktivistin, sie koordiniert das *Bits & Bäume*-Bündnis.

Für die Anwendungen, über die diskutiert wird, wenn es um eine sinnvolle digitale Grundversorgung geht, bestehen die notwendigen Infrastrukturen längst. Selbst für größere KI-Modelle beispielsweise im medizinischen Bereich, für die Hochleistungscomputer notwendig sind, reicht häufig ein Rechner in einem Uniklinikum und es ist keine KI-Gigafactory nötig.

Silver Lining hinter der Cloud?

Diese Analyse scheint vielleicht pessimistisch, aber sie eröffnet auch neue Möglichkeiten:

Wenn das Ziel digitaler Souveränität nicht allein Wirtschaftswachstum und die Konkurrenz im Kampf um generative KI ist, dann liegen plötzlich vielfältige Möglichkeiten und Vorschläge auf dem Tisch, wie digitale Infrastrukturen unabhängig von großen Tech-Konzernen gestaltet werden können. Führt man sie zusammen, entsteht ein hoffnungsvolles Mosaik für eine nachhaltige, gemeinwohlorientierte digitale Zukunft, von dem hier drei Ansätze skizziert sind:

Freie und Open Source Software

Die FOSS-Community legt bereits seit Jahren Alternativen zu großen Tech-Konzernen vor. Von alternativen Sozialen Medien und Cloud-Lösungen zur jahrzehntelangen Grundlagenarbeit für das gesamte Back-End des Internets. Der dezentrale Open-Source-Gedanke kann ein wichtiger Baustein für demokratische Kontrolle über Technologie sein und ermöglicht, sie weltweit zu nutzen und weiterzuentwickeln – unabhängig von großen Konzernen. Eine ernsthaftes Commitment würde Investitionen in FOSS bedeuten, um die Technologien nutzer:innenfreundlich, verlässlich und nachhaltig zu gestalten.

Community Data Center

Ein aktuelles Forschungsprojekt am Weizenbaum-Institut[17] greift die Idee von digitalen Infrastrukturen für und von Communities auf – Community Data Center folgen einer ähnlichen Idee wie Bürger:innen-Energie. Rechenzentren werden von Communities für Communities demokratisch betrieben. Eigentumsformen können Genossenschaften, Anstalten öffentlichen Rechts oder öffentliche Träger sein. Sie können Nutzer:innen, Forschung, Unternehmen und Verwaltung mit Rechenkapazitäten versorgen und sind eng rückgebunden an die Orte, an denen sie stehen.

Vergesellschaftung & Suffizienz

Der Gedanke scheint radikal: Aber die benötigte digitale Infrastruktur für eine digitale Daseinsvorsorge besteht bereits. In Deutschland und global existieren genug Rechenzentren, Netzinfrastruktur und Hardware für eine breite digitale Versorgung. Eine alternative Infrastruktur neben der bestehenden Infrastruktur aufzubauen, wäre ökologisch und wirtschaftlich kaum möglich, da dies massive Ressourcenmengen benötigen und auf Land und Energienetze zugreifen würde. Die Grundfrage ist jedoch: Wie sähe demokratische Kontrolle aus, die dringend notwendig ist? In ihrer radikalsten Form müsste es eine Aneignung der Infrastrukturen geben, was insbesondere im Globalen Süden eine Emanzipation von großen Tech-Konzernen bedeuten würde. Diese Strukturen müssten dann in gemeinwohlorientierte und demokratische Kontrolle gebracht werden – wie öffentliche Straßen- oder Schienennetze. Konzepte für solche Prozesse werden bereits für den Energiesektor[18] vorgedacht und beispielsweise auch in Berlin in Bezug auf Wohnkonzerne diskutiert.[19] In Deutschland existiert für diesen Zweck sogar Artikel 15 im Grundgesetz, in dem es heißt: „Grund und Boden, Naturschätze und Produktionsmittel können zum Zwecke der Vergesellschaftung durch (…), in Gemeineigentum (…) überführt werden".[20]

Plädoyer für eine digitale Gerechtigkeit von unten

All diese Vorschläge sind nicht nur ökologisch und gemeinwohlorientiert – sie sind auch global skalierbar. Open-Source-Technologie lässt sich auch in Ländern des globalen Südens einsetzen und etablieren, Community Center schaffen lokale Gerechtigkeit und reduzieren koloniale Abhängigkeiten und die Demokratisierung bestehender Infrastrukturen holt die Entscheidungsmacht zurück an die Orte, an denen Menschen die Strukturen nutzen. Das steht im starken Kontrast zu einem *Europa-First*-Gedanken, der auf europäische Digitalkonzerne setzt und intern für Souveränität sorgt, aber global dieselben Abhängigkeiten produzieren könnte.

Die schlechte Nachricht ist: Wenn Digitale Souveränität wie bisher vor allem als Wirtschaftsförderung verstanden wird, ist sie weder gemeinwohlorientiert noch nachhaltig. Die gute Nachricht: Die Lösungen liegen ungenutzt, aber einsatzbereit vor, sie werden von einer starken, kreativen Community getragen und haben das Potenzial, global für digitale Gerechtigkeit zu sorgen.

Anmerkungen

1 *https://bits-und-baeume.org/*
2 *https://cableresist.de/*
3 *https://www.srgresearch.com/articles/cloud-market-share-trends-big-three-together-hold-63-while-oracle-and-the-neoclouds-inch-higher*
4 *https://discovery.ucl.ac.uk/id/eprint/10202865/1/reclaiming-digital-sovereignty.pdf*
5 *https://www.euro-stack.info/*
6 *https://bmds.bund.de/ministerium/bilanz*
7 *https://www.bundestag.de/dokumente/textarchiv/2026/kw16-de-rechenzentrumsstrategie-1158228*
8 *https://www.deutschlandfunk.de/ki-rechenzentren-ressourcen-chatbot-energieverbrauch-100.html*
9 *https://www.rheinisches-revier.de/service/neuigkeiten/detail/spatenstich-fuer-microsoft-rechenzentrums-cluster-im-rheinischen-revier*
10 *https://netzpolitik.org/2025/kuenstliche-intelligenz-die-hype-tech-agenda-der-bundesregierung/*
11 *Servaas Storm (2025) The U.S. Is Betting the Economy on 'Scaling' AI: Where Is the Intelligence When One Needs It? International Journal of Political Economy, 54:4, 425-452. DOI: 10.1080/08911916.2026.2616133*

12 *https://www.maz-online.de/brandenburg/cloud-daten-sicher-vor-usa-amazon-startet-in-potsdam-aws-european-sovereign-cloud-3KS7ACVY5NA6NLITULTQN6PZA4.html*
13 *Servaas Storm (2025) The U.S. Is Betting the Economy on 'Scaling' AI: Where Is the Intelligence When One Needs It? International Journal of Political Economy, 54:4, 425-452. DOI: 10.1080/08911916.2026.2616133*
14 *https://www.artificialintelligence-news.com/wp-content/uploads/2025/08/ai_report_2025.pdf*
15 *https://www.iea.org/reports/energy-and-ai/energy-demand-from-ai*
16 *https://www.dena.de/infocenter/nachhaltige-rechenzentren*
17 *https://www.weizenbaum-institut.de/forschung/forschungsprojekte/community-data-centers/*
18 *https://communia.de/konzeptpapier-gemeingut-energie/*
19 *https://dwenteignen.de/*
20 *https://www.gesetze-im-internet.de/gg/art_15.html*

https://bits-und-baeume.org/posts/B&B_NRW_PolitischeForderungen_2026_html/

Werner Winzerling, ***Hochschule Fulda, Angewandte Informatik***

Big Tech und die Probleme mit der digitalen Souveränität

Ökonomische Netzwerkeffekte (economies of networks) haben zur Dominanz von Produkten und Diensten der Big Tech in der IT-Welt geführt. Der Beitrag zeigt politische und technische Schwierigkeiten auf, die daraus für die angestrebte Digitale Souveränität in Deutschland und der EU resultieren. Hierfür wird ein klassischer *politökonomischer Ansatz gewählt, aus dem zwei alternative Handlungsvorschläge abgeleitet werden.*

Direkte und indirekte Netzwerkeffekte in der Computerindustrie

Wenn von *Digitaler Souveränität* gesprochen wird[1], ist derzeit vor allem die Verringerung der Abhängigkeit von führenden US-amerikanischen IT-Unternehmen, den *Big Tech*[2] das Ziel. Ihre weltweit dominante Stellung verdanken diese Unternehmen sogenannten Netzwerkeffekten, die im Folgenden kurz beschrieben werden.[3]

Mit *Externalitäten* werden in der ökonomischen Theorie sekundäre Auswirkungen beschrieben, die eine Markthandlung zusätzlich zu der primär beabsichtigten hervorruft und die nicht über den Preis abgegolten wurden. Bezogen auf technische wie auch soziale Netzwerke beschreibt dies die Auswirkungen, die ein weiterer Teilnehmer für den Wert eines Netzwerks und damit für die schon vorhandenen Teilnehmer hat.

Ein *direkter Netzwerkeffekt* entsteht, wenn der Wert eines Netzwerks mit der Zahl seiner Nutzer steigt. Dieser Zusammenhang ist meist nicht linear, sondern progressiv. Das klassische Beispiel ist hier das Telefonnetz. Je mehr Teilnehmer ein solches Netz hat, umso interessanter ist es für potenzielle neue Teilnehmer. In diesem Fall tritt die zugrunde liegende Technologie (generischer Produktnutzen) hinter der Größe des Netzwerks (derivater Nutzen) zurück. Dies können auch die Teilnehmer in einem sozialen Netzwerk sein oder die auf einem Marktplatz vertretenen Anbieter oder erreichbaren Kunden.

Dagegen treten *indirekte Netzwerkeffekte* hauptsächlich bei Systemprodukten auf. Ein solches Produkt ist für den Nutzer umso wertvoller, je mehr ergänzende Komplementärleistungen dafür erhältlich sind. Dies kann beispielsweise eine bestimmte Computer-Architektur sein, für die eine große Auswahl preiswerter Ergänzungsbaugruppen sowie viele Softwareprodukte erhältlich sind. Gleichzeitig kann von Bedeutung sein, dass Fachzeitschriften umfangreich über diese Architektur informieren und bei Problemen viele Personen um Rat gefragt werden können.

Sowohl direkte wie auch indirekte Netzwerkeffekte steigern den Wert eines Netzwerks. Dadurch wird es für neue Teilnehmer (direkter Nutzen) aber auch für weitere Anbieter von Komplementärleistungen (indirekter Nutzen) interessant, so dass es zu Lasten konkurrierender Netzwerke eine dominante Stellung im Markt erlangen kann. Dieser Effekt wird als *positives Feedback* (Increasing Returns) bezeichnet und bildet auch die Grundlage für das Entstehen von *digitalen Monopolen*.

Digitale Monopole

Insbesondere indirekte Netzwerkeffekte begünstigen so genannte *Lock-In-Situationen*. Diese entstehen, wenn sich der Wechsel zu einem alternativen Netzwerk (beispielsweise eine andere IT-Architektur) für die Teilnehmer nicht lohnt, da der Aufwand für den Wechsel höher ist als der Nutzen, den das alternative Netzwerk bietet. Der Aufwand besteht hier nicht nur in den Anschaffungskosten, sondern auch darin, dass das Wissen über die alten Produkte wertlos wird und die Nutzung des alternativen Netzwerkes neu *erlernt* werden muss. Eine solche Lock-In-Situation festigt zusätzlich ein schon bestehendes Monopol.

Die Auflösung einer Lock-In-Situation erfordert im Allgemeinen die Existenz eines alternativen Angebotes, dessen Nutzen größer ist. In der Praxis ergab sich dies meist erst mit einer neuen technologischen Generation, wie zum Beispiel bei der Ablösung der Schallplatte durch die CD (besserer Klang, Haltbarkeit, Abmaße, Kopierkosten u. ä.).[4]

Zusätzlich half im Fall der Big Tech auch noch eine besondere Börsensituation in den 1990er Jahren.[5] Internationale Investoren verfügten über bedeutende Finanzmittel, und die IT-Branche galt als besonders interessantes Anlageobjekt. So verfügten IT-Unternehmen, die als aussichtsreich galten, über nahezu unbegrenzte finanzielle Mittel, um lange Anlaufphasen zu überbrücken (Amazon, Google), oder um ähnliche Unternehmen und damit deren Kunden aufzukaufen (Facebook).[6]

Skaleneffekte in der Digitalisierung

Neben den Netzwerkeffekten profitieren die Big Tech auch von den Skaleneffekten digitaler Güter. Hier entstehen häufig nur fixe Entwicklungskosten. Die variablen Grenzkosten sind dagegen oft zu vernachlässigen, wie in der Software-Entwicklung. Hier müssen nur die fixen Entwicklungskosten auf die Kunden umgelegt werden. Je größer dann die Kundenbasis ist, umso preiswerter können die digitalen Güter je Kunde angeboten werden.

Zur schnellen Gewinnung einer möglichst großen Kundenbasis werden die Produkte häufig zunächst kostenlos oder zumindest stark subventioniert angeboten. Ist die Kundenbasis dann groß genug, entsteht eine Monopolsituation, die von Wettbewerbern im Allgemeinen nicht mehr aufgeholt werden kann.

Digitale Abhängigkeiten

Die oben beschriebenen Mechanismen haben letztlich dazu geführt, dass sich in verschiedenen IT-Anwendungsfeldern digitale Monopole bilden konnten. Besondere Rahmenbedingungen in den USA haben es begünstigt, dass sich die Big-Tech-Unternehmen dort als erste herausbilden konnten und in der Folge eine weltweite Dominanz erreicht haben (*First-Mover*-Vorteil).

Inzwischen fürchten selbst Staaten wie Deutschland und die EU (obwohl politisch eng mit den USA verbunden), dass diese Abhängigkeit durch Regierungen der USA machtpolitisch ausgenutzt werden könnten. Auch um sich davor zu schützen, streben Deutschland und die EU nach einer größeren digitalen Souveränität und verfolgen dabei Ansätze, die von der Regulierung der Big Tech bis zur Förderung alternativer Angebote reichen.

Neben der Vermeidung einer technologischen und digitalen Erpressbarkeit zielt die digitale Souveränität auch auf den Erhalt und die Weiterentwicklung der eigenen technischen Kompetenz. Das Ziel dieses Beitrags ist jedoch, die begrenzenden Bedingungen aufzuzeigen, die einer digitalen Souveränität (vorrangig bezogen auf die Big Tech und deren Einsatz in Cloud-Rechenzentren) entgegenstehen könnten. Weitere Souveränitätsziele, beispielsweise im Hardwarebereich, die dann u. a. auch chinesische Hersteller betreffen, werden hier nicht betrachtet.

Demokratische vs. staatliche Kontrolle

Werner Ruf hat (in einem anderen Zusammenhang) kürzlich auf ein derzeit häufig zu beobachtendes Phänomen in der gesellschaftspolitischen Diskussion hingewiesen:

> *„Der wohl ideologisch bedingte Verzicht auf die wahrscheinlich fruchtbareren Ansätze der politischen Ökonomie bedingt oft die Aporie wohlgemeinter Studien.“*[7,8]

Forderungen verschiedener zivilgesellschaftlicher Gruppen nach einer weitgehenden *(demokratischen) Regulierung* der Big Tech, bis hin zur Forderung nach deren Zerschlagung[9,10], kann als eine derartige Aporie (Ratlosigkeit) angesehen werden – denn (nur) unter *wahrhaft* demokratischen Produktionsverhältnissen hätte die Gesellschaft solche weitreichenden Einflussmöglichkeiten. Der Überbau der Gesellschaft leitet sich aus den herrschenden Produktionsverhältnissen ab, und die sind hier (zumindest derzeit noch) kapitalistisch – d. h. auf die Erzielung eines (maximalen) Profits gerichtet.[11]

Was unter diesen Bedingungen mit einer Regulierung tatsächlich erreicht werden kann, ist nur eine solche *Regulierung*, die nicht im Widerspruch zu den vorherrschenden kapitalistischen Produktionsverhältnissen steht. Die Eigentumsgarantie des Grundgesetzes (Artikel 14 GG) sowie die europäischen Verträge setzen staatlichen Regulierungen hier sehr enge Grenzen.

Ein Eingriff in das Eigentum eines Unternehmens ergibt sich bei den Big Tech bereits dann, wenn beispielsweise entscheidende Netzwerkeffekte beeinträchtigt werden, aus denen der Wert des Unternehmens erwächst. So könnte eine erzwungene Reduzierung der Teilnehmer des Netzwerkes den Wert des Unternehmens substanziell reduzieren – oder sogar vollständig vernichten.[12]

Das beginnt in der Praxis bereits bei IT-Unternehmen, die ihren Gewinn aus dem Verkauf von Werbung erzielen.[13] Wie weit das *berechtigte Interesse* nach Artikel 6 DSGVO an der Gewinnung und Verarbeitung personenbezogener Daten der Teilnehmer reicht, die hier für eine individualisierte Werbeansprache benötigt werden, ist, wenig überraschend, Gegenstand langwieriger juristischer Auseinandersetzungen in der EU.[14,15]

Souveräne EU-Cloud

Mit dem Ziel der digitalen Souveränität werden derzeit in Deutschland vermehrt Cloud-Rechenzentren eingeweiht.[16,17,18] Dass diese Rechenzentren durchweg Software-Produkte der Big Tech nutzen und teilweise sogar von Big Tech selbst betrieben werden[19], wird auch als *Souveränitäts-Washing* kritisiert.[20]

Dieser pragmatische Ansatz, die digitale Souveränität nur in Teilen umzusetzen, dürfte auch aus dem praktischen Scheitern des 2019 gestarteten EU-Projektes *Gaia-X* resultieren. Dessen hoch gesteckte Ziele waren politisch wie technisch so nicht umsetzbar.[21] So musste trotz der Förderung Nextcloud seine Mitwirkung in Gaia-X aufgrund fehlender eigener Kapazitäten praktisch wieder beenden.

Derartige Probleme scheinen sich auch mit dem *Deutschland-Stack* fortzusetzen, der eine nationale souveräne Technologie-Plattform für die Digitalvorhaben in Deutschland definieren soll.[22] Auch noch Anfang 2026 schreibt Heise-Online: *„Die langen Listen offener Festlegungsbedarfe in praktisch jeder Schicht zeigen, dass der Stack in weiten Teilen eher einen Rahmen absteckt als eine fertige Architektur liefert"*[23] – die dann in absehbarer Zeit auch einsatzbereit wäre.

So verwundert es nicht, wenn mit den *souveränen* Cloud-Rechenzentren derzeit nur zwei wesentliche Ziele verfolgt werden:

- Die Daten der Kunden werden im Cloud-Rechenzentrum verschlüsselt abgelegt. Die Schlüsselverwaltung erfolgt dabei ausschließlich durch den Kunden, so dass Dritte (zum Beispiel die Sicherheitsorgane der USA) diese Daten nicht lesen können.

- Die konkrete Lizenzverwaltung verhindert, dass die genutzte Software durch den Entwickler einfach *abgeschaltet* werden kann. Im Konfliktfall kann die kritische Software (freilich dann nur in der aktuellen Version) weiter genutzt werden bis diese gegebenenfalls auf eine Alternative umgestellt wurde.

Warum beispielsweise die Schwarz-Gruppe (Lidl, Kaufland) in ihrem Cloud-Rechenzentrum als Bürosoftware kein Open-Source-Produkt nutzt[24], beantwortet ein Geschäftsführer der dortigen IT-Sparte wie folgt: *„Für Open-Source-Anwendungen konnten wir keine Referenzkunden in vergleichbarer Größe finden. Es konnte auch nicht unser Ansatz sein, einfach etwas auszuprobieren. Wir mussten auf etwas setzen, das große Unternehmen seit einigen Jahren nutzen."*[25]

Um diese Situation zu verbessern, wird (auch vom FIfF) gefordert, dass die öffentliche Hand ihre IT-Ausgaben gezielt in alternative Open-Source-Produkte und entsprechende Dienstleistungen investiert.[26] Neben vielen anderen hierbei noch ungelösten Problemen, bleibt auch die Frage, ob dieses Investitionsvolumen allein ausreichen würde, um hier kurz- bis mittelfristig Änderungen zu erreichen, insbesondere wenn die Privatwirtschaft durchweg anders entscheidet.

Grenzen der staatlichen Regulierung und eine mögliche Alternative

Mit dem derzeit umstrittenen Omnibus-Verfahren der EU, mit dem eine Reihe von Datenschutz- und KI-Regulierungen wieder zurückgenommen bzw. *aufgeweicht* werden[27], zeigt sich ein weiteres Problem. Vorgaben, die die Gesellschaft zumindest teilweise vor den negativen Wirkungen der kapitalistischen Produktionsweise schützen soll, haben inzwischen einen solchen Umfang (vulgo Bürokratie) erreicht, dass er inzwischen bis in Teile der Zivilgesellschaft hinein als nicht mehr handhabbar angesehen wird.[28]

Eine Alternative wäre, die Wirtschaft so zu organisieren, dass diese inhärent (also auch ohne Regulierung) negative gesellschaftliche Entwicklungen vermeidet.

Totalüberwachte Einsamkeit, generiert mit ChatGPT

Google schrieb 2004 in seinem Börsenprospekt: *„Don't be evil."*[29] Da seine Suchmaschine durch den Verkauf von Werbung finanziert wird, sicherte Google damit den Nutzern lediglich zu, die Suchergebnisse nicht zugunsten der Reichweite von Werbung zu *manipulieren*. In der Öffentlichkeit (und auch von Mitarbeitern des Unternehmens selbst) wurde dieses Versprechen oft sehr viel weitgehender interpretiert – als eine Selbstverpflichtung sich den gröbsten Zumutungen der herrschenden Produktionsweise zu verweigern.[30]

Solchen Selbstverpflichtungen sind unter kapitalistischen Produktionsverhältnissen naturgemäß sehr enge Grenzen gesetzt. Andererseits könnten Selbstverpflichtungen von Unternehmen aber auch ein *Einfallstor* sein, mit dem (nach Karl Marx) eine neue Produktionsweise bereits innerhalb des alten Systems entsteht, noch bevor das alte System ganz verschwunden ist!

Kooperation statt Abschottung

Letztlich stellt sich auch die Frage, ob das Streben nach einer (vollständigen) digitalen Souveränität überhaupt der richtige Ansatz ist – auch wenn die weltpolitischen Ereignisse dies derzeit aufdrängen.

So wird die aktuell häufig genutzte Metapher des *KI-Wettrüstens* kritisch hinterfragt.[31] Anstatt die KI-Entwicklung als ein Wettrüsten zu werten (das dann auch große Eskalationsrisiken birgt), wird vorgeschlagen dies besser als einen *geopolitischen Innovationswettlauf* zu verstehen, der sowohl Wettbewerb wie auch Kooperation einschließt. So könne *„die Stärkung kooperativer Rahmenordnungen durch internationale Standards und Regulierung Rivalitäten abmildern und verantwortungsvolle Innovationen fördern."*[32]

Dieser Ansatz kann auch auf die *digitale Souveränität* übertragen werden. Eingedenk der oben beschriebenen Netzwerkeffekte scheint es wenig sinnvoll, riesige Investitionen und hochqualifizierte Arbeitskräfte (!) für (eigentlich unnötige) nachträgliche Parallelentwicklungen zu verschwenden. Diese knappen Kapazitäten sollten genutzt werden, für die wesentlich drängenderen Aufgaben, vor denen die Menschheit derzeit steht!

Anmerkungen

1 *EU-Summit: Das war der Gipfel zur europäischen Digitalen Souveränität. BMDS. 2025, https://bmds.bund.de/aktuelles/aktuelle-meldungen/detail/eu-summit-das-war-der-gipfel-zur-europaeischen-digitalen-souveraenitaet*

2 *Unter dem Begriff Big Tech werden meist die 5 größten IT-Unternehmen aus den USA zusammengefasst: Microsoft, Alphabet/Google, Meta/Facebook, Amazon, Apple. Mit dem Aufkommen der KI wird neuerdings noch NVIDIA dazugezählt.*

3 *Unter Verwendung von: Zerdick, Axel; Picot, Arnold; Schrape, Klaus u. a. (2001): Die Internet-Ökonomie – Strategien für die digitale Wirtschaft. Berlin, Heidelberg, New York: Springer 2001 (European Communication Council Report)*

4 *Inzwischen wurde die CD wiederum durch Streamingdienste wie Spotify abgelöst.*

5 *Philipp Staab: Digitaler Kapitalismus. Suhrkamp 2022 (Abschnitt: 3. Finanzkapitalismus online)*

6 *Allerdings führte die dabei entstandene Spekulationsblase (Dotcom-Blase) Anfang 2000 auch zu einem der größten Börsencrashs in der Geschichte.*

7 *Ruf, Werner: Die Friedensforschung und der Markt. In Quo vadis, Friedensforschung, W&F Dossier 96, 2023, S. 3 – 6*

8 *Ähnlich äußerte sich auch Frieder Nake in seinem Grußwort zum 40. FIfF-Geburtstag auf der #FIfFKon2024 in Bremerhaven. https://www.fiff.de/beitraege/2024/einladung-zur-fiffkon24/*

9 *Beispielsweise Petition an: EU-Wettbewerbskommissarin Teresa Ribera. Google Zerschlagen. FIfF-Kommunikation 4/25, S. 46*

10 *Rebalance now – Beyond Big Tech – Ein Manifest für eine neue digitale Wirtschaft. https://rebalance-now.de/beyond-big-tech-ein-manifest-fuer-eine-neue-digitale-wirtschaft/*

11 *Da dies (zumindest für FIfF-Kon-Leser) zum Allgemeinwissen gehört, wird hier auf Quellenangaben verzichtet. ;-)*

12 *Wenn sich CEOs der Big Tech vehement gegen profitreduzierende Regulierungen wehren, sollte dabei nicht außer Acht gelassen werden, dass in deren Aufsichtsräten (zunehmend) Investoren sitzen, die aus diesen Profiten zugesagte Altersrenten für Arbeitnehmer finanzieren (müssen). Man kann dies durchaus als Perversion kapitalistischer Produktionsverhältnisse ansehen.*

13 *Für viele häufig genutzte Internet-Anwendungen ist der Verkauf von Werbung wohl das profitabelste Geschäftsmodell. Zur Wahrheit gehört aber auch, dass sehr oft gar keine alternative Finanzierungsform gefunden wurde (zumindest unter der derzeit herrschenden kapitalistischen Produktionsweise).*

14 *Bleich, Holger: Zweckgebundener Widerstand. c't 2025, Heft 23, S. 72-73*

15 *Lediglich für Daten zur Religion, Gesundheit, Sexualität und politischen Einstellung setzt die DSGVO im Artikel 9 engere Grenzen.*

16 *Weiss, Harald: AWS-Cloud: Marketing statt Souveränität. vdi-nachrichten, 2026-01-23, S. 12. https://www.vdi-nachrichten.com/technik/informationstechnik/aws-cloud-marketing-statt-souveraenitaet/*

17 *Windeck, Christof: KI von Lidl – KI-Rechenzentren boomen in Deutschland. c't 2025, Heft 26, S. 12 – 14*

18 *Born Achim: SAP: 20 Milliarden Euro für die Souveränität. Heise-Online, 2025-9-5, https://www.heise.de/news/SAP-20-Milliarden-Euro-fuer-die-Souveraenitaet-10634104.html*

19 *Insbesondere, wenn eine Kontinent-übergreifende Verfügbarkeit angestrebt wird, dominieren Big Tech betriebene Cloud-RZ.*

20 *Wehnes, Harald ; Kunkel, Julian ; Weigele, Martin: Schein-Lösungen stoppen: Souveränitäts-Washing von Big Tech gefährdet Sondervermögen. GI-Blog, 2025-4-8, https://gi.de/themen/beitrag/kritik-zu-souveraenitaets-washing-von-big-tech*

21 *Wölbert, Christian: Projekt für „souveräne" Dateninfrastruktur: Was aus Gaia-X wurde. c't-Magazin, 2023-11-17, https://www.heise.de/hintergrund/Projekt-zur-Dateninfrastruktur-Was-aus-dem-Cloudprojekt-Gaia-X-wurde-9528946.html*

22 *https://deutschland-stack.gov.de/*

23 *Förster Moritz: Deutschland-Stack: Mit über 50 offenen Standards zur souveränen Verwaltung. Heise-Online, 2026-3-26 https://www.heise.de/hintergrund/Deutschland-Stack-Mit-ueber-50-offenen-Standards-zur-souveraenen-Verwaltung-11225614.html*

24 *Die Schwarz-Gruppe hat ihre Bürosoftware aus Kostengründen von der Microsoft-Suite auf Google Workspace umgestellt.*

25 *Wölbert, Christian: Warum die Schwarz-Gruppe Microsoft Office ablöst – Interview mit Michael Brenzel. c't 2026, Heft 6, S. 40 – 41. https://www.heise.de/hintergrund/Digitale-Souveraenitaet-Stackit-Geschaeftsfuehrer-Michael-Brenzel-im-Interview-11146991.html*

26 *Offener Brief an Claudia Plattner (BSI): Digitale Souveränität für Deutschland und Europa ist möglich. 2025-8-26, https://www.fiff.de/pressemitteilungen/2025/offener-brief-an-claudia-plattner-bsi-digitale-souveraenitaet-fuer-deutschland-und-europa-ist-moeglich/*

27 *EU muss hart erkämpften Schutz digitaler Menschenrechte bewahren. https://www.fiff.de/pressemitteilungen/2025/eu-muss-hart-erkaempften-schutz-digitaler-menschenrechte-bewahren/*

28 *Siehe hierzu auch: Eine Bürokratie 5.0 darf es nicht geben. MITTELDEUTSCHE MITTEILUNGEN, forum der technisch-wissenschaftlichen Vereine und Verbände Sachsen-Anhalts (VDI, VDE, iK, RKW). 4/2025*

29 *https://en.wikipedia.org/wiki/Don%27t_be_evil*

30 *Pakalski, Ingo: Google verabschiedet sich von „Don't be evil". Golem-Online. 2018-5-21. https://www.golem.de/news/verhaltenskodex-google-verabschiedet-sich-von-don-t-be-evil-1805-134479.html*

31 *Schmid, Stefka; Diehl, Carlo; Reuter, Christian: Das gefährliche Bild des „KI-Wettrüstens": Wie Methapern die globale KI-Politik prägen. FIfF-Kommunikation 4/25, S. 19 – 22*

32 *Ebenda S. 21*

Werner Winzerling

Prof. Dr. **Werner Winzerling** (i. R.) ist Informatiker. Er wurde in der früheren DDR sozialisiert. Nach beruflichen Stationen in der Industrie und bei der Deutschen Telekom arbeitete er bis zu seiner Pensionierung am FB Angewandte Informatik der HS Fulda. Hier lehrte und forschte er auch auf dem Gebiet Informatik und Gesellschaft.

Laura Dornheim, ***Chief Digital Officer der Stadt München***

Digitale Souveränität in München: Ein Leitfaden für die Zukunft unserer Städte

In einer zunehmend digitalisierten Welt ist die Frage der digitalen Souveränität für Städte wie München von großer Bedeutung. Sie ist eine zentrale Voraussetzung für eine sichere, verlässliche und handlungsfähige Stadtverwaltung.

In den vergangenen Jahren haben wir alle die Herausforderungen der digitalen Transformation hautnah erlebt. Die Abhängigkeit von großen internationalen Konzernen, die Unsicherheiten in den globalen Lieferketten und die Frage, wie wir verantwortungsvoll mit unseren Daten umgehen, sind Themen, die uns alle betreffen. Digitale Souveränität ist kein abstraktes Zukunftsthema mehr. Sie ist eine Schlüsselkompetenz, die darüber entscheidet, ob Kommunen handlungsfähig bleiben – politisch, wirtschaftlich und technisch.

Digitale Souveränität: Ein Balanceakt

Was bedeutet digitale Souveränität konkret? Ein Gedankenexperiment: Stellen Sie sich eine Gefängniszelle vor – keine Wahlmöglichkeiten, totale Abhängigkeit. Im Kontrast dazu steht die Vorstellung einer einsamen Insel, auf der man alles selbst herstellen muss. Beide Szenarien sind Einschränkungen der Freiheit. Wahre digitale Souveränität liegt in der Balance. Es geht darum, eigenständig entscheiden zu können, welche Technologien wir nutzen, und dabei ein sicheres, stabiles Ökosystem zu schaffen.

Die drei Kernaspekte der digitalen Souveränität

Die Landeshauptstadt München orientiert sich bei ihrer Definition von digitaler Souveränität an den Vorgaben des Bundes. Digitale Souveränität beschreibt die Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können. Dies manifestiert sich in drei Kernaspekten:

1. **Selbstständigkeit:** Die Stadtverwaltung muss vollständig eigenständig handlungsfähig sein, wobei Abhängigkeiten von anderen Akteuren minimiert werden.

2. **Selbstbestimmtheit:** Wir müssen die Entscheidungshoheit über den Wechsel von Produkten und Anbietern haben und können jederzeit die Richtung unserer digitalen Transformation beeinflussen.

3. **Sicherheit:** Transparenz über Software, Herkunft, gesetzliche Vorgaben und Sicherheitsstandards ist unerlässlich, um das Vertrauen der Bürger in unsere digitalen Angebote zu sichern.

Digitale Souveränität ist dabei kein Selbstzweck, sondern wird stets gemeinsam mit anderen Kriterien wie Datenschutz, Barrierefreiheit, Nutzbarkeit und Funktionalität abgewogen.

Warum ist digitale Souveränität so wichtig?

Eine stabil funktionierende Behörden-IT ist Teil der kritischen Infrastruktur. Internationale Abhängigkeiten, geopolitische Spannungen und rechtliche Unsicherheiten können Risiken für den Betrieb, den Datenschutz oder die Kostenkontrolle bedeuten. Digitale Souveränität bedeutet nicht vollständige Unabhängigkeit von externen Anbietern. In einer multipel vernetzten Welt sind Abhängigkeiten unvermeidbar. Die Digitalisierung kann nur mit Arbeitsteilung und Partnerschaften vorankommen, was zwangsläufig Abhängigkeiten mit sich bringt.

Entscheidend ist, bewusst in jedem Einzelfall festzulegen, wo digitale Souveränität notwendig ist, um handlungsfähig zu bleiben, und inwieweit die in diesen Abhängigkeiten bestehenden Risiken verringert oder akzeptiert werden können. Genau daran arbeiten wir – mit dem Ziel, uns dort, wo es sinnvoll ist, möglichst digital souverän aufzustellen.

Die vier Säulen der digitalen Souveränität

In München verfolgen wir diesen Ansatz in vier zentralen Bereichen: Infrastruktur, Software, Daten und Menschen.

1. **Infrastruktur:** Wir haben in ein eigenes Rechenzentrum investiert, das uns die nötige Flexibilität und Sicherheit bietet. Dieses Rechenzentrum ist nicht nur ein technisches Fundament, sondern auch ein Symbol für unsere Unabhängigkeit. Es ermöglicht uns, digitale Dienste selbst zu betreiben und dabei die Kontrolle über unsere Daten zu behalten.

2. **Software:** Bei der Auswahl von Softwarelösungen setzen wir konsequent auf Open Source. Diese Herangehensweise ermöglicht es uns, Abhängigkeiten zu minimieren und die Transparenz zu erhöhen. Wo es nötig ist, nutzen wir auch marktübliche Lösungen, jedoch immer mit dem Ziel, die Kontrolle über unsere Systeme zu behalten. Wir verfolgen das Prinzip *Public Money, Public Code*, was bedeutet, dass Software, die mit öffentlichen Mitteln entwickelt wird, als

Open Source veröffentlicht wird. Dies fördert nicht nur die Zusammenarbeit und Innovation, sondern auch das Vertrauen der Bürgerinnen und Bürger in die digitalen Lösungen, die wir anbieten.

3. **Daten:** Ein zentraler Baustein digitaler Souveränität ist der souveräne Umgang mit Daten. Wir möchten Daten nicht nur für eine effizientere interne Verwaltung nutzen, sondern auch transparente, offene Datenangebote schaffen, die Wirtschaft, Wissenschaft, Start-ups und Zivilgesellschaft gleichermaßen zugutekommen. Dabei geht es nicht nur um die Bereitstellung, sondern auch um die qualitativ hochwertige Aufbereitung und die sichere Verwaltung dieser Daten. Einheitliche Standards und klare Verantwortlichkeiten sind entscheidend, um sicherzustellen, dass Daten verlässlich und datenschutzkonform genutzt werden können.

4. **Menschen:** Technologie allein schafft keine Souveränität. Es braucht Menschen, die diese Technologien verstehen, anwenden und weiterentwickeln. Deshalb setzen wir auf Weiterbildung und Teilhabe sowohl für unsere Mitarbeitenden in der Verwaltung als auch für unsere Bürgerinnen und Bürger. Digitale Kompetenz ist der Schlüssel, um technologische Entwicklungen selbstbewusst zu begleiten und aktiv zu gestalten. Nur so können wir sicherstellen, dass alle an der digitalen Transformation teilhaben und nicht in Abhängigkeit von großen Konzernen und ihren Algorithmen geraten.

Der Souveränitätscheck: Digitale Souveränität messbar machen

Ein entscheidender Schritt in Richtung digitaler Souveränität ist die systematische Bewertung unserer IT-Services. Hierbei setzen wir auf den neu entwickelten *Score für Digitale Souveränität (SDS)*. Diese Methodik wurde in Zusammenarbeit mit der Technischen Universität München entwickelt und ermöglicht uns, Abhängigkeiten, Risiken und Handlungsoptionen transparent zu machen.

Im Rahmen des Souveränitätschecks untersuchen wir verschiedene Aspekte, darunter Hersteller- und Anbieterabhängigkeiten, Wechselmöglichkeiten, Open-Source-Lösungen, offene Standards sowie Sicherheits- und Rechtsaspekte. Anhand eines strukturierten Fragenkatalogs und einer quantitativen Bewertung können wir den Grad der digitalen Souveränität unserer IT-Services bestimmen.

Aktuell haben wir 2.780 Anwendungsservices der Stadt München analysiert und 194 davon auf ihre digitale Souveränität geprüft. Die Ergebnisse zeigen, dass 74 Prozent dieser Services in den Kategorien 1, 2 und 3 eine hohe digitale Souveränität aufweisen. Diese Services sind nicht nur sicher, sondern auch flexibel und ermöglichen uns, potenzielle Risiken frühzeitig zu erkennen und zu minimieren.

Was machen wir mit diesen Ergebnissen?

Auf Basis der ermittelten Werte aus dem SDS dokumentieren wir systematisch Risiken, bereiten Umstiegsszenarien vor und stärken offene Standards in unseren Beschaffungen. Zudem informieren wir den Stadtrat jährlich über den Stand der digitalen Souveränität und wägen Umstiege stets unter Berücksichtigung von Wirtschaftlichkeit, Fachlichkeit und Sicherheit ab.

Digitale Souveränität ist ein Prozess, der nicht durch Einzelmaßnahmen entsteht, sondern durch transparente Bewertung, strategische Entscheidungen und langfristige Planung. Mit der Annahme der Beschlussvorlage zur digitalen Souveränität als strategisches Leitprinzip haben wir den Rahmen geschaffen, um diese Methodik weiterzuentwickeln und in unsere bestehenden IT-, Risiko- und Vergabeprozesse zu integrieren.

Gemeinsam den Wandel gestalten

Ich lade Sie ein, diesen Wandel aktiv mitzugestalten. Lassen Sie uns gemeinsam daran arbeiten, eine digitale Zukunft zu schaffen, die unseren Städten und unseren Bürgerinnen und Bürgern dient – sicher, verlässlich und in Verbundenheit mit anderen. Digitale Souveränität ist kein Elitenprojekt. Sie gelingt nur, wenn alle mitgenommen werden – von der Verwaltung über die lokale Wirtschaft bis zur Bürgerschaft.

Jeder von uns kann einen Beitrag leisten: kritisch hinterfragen, welche Dienste genutzt werden, wie Daten verarbeitet werden und ob es gute offene Alternativen gibt. In München legen wir großen Wert auf Beteiligung und Austausch, um eine Community zu bilden, die digitale Souveränität nicht nur versteht, sondern aktiv mitgestaltet.

Ich bin überzeugt, dass wir gemeinsam eine starke, demokratische und souveräne digitale Infrastruktur in Europa schaffen können. Denn am Ende bedeutet digitale Souveränität nichts anderes als die Freiheit, eigene Entscheidungen zu treffen.

Nicht als einzelne Person, nicht als einzelnes Unternehmen, nicht als einzelne Stadt, sondern gemeinsam als Gesellschaft, in der wir die gleichen Werte teilen und wissen, dass wir zusammen stärker sind als alleine.

Laura Dornheim

Dr. **Laura Dornheim** ist IT-Referentin und Chief Digital Officer (CDO) der Stadt München. Sie ist diplomierte Wirtschaftsinformatikerin und hat im Bereich Gender Studies promoviert. Dr. Dornheim verfügt über mehr als 20 Jahre Erfahrung in der digitalen Branche und genießt Anerkennung auch als Feministin und politisch engagierte Persönlichkeit. Als IT-Referentin und als CDO setzt sie sich neben der Digitalisierung für die Verwaltung insbesondere für die Digitale Teilhabe aller Bürger:innen in München sowie für die Verbesserung der BildungsIT in der Stadt ein.

Foto: Michael Nagy/LH München

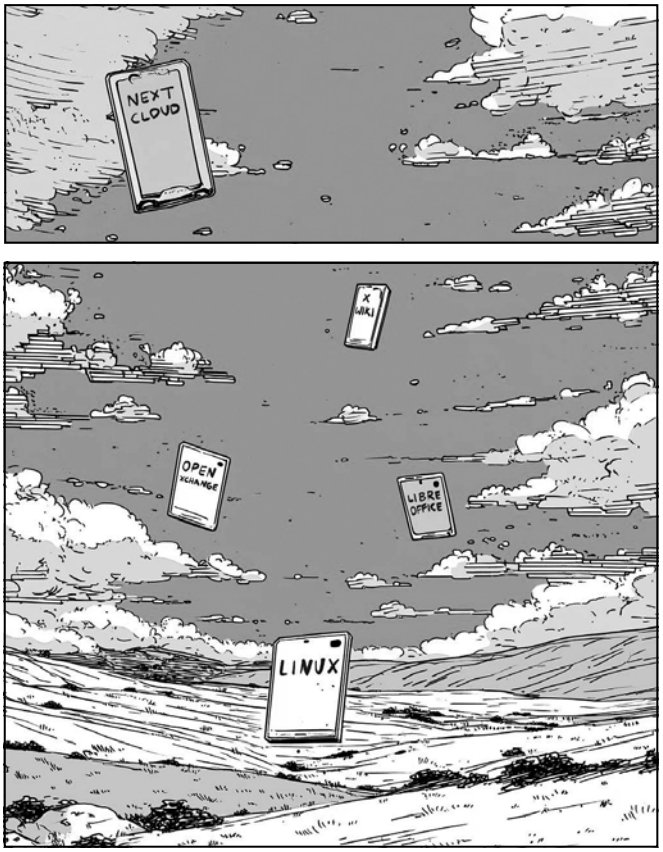
Der Ministerpräsident des Landes Schleswig-Holstein – *Staatskanzlei*

Digitalstrategie Schleswig-Holstein 2026

Schleswig-Holstein positioniert sich mit der Digitalstrategie 2026 als digitaler Vorreiter im Norden Europas. Die Strategie setzt auf digitale Souveränität, Open Source und gesellschaftlichen Nutzen. Ziel ist eine moderne, resiliente und bürgernahe Verwaltung, die technologische Innovationen konsequent mit den Bedürfnissen von Bürgerinnen und Bürgern sowie Unternehmen verknüpft und so den gesellschaftlichen Fortschritt aktiv gestaltet.

Im Folgenden werden Auszüge aus dem Gesamt-Dokument (Stand März 2026) abgedruckt.[1]

Strategisches Fundament



Digitale Souveränität und offene Innovation[2]

Motivation und Nutzen

Die digitale Transformation durchdringt alle Bereiche staatlichen Handelns – und das Informationssystem der Verwaltung ist längst systemrelevant geworden. Um in einer zunehmend dynamischen und globalisierten Technologielandschaft handlungsfähig zu bleiben, braucht das Land Schleswig-Holstein digitale Souveränität: also die Fähigkeit, zentrale digitale Prozesse, Systeme und Daten eigenständig gestalten, betreiben und kontrollieren zu können. Diese strategische Ausrichtung schützt nicht nur vor kritischen Abhängigkeiten, sondern stärkt Datenschutz, Informationssicherheit und das Vertrauen der Bürgerinnen und Bürger.

Der konsequente Einsatz von Open Source sowie die Öffnung von Entwicklungs- und Innovationsprozessen („Open Innovation") leisten hierzu einen zentralen Beitrag. Sie ermöglichen technologische Unabhängigkeit, beschleunigen Entwicklungszyklen und fördern eine vielfältigere Anbieterlandschaft. Davon profitiert der gesamte Digitalstandort Schleswig-Holstein – durch gesteigerte Resilienz, größere Flexibilität und ein innovationsfreundliches Klima.

Vision

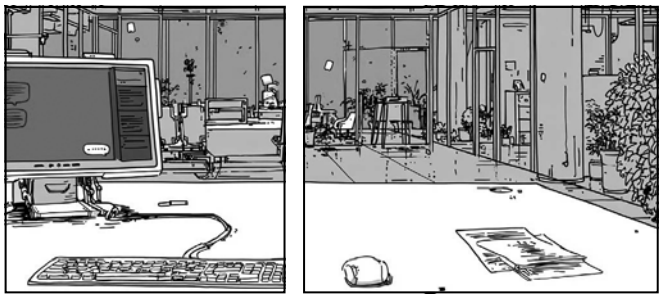
Langfristige Vision (5–10 Jahre): Schleswig-Holstein hat digitale Souveränität erfolgreich als gesamtgesellschaftliche Aufgabe etabliert. In einem ganzheitlichen Ansatz ist ein souveränes, offenes und zukunftsfähiges digitales Ökosystem entstanden – getragen von Verwaltung, Zivilgesellschaft, Wissenschaft und Wirtschaft. Technologische Entwicklungen werden eigenständig gestaltet und basieren auf offenen, transparenten Infrastrukturen.

Kurz bis mittelfristig steht der Umbau der Landes-IT im Sinne der digitalen Souveränität im Fokus:

- Das Rechenzentrum von Dataport wird bis Ende 2030 digital souverän aufgestellt.
- Die schrittweise Migration der Fachverfahren auf Open-Source-Basis wird unter Berücksichtigung der Wirtschaftlichkeit, der technischen Möglichkeit und des Beitrags zur Digitalen Souveränität bis Ende 2030 erreicht. Ausnahmen können die bereits in der Anwendung befindlichen, ressortübergreifend genutzten oder im Rahmen von länderübergreifenden Entwicklungsverbünden konzipierten Fachverfahren darstellen (z. B. KoPers oder VKoopUIS).
- Bis Mitte 2027 wird das Open Source Program Office Schleswig Holstein (OSPO SH) etabliert, das als zentrale kommunikative und beratende Schnittstelle den Wandel der Landes-IT hin zu mehr Offenheit und digitaler Souveränität unterstützt. Parallel hierzu entwickeln das OSPO SH und der DigitalHub SH bis Ende 2027 ein gemeinsam abgestimmtes Leistungsangebot, um die digitale Souveränität und offene Innovationskultur im Land sichtbar zu machen, zu stärken und über Landesgrenzen hinaus zu vertreten.
- Die Einführung offener Entwicklungsprinzipien ist ein zentraler Bestandteil der digitalen Transformation in Schleswig-Holstein. Bis Ende 2027 werden in der Landesverwaltung Schleswig-Holstein verbindliche vertragliche Grundlagen und organisatorische Richtlinien für offene Softwareentwicklung in mindestens zwei Verfahren geschaffen. Für die darauf aufbauende Beratung schaffen wir zentrale Beratungskompetenzen in der Landesverwaltung SH.

Abhängigkeiten und Synergien zu anderen Themenfeldern	
Cybersicherheit	Resilienz und Informationssicherheit sind Grundpfeiler digitaler Souveränität.
Tiefendigitalisierung & Digitale Plattform SH	Offene Standards und einheitliche Schnittstellen ermöglichen den Informationsaustausch und eine modulare, souveräne IT-Architektur.
Innovationsmanagement	Digitale Souveränität ist ein strategischer Hebel für langfristige, innovative Eigenentwicklungen auf Basis von Open Source.

Technische Infrastruktur & Plattformen



Die Digitale Plattform SH – Grundlage einer zukunftsfähigen Verwaltung[3]

Motivation und Nutzen

Das zentrale IT-Management betreibt die Digitale Plattform SH als infrastrukturelle Grundlage für die Digitalisierung der öffentlichen Verwaltung auf Landes- und Kommunalebene. Sie ist somit ein zentraler Baustein für die erfolgreiche Digitalisierung der Prozesse des öffentlichen Sektors. Besonders in einem Flächenland wie Schleswig-Holstein – mit seinen vielfältigen Verwaltungsstrukturen – ist ein langfristig ausgerichtetes Vorgehen essenziell, um ein einheitliches, flexibles und skalierbares digitales Fundament zu schaffen. Ohne ein weitgehend einheitliches Vorgehen beim Ausbau der Infrastruktur drohen Insellösungen, Doppelstrukturen und hohe Folgekosten: Parallelentwicklungen führen zu fragmentierten Prozessen, inkompatiblen Systemen und mangelnder Interoperabilität. Eine moderne digitale Plattform ermöglicht die Wiederverwendung von Diensten, eine zentrale Datenbasis, sichere Schnittstellen und die schnelle und kontinuierliche Einführung neuer digitaler Funktionen – und leistet damit einen entscheidenden Beitrag zur Effizienz und Zukunftsfähigkeit der öffentlichen Verwaltung im Land. Zugleich muss sich die digitale Plattform in die föderalen und europäischen E-Governmentstrukturen einbinden und ist damit Teil des digitalen Ökosystems des Landes.

Vision

Langfristige Vision (5–10 Jahre): Die Digitale Plattform SH bildet das technologische Rückgrat einer vollständig digitalisierten, integrierten, proaktiven und bürgernahen Verwaltung für Schleswig-Holstein. Sie bündelt alle zentralen Elemente der E-Government-Infrastruktur – von Infrastrukturkomponenten über Prozesse bis hin zu Daten – in einer modularen, standardisierten und resilienten Architektur, durch standardisierte Schnittstellen interoperabel auch innerhalb der bundesweiten Infrastruktur und darüber hinaus.

Lösungen werden auf Basis von OpenCode entwickelt und veröffentlicht, sodass strategische Abhängigkeiten vermieden, die digitale Souveränität der Verwaltung gewahrt und politische wie gesellschaftliche Ziele eigenständig umgesetzt werden können. Gleichzeitig entstehen breite Nachnutzungsmöglichkeiten für weitere Akteure und Organisationen im Sinne von offener Innovation (vgl. Themenfeld Digitale Souveränität und Offene Innovation).

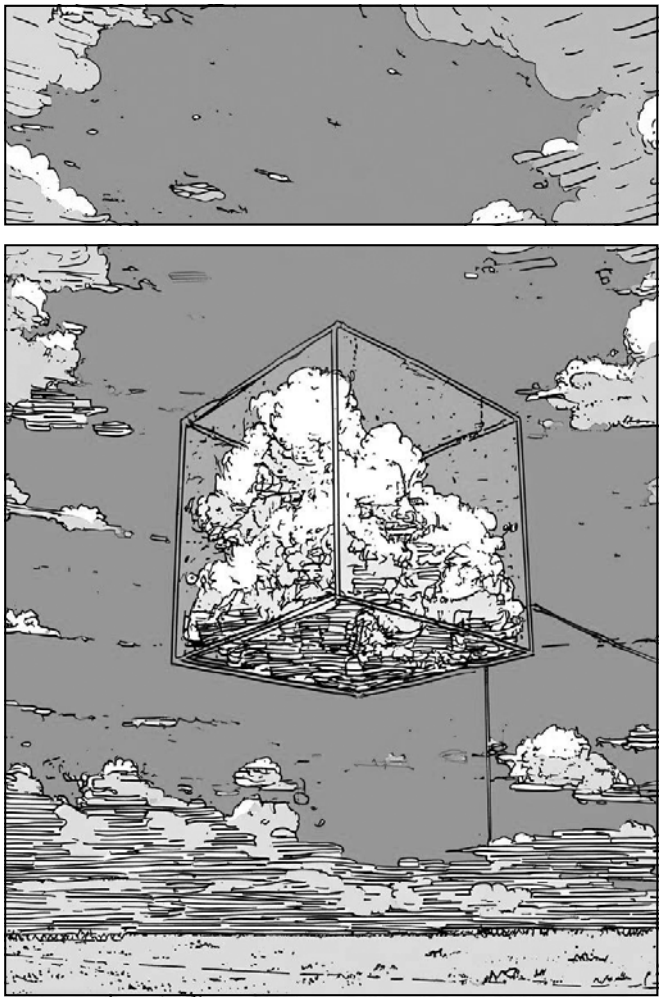
Digitale Lösungen ermöglichen ein proaktives Verwaltungshandeln, bei dem Leistungen initiativ und ressourceneffizient erbracht werden. Ein offener UX-Standard sorgt dafür, dass Anwendungen barrierefrei und intuitiv nutzbar sind. Neue Fachverfahren werden mithilfe von Formular-Assistenten und Low-Code-Technologien standardisiert, um Abläufe effizient und plattformfähig zu gestalten (vgl. Ende-zu-Ende Digitalisierung). Verwaltungsprozesse werden – wo technisch möglich und rechtlich zulässig – automatisiert und dafür gezielt digital tauglich ausgestaltet (vgl. Modernes Prozessmanagement sowie Rechtsrahmen). Den Kommunen stehen offene Infrastrukturen kostenfrei zur Verfügung, um diese in der Rolle als Dienstleister optimal zu unterstützen. Technologische Entwicklungen und Innovationen werden fortlaufend geprüft, sodass finanzielle Mittel effizient eingesetzt und Infrastrukturen nachhaltig sowie strategisch ausgerichtet sind (vgl. Innovationsmanagement sowie IT-Haushalts- und Finanzmanagement).

Kurz- bis mittelfristig besteht das Ziel, die langfristige Ausrichtung und Gestaltung der Digitalen Plattform des Landes Schleswig-Holstein strategisch bis 2026 zu beschreiben. Die Weiterentwicklung der E-Government-Infrastruktur soll durch einen ganzheitlichen, synergetischen Blick auf die Bedarfsbasis erfolgen. Hierzu werden ab dem 01.01.2027 alle Entwicklungsbedarfe über einen zentralisierten Prozess dokumentiert und entlang definierter Kriterien weiterverarbeitet. Zusätzlich werden die notwendigen Strukturen für ein E-Government-Infrastruk-

Abhängigkeiten und Synergien zu anderen Themenfeldern	
Service Design (Tiefendigitalisierung)	Alle Lösungen der Plattform werden barrierefrei und intuitiv nutzbar gestaltet.
Cybersicherheit	Der Ausbau erfolgt nach höchsten Sicherheitsstandards und vermeidet Single-Points-of-Failure.
Tiefen-digitalisierung	Ein standardisierter und koordinierter Ausbau der Plattform fördert die Integration der Landes-IT in der Tiefe. Einheitliche Standards und Schnittstellen der Plattform sorgen für durchweg integrierte Lösungen, auch über die Landesgrenze hinaus.
Digitale Souveränität	Jede Ausbauentscheidung der Plattform stärkt die Handlungsfähigkeit des Landes.

tur- bzw. Architektur-Management bis 2027 verstärkt. Ziel ist zudem, den Zugang zur digitalen Plattform über Maschinenschnittstellen zu öffnen und so die Integration der Plattform in andere Infrastrukturen zu ermöglichen.

Souveräne Cloud für eine resiliente Verwaltung in Schleswig-Holstein[4]



Motivation und Nutzen

Cloudtechnologien bilden eine zentrale technische Grundlage für die digitale Transformation der öffentlichen Verwaltung. Schleswig-Holstein verfolgt das Ziel, eine digital souveräne Cloudinfrastruktur aufzubauen und zu nutzen, die sowohl wirtschaftlich tragfähig als auch technologisch zukunftssicher ist. Dabei steht nicht nur die Effizienz des Verwaltungshandelns im Mittelpunkt, sondern auch die Stärkung der digitalen Selbstbestimmung im europäischen Rechtsrahmen.

Die Landesregierung bekennt sich klar zur Nutzung offener, europäisch geprägter Cloudlösungen. Im Rahmen der Deutschen Verwaltungscloud (DVC), deren Umsetzung Schleswig-Holstein als aktives Mitglied im Kundenbeirat mitgestaltet, sollen zentrale Fachverfahren cloudfähig entwickelt und bundesweit nachnutzbar bereitgestellt werden. Gleichzeitig kommen eigene Cloudlösungen über Dataport zum Einsatz – immer dort, wo dies wirtschaftlich sinnvoll und technologisch geboten ist. Beide Ansätze werden kontinuierlich gegeneinander abgewogen, um Handlungsspielräume zu erhalten und eine resiliente, zukunftsfähige IT-Infrastruktur für das Land zu etablieren. Durch die Kombination beider Ansätze entsteht zugleich eine zusätzliche Sicherheitsebene: Die Cloud dient auch als redundante Infrastruktur und ermöglicht im Bedarfsfall die schnelle Wiederherstellung kritischer Anwendungen und Daten. Damit wird die Cloud zum zentralen Bestandteil der Backup- und Ausfallsicherheitsstrategie des Landes.

Durch die Nutzung cloudbasierter Lösungen ergeben sich wesentliche Vorteile:

- Verwaltungsverfahren können effizienter, schneller und nutzerfreundlicher umgesetzt werden.
- Technologische Innovationen lassen sich leichter adaptieren und in die Praxis überführen.
- Die eingesetzte Infrastruktur kann wirtschaftlich betrieben und bedarfsgerecht skaliert werden.
- Ressourceneffizienz und Energieverbrauch werden durch moderne Rechenzentren verbessert – ein Beitrag zu mehr Nachhaltigkeit.

Vision

Langfristige Vision (5–10 Jahre): Schleswig-Holstein verfügt über eine souveräne Cloudinfrastruktur als Rückgrat einer modernen, sicheren und kooperativen Landes-IT. Fachverfahren werden modular, skalierbar und cloudfähig in einer einheitlichen Verwaltungs-Cloud betrieben. Die Landesverwaltung nutzt dabei sowohl eigene Lösungen über Dataport als auch gemeinsam mit dem Bund und anderen Ländern entwickelte Verfahren aus der DVC. Gleichzeitig stellt Schleswig-Holstein eigene cloudfähige Entwicklungen zur Nachnutzung bereit. Die Verwaltungs-Cloud wirkt so als verbindendes Infrastrukturelement, das technologische Weiterentwicklung ermöglicht und die Grundlage für eine resiliente, zukunftsfähige IT-Landschaft schafft.

Kurz- bis mittelfristig liegt der Fokus auf dem strukturierten Ausbau cloudfähiger Fachverfahren und der konsequenten Umsetzung einer dualen Cloudstrategie:

- der gezielten Nutzung eigener Cloudlösungen über Dataport einerseits,
- sowie der aktiven Beteiligung an der DVC andererseits.

Ein konkretes Leuchtturmprojekt ist die Entwicklung und Bereitstellung einer cloudfähigen Version einer E-Akte. Das Zentrale IT-Management bindet die Ressorts frühzeitig in die Entwicklung ein. Schleswig-Holstein wirkt hier über den Dienstleister Dataport auf eine Bereitstellung in der Deutschen Verwaltungscloud bis Ende 2027 hin.

Bis 2026 soll ein klarer Rahmen für die Cloud-Readiness von Fachverfahren und digitalen Services definiert und in den Ressorts verankert werden. Dabei ist die Integration neuer Technologien wie KI oder föderierter Datenplattformen von Anfang an

mitzudenken. Alle Cloudentscheidungen erfolgen auf Basis einer Wirtschaftlichkeitsbetrachtung. Schleswig-Holstein steht damit am Übergang von der Einführungs- zur Skalierungsphase seiner Cloudstrategie – mit dem Ziel, die Cloudfähigkeit der Landes-IT Schritt für Schritt auszubauen.

Abhängigkeiten und Synergien zu anderen Themenfeldern	
Cybersicherheit	Cloud-Infrastrukturen fördern die Resilienz der Verwaltung durch einen BSI-konformen, DSGVO-zertifizierten Betrieb und lassen sich flexibel an Bedarfe anpassen.
Green-IT	Moderne Cloud-Infrastrukturen bündeln Rechenkapazitäten effizient, können erneuerbare Energien nutzen und unterstützen so die Klimaneutralitätsziele des Landes.
Innovationsmanagement	Über die Cloud erhalten Verwaltung und Partner vereinfachten Zugang zu modernen digitalen Diensten.
Digitale Souveränität	Als staatlich kontrollierte und gemeinwohlorientierte Infrastruktur ist die Cloud ein zentraler Baustein für digitale Souveränität

Landesdatennetz und Registermodernisierung – die Zukunft der Dateninfrastruktur in Schleswig-Holstein[5]

Motivation und Nutzen

Für die erfolgreiche Verwaltungsdigitalisierung braucht es ein verbindendes Element, das zentrale Vorgehen zusammenführt. Informationsinseln bestimmen den Ist-Zustand: Fachverfahren und Datenbanken sind oft in sich geschlossen, Schnittstellen fehlen oder sind nur punktuell vorhanden.

Dieser Zustand steht einem vernetzten Verwaltungshandeln entgegen. Es gilt, eine grundlegende Fragestellung zu lösen: Wie können verschiedene Beteiligte und Organisationen sicher, effizient und datenschutzkonform miteinander kommunizieren und Daten austauschen – ohne zentrale Datenhaltung und ohne Medienbrüche? Initiativen wie die Registermodernisierung, die Bereitstellung von Verwaltungsleistungen und -services online (OZG/OZG 2.0) oder die Weiterentwicklung der E-Government-Infrastruktur haben bereits große Fortschritte erzielt, entfalten ihr volles Potenzial aber erst dann, wenn sie in einer gemeinsamen, sicheren und interoperablen Dateninfrastruktur verknüpft werden. Genau hier setzt Schleswig-Holstein an und geht voran: Schleswig-Holstein wird schrittweise ein Landesdatennetz entwickeln, das nicht nur die Verwaltung des Landes und der Kommunen verbindet, sondern auch die geregelte Einbindung nicht-öffentlicher Stellen ermöglicht für ein starkes digitales Ökosystem in Schleswig-Holstein und darüber hinaus. Bei der Entwicklung greift es auf bestehende und bewährte Lösungen (z. B. XRoad) zurück, die zudem die digitale Souveränität und Resilienz des Landes fördern.

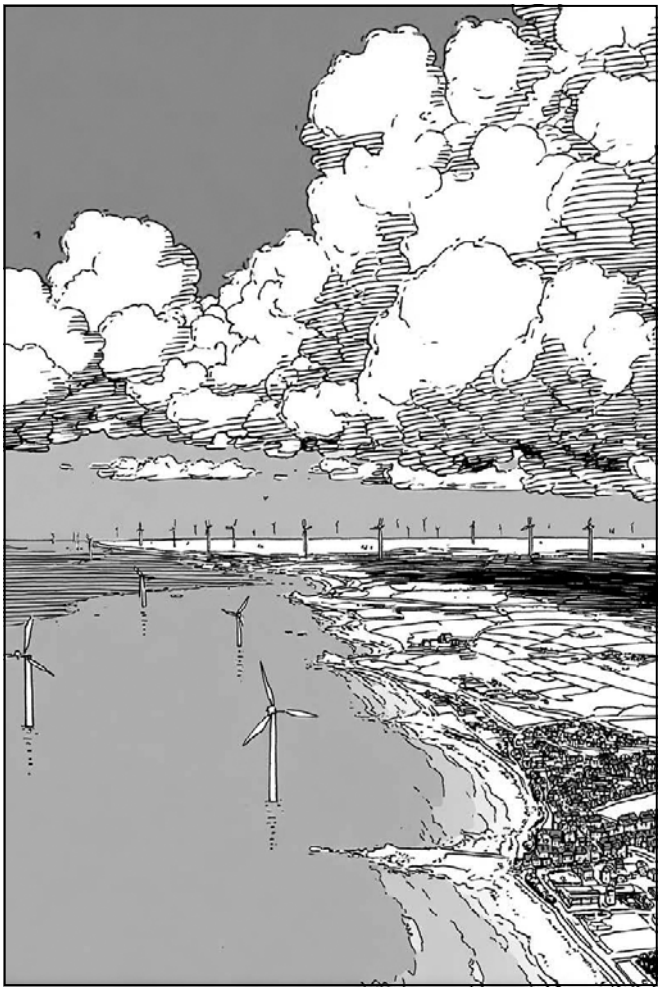
Dabei ist eine weitgehend dezentrale Datenhaltung aus föderaler Sicht keine technische Kompromisslösung, sondern ein bewusst gewähltes Ziel:

- Sie ermöglicht es beteiligten Stellen, die Hoheit über ihre Daten zu behalten,
- Sie reduziert zentrale Abhängigkeiten und erhöht die Resilienz gegenüber technischen Ausfällen oder Sicherheitsvorfällen (Stichwort „single point of failure"),
- Sie erlaubt flexible Anpassungen an lokale Gegebenheiten und fördert die Selbstverwaltung.

Gleichzeitig bringt diese Dezentralität technische Herausforderungen mit sich: Denn für eine funktionierende, digital vernetzte Verwaltung müssen dezentrale Systeme dennoch in der Lage sein, sicher, standardisiert und effizient miteinander zu kommunizieren.

Vision

Langfristige Vision (5–10 Jahre): Schleswig-Holstein verfügt über ein leistungsfähiges Landesdatennetz, das alle zentralen Bereiche der Verwaltungsdigitalisierung verbindet. Fachverfahren sind durchgängig angebunden, sodass Leistungen – etwa die Beantragung von Wohngeld oder eines Kita-Platzes – vollständig digital, medienbruchfrei und ohne doppelte Dateneingaben erfolgen können. Die E-Government-Infrastruktur ist integriert: Zahlungen werden automatisch ausgelöst, Bescheide digital bereitgestellt und Bürgerinnen und Bürger über sichere Nachrichtenkanäle informiert. Registerdaten werden über eine



zentrale Plattform bereitgestellt, wodurch das Once-Only-Prinzip Realität ist und die Registermodernisierung nahtlos gelingt.

Grundlage dafür ist ein durchgängiger, sicherer und vertrauenswürdiger Datenaustausch zwischen Verwaltung, Wirtschaft und Gesellschaft, der organisationsübergreifend und unter Wahrung dezentraler Datenhoheit funktioniert. Zugleich ermöglicht es die Vernetzung mit föderalen Infrastrukturen und bildet damit das Rückgrat zentraler Digitalisierungsvorhaben wie des OZG 2.0, der Registermodernisierung (NOOTS) und der vernetzten Nutzung öffentlicher Daten. Das Land stellt dafür alle zentralen Infrastrukturen bereit und hat die Kommunen erfolgreich bei der dezentralen Anbindung unterstützt.

Einheitliche, interoperable Standards sorgen dafür, dass Daten einmalig erfasst und bereichsübergreifend effizient, rechtssicher und transparent genutzt werden. Offene Technologien (Open-Code) stärken die digitale Souveränität der Verwaltung und ermöglichen eine skalierbare, flexible Anbindung unterschiedlichster Akteure im ganzen Land – von kleinen Kommunen bis hin zu öffentlichen Unternehmen wie Stadtwerken, ÖPNV-Betrieben oder Krankenkassen.

Die gemeinsame Infrastruktur bildet außerdem die Basis für datenbasierte Kooperationen in Bereichen wie Mobilität, Energie, Gesundheit oder Smart City. So ist ein zukunftssicheres, digitales Ökosystem mit starkem Community-Gedanken entstanden, das Interoperabilität, Sicherheit, Innovationsfähigkeit und eine vernetzte, souveräne öffentliche Verwaltung im föderalen Kontext vereint.

Bürgerinnen und Bürger erleben dadurch eine Verwaltung, die schneller, transparenter und nachvollziehbarer arbeitet – vom Kita-Platz bis zur Baugenehmigung.

Kurz- bis mittelfristig konzentriert sich das Land auf folgende Ziele:

- Verprobung der Anbindung eines öffentlichen Registers über das Landesdatennetz an das NOOTS und erste Maßnahmen zur Umsetzung des Identifikationsnummerngesetzes (IDNrG)
- Bereitstellung eines Open-Source-Adapters bis Ende 2026, mit dem Kommunen ihre Systeme technisch an das Landesdatennetz anschließen können
- Umsetzung eines rein kommunalen Pilotszenarios für den Once-Only-Datenaustausch zwischen zwei Kommunen bis Mitte 2026 mit Unterstützung des ITV.SH
- Vorbereitung und Test erster grenzüberschreitender Datenaustausch-Szenarien mit europäischen Partnern im Ostseeraum bis Ende 2027.
- Anbindung einer Zentralen Registerplattform an das Landesdatennetz bis Ende 2026

Abhängigkeiten und Synergien zu anderen Themenfeldern	
Tiefen-digitalisierung	Das Landesdatennetz bündelt alle Elemente, damit das Once-Only-Prinzip funktioniert und Verwaltungsleistungen medienbruchfrei erbracht werden können.
Datenbasiertes Verwaltungs-handeln	Einheitliche Schnittstellen und Datenformate sind die Grundlage für ein funktionierendes Datennetzwerk und für ein offenes Landesdatennetz.
Cybersicherheit	Ein Landesdatennetz muss höchsten Sicherheitsstandards genügen, um vertrauenswürdig zu sein und kritische Verwaltungsprozesse abzusichern
Digitale Souveränität und offene Innovation	Ein geregelter Zugang für nicht-öffentliche Stellen und Organisationen (z. B. Stadtwerke, Hochschulen, Unternehmen) macht das Netz zu einer Plattform für neue Ökosysteme und Innovationen.

Anmerkungen

1 *Das vollständige Dokument befindet sich unter: https://www.schleswig-holstein.de/DE/landesregierung/themen/digitalisierung/digitalisierung-zukunftsthema/Digitale-Verwaltung/digitalstrategie/_documents/digitalstrategie2026.pdf?__blob=publicationFile&v=4*
2 *S. 28-30*
3 *S. 38-39*
4 *S. 40-42*
5 *S. 43-45*

Land Schleswig-Holstein – Staatskanzlei

Der Ministerpräsident des Landes Schleswig-Holstein
Staatskanzlei
Düsternbrooker Weg 104
24105 Kiel

Tomas Rudl

Verfahren gegen Tech-Konzerne: EU-Kommission zögert, Abgeordnete verlieren Geduld

7. Mai 2026 – *Wann setzt Europa seine Digitalgesetze gegen Tech-Konzerne durch? Die EU-Kommission knickt ein, fürchten Abgeordnete und Vertreter:innen der Zivilgesellschaft. Nun wollen sie Kommissionspräsidentin Ursula von der Leyen Beine machen.*

Der Druck steigt auf die EU-Kommission, europäische Digitalgesetze konsequent durchzusetzen. In einem offenen Brief[1] fordern dutzende zivilgesellschaftliche Organisationen EU-Kommissionspräsidentin Ursula von der Leyen (CDU) auf, den Digital Markets Act (DMA) „buchstabengetreu und frei von politischer Einflussnahme" zu vollstrecken.

Ähnliche Töne kommen aus dem EU-Parlament. Externer Druck dürfe die Souveränität und Autonomie der EU bei der Festlegung ihrer eigenen Regeln nicht beeinträchtigen, mahnen die Abgeordneten in einer vergangene Woche verabschiedeten Resolution[2]. Wirksame und verhältnismäßige Geldstrafen seien „unerlässlich, um Abschreckung zu gewährleisten und die Wirksamkeit des Gesetzes über digitale Märkte zu sichern", so der Tenor der nicht bindenden Entschließung.

Hintergrund für die Appelle sind vermehrte Zeichen, dass die EU-Kommission Beißhemmungen gegenüber großen, vor allem in den USA ansässigen Tech-Unternehmen hat – genau die Unternehmen, deren Macht der DMA eigentlich einhegen soll. Das seit wenigen Jahren wirksame Gesetz macht sogenannten Gatekeepern[3], die in bestimmen Digitalsektoren übermäßig viel Marktmacht angesammelt haben, eine Reihe von Auflagen, um einen funktionierenden Wettbewerb sicherzustellen.

Ergebnis im Google-Verfahren überfällig

Zwar hat die EU-Kommission, die für die Aufsicht der Gatekeeper zuständig ist, zahlreiche Untersuchungen wegen Verdachts von DMA-Verletzungen eingeleitet. Vor über einem Jahr hatte sie etwa Google und Apple vorgeworfen, ihre App-Marktplätze[4] nicht ausreichend zu öffnen. Zum anderen sollte Google in der Suchmaschine eigene Angebote für Shopping oder Reisen bevorzugt haben.

Auf das Ergebnis dieser Untersuchungen wartet die Öffentlichkeit jedoch weiterhin. Fällig wäre es Ende März gewesen. Darauf scheint sich Alphabet vorbereitet zu haben: Anonyme Quellen hatten der Nachrichtenagentur Reuters zufolge zu Beginn des Jahres in Aussicht gestellt, dass Google seine Wettbewerber prominenter in den Suchergebnissen anzeigen[5] werde, um der drohenden Geldstrafe zu entgehen. Umgesetzt hat Google das nicht.

Von der Leyen soll auf der Bremse stehen

Tatsächlich soll die EU-Wettbewerbsabteilung zu dem Schluss gekommen sein, dass Alphabet gegen den DMA verstoßen habe, berichtete jüngst das Handelsblatt[6]. Die Entscheidung – samt einer milliardenschweren Geldbuße – soll jedoch nach einer Intervention von Ursula von der Leyen wieder in der Schublade verschwunden sein.

Dem Fachblatt The Capitol Forum[7] zufolge soll die Kommissionspräsidentin bereits seit Januar auf der Bremse[8] stehen. Anstelle einer Verurteilung setzte die Kommission seit Jahresanfang weitere Verfahren in die Welt[9]: Unter anderem will sie Alphabet dabei unterstützen, das Android-Betriebssystem für Entwickler:innen weiter zu öffnen sowie Dritt-Anbietern den Zugriff auf bestimmte Daten der Google-Suchmaschine zu geben.

Auf Anfrage bestreitet die EU-Kommission die Vorwürfe. „Es gibt absolut keine politische Blockade von Fällen", sagte heute ein Kommissionssprecher bei einem Presse-Briefing[10]. Abgeschlossene Untersuchungen seien auch in ihrem Interesse. Es gehe nicht darum, eine Strafe nur der Strafe wegen zu verhängen. Eine Entscheidung werde von der Kommission erst dann final abgesegnet, wenn sie „technisch fertig und solide genug" sei, so der Sprecher.

Europäische Digitalgesetze, neben dem DMA auch der Digital Services Act (DSA) oder die Datenschutz-Grundverordnung (DSGVO), sind für große Tech-Konzerne wie Alphabet oder Apple ein rotes Tuch. Jahrzehntelang konnten sie weitgehend ungehindert wachsen und bestimmte Marktsegmente besetzen, ohne auf nennenswerten Widerstand von Kartellbehörden zu stoßen. Vor allem der in der ersten Amtsperiode von der Leyens verabschiedete DMA hat das wachsende Ungleichgewicht auf digitalen Märkten im Visier.

Mit dem Wahlsieg Donald Trumps und seiner America-First-Agenda hat die Tech-Branche einen willigen Unterstützer[11] in ihrem Kampf gegen angebliche Überregulierung gefunden. Unmittelbar nach seinem Amtsantritt im Januar 2025 legte der US-Präsident etwa in einem Memorandum[12] mit Verweis auf DMA und DSA fest, US-amerikanische Unternehmen vor „Erpressung und unfairen Geldbußen aus dem Ausland" schützen zu wollen.

Meeting between Ursula von der Leyen, President of the EC, and Donald Trump, President of the United States – 2025
Foto: Fred Guerdin/European Union, CC BY 4.0

Gedroht hatte Trump unter anderem mit Strafzöllen, die er einige Monate später tatsächlich vorstellte[13]. Zwar konnte sich die EU im Spätsommer auf einen Deal mit den USA einigen, ohne auf dem Papier die Digitalgesetze anzufassen. Vom Tisch ist die Auseinandersetzung jedoch nicht: Bis heute haben sich die EU-Institutionen nicht darauf geeinigt[14], wie die Zollvereinbarung aus dem Vorjahr umgesetzt werden soll.

„Die EU-Kommission knickt ein"

Auch für die US-Seite ist die Angelegenheit nicht abgeschlossen. Hochrangige US-Vertreter schießen weiterhin gegen EU-Digitalgesetze und verknüpfen sie mit dem Handelsstreit. Die EU müsse ihre Regulierung von Big Tech lockern, um im Gegenzug geringere Zölle auf Stahl und Aluminium entrichten zu müssen, sagte US-Handelsminister Howard Lutnick im Herbst[15]. Zugleich warnte der US-Botschafter bei der EU, Andrew Puzder, dass der DMA zu sehr auf US-amerikanische Tech-Konzerne[16] ziele.

Im April war bekannt geworden, dass die EU-Kommission ein Gremium[17] plant, um der Trump-Regierung entgegenzukommen. Darin soll sich die US-Regierung mit der EU zu Digitalregeln und Kartellverfahren abstimmen, wie die EU-Kommission dem Handelsblatt bestätigte[18].

Das nachgiebige und intransparente Vorgehen der EU-Kommission stößt jedoch immer mehr auf Kritik[19]. Felix Duffy von der Nichtregierungsorganisation LobbyControl sagt etwa: „Die EU-Kommission knickt ein und sendet ein fatales Signal: Wenn Tech-Konzerne bei Verstößen gegen die EU-Digitalregeln keine Konsequenzen zu fürchten haben, bleiben Gesetze wie der DMA wirkungslos."

Dem pflichtet Max Bank von der Organisation Rebalance Now[20] bei: Zwar zeige der DMA Wirkung[21], drohe aber zum zahnlosen Tiger zu werden, weil die Kommission nicht konsequent handle. „Wenn selbst überfällige Strafzahlungen gegen Konzerne wie Google politisch gestoppt werden, untergräbt das die Glaubwürdigkeit des Gesetzes", sagt Bank.

Referenz: https://netzpolitik.org/2026/verfahren-gegen-tech-konzerne-eu-kommission-zoegert-abgeordnete-verlieren-geduld/

Anmerkungen

1 *https://static1.squarespace.com/static/5e449c8c3ef68d752f3e70dc/t/69f9e35a1ae3236ed929a5c7/1777984350612/Google+DMA+Fine+Letter*
2 *https://www.europarl.europa.eu/news/de/press-room/20260423IPR41844/gesetz-uber-digitale-markte-durchsetzen-trotz-externen-politischen-drucks*
3 *https://netzpolitik.org/2023/digitale-gatekeeper-einer-fehlt-im-club-der-grossen/*
4 *https://netzpolitik.org/2025/digital-markets-act-apple-und-google-sollen-sich-weiter-oeffnen/*
5 *https://www.reuters.com/world/google-test-changes-search-results-source-says-eu-fine-looms-2026-02-25/*
6 *https://www.handelsblatt.com/politik/international/tech-konzern-google-umgeht-vorerst-milliardenstrafe-der-eu/100217105.html (€)*
7 *https://library.thecapitolforum.com/docs/9fwr216j88fk (€)*
8 *https://bsky.app/profile/capitolforum.bsky.social/post/3ml4em6zynk2l*
9 *https://ec.europa.eu/commission/presscorner/detail/en/ip_26_202*
10 *https://audiovisual.ec.europa.eu/en/media/video/I-289037*
11 *https://netzpolitik.org/2024/us-milliardaere-big-tech-fuer-trump/*
12 *https://netzpolitik.org/2025/dma-dsa-und-dsgvo-trump-droht-mit-zoellen-gegen-eu-regulierung-von-big-tech/*
13 *https://netzpolitik.org/2025/zollkrieg-im-digitalen-was-die-eu-gegen-donald-trump-in-der-hand-hat/*
14 *https://www.zeit.de/wirtschaft/2026-05/eu-einigung-ausbleiben-zoelle-usa-donald-trump*
15 *https://www.ft.com/content/19912b20-582d-46fe-90a5-ee208a28f4df?syn-25a6b1a6=1*
16 *https://www.ft.com/content/b6d9fb9c-901e-42e3-9610-5a449247fd49?syn-25a6b1a6=1*
17 *https://netzpolitik.org/2026/neues-gremium-geplant-eu-will-trump-bei-digitalgesetzen-entgegenkommen/*
18 *https://www.handelsblatt.com/politik/international/apple-meta-und-co.-eu-kommt-trump-bei-digitalregulierung-entgegen/100211705.html*

Tomas Rudl

Tomas Rudl[22] ist in Wien aufgewachsen, hat dort für diverse Provider gearbeitet und daneben Politikwissenschaft studiert. Seine journalistische Ausbildung erhielt er im *Heise-Verlag*, wo er für die *Mac & i*, *c't* und *Heise Online* schrieb.
Kontakt: *E-Mail*[23] (*OpenPGP*[24]), *Bluesky*[25]

19 *https://www.lobbycontrol.de/pressemitteilung/von-der-leyen-stoppt-milliardenstrafe-gegen-google-kritik-von-parlament-und-zivilgesellschaft-125080/*
20 *https://rebalance-now.de/ueber-uns/*
21 *https://netzpolitik.org/2026/bilanz-zum-digital-markets-act-eu-digitalgesetz-ist-kein-selbstlaeufer/*
22 *https://netzpolitik.org/author/tomas/*
23 *mailto:tomas@netzpolitik.org*
24 *https://keys.openpgp.org/search?q=tomas%40netzpolitik.org*
25 *https://bsky.app/profile/tomasrudl.bsky.social*

Andre Meister

Bundesregierung beschließt anlasslose Vorratsdatenspeicherung

22. April 2026 – *Die Bundesregierung nimmt einen dritten Anlauf zur Vorratsdatenspeicherung. Internet-Zugangs-Anbieter sollen IP-Adressen aller Nutzer speichern – anlasslos und massenhaft. Internet-Dienste wie E-Mails und Messenger müssen auf Anordnung ebenfalls Daten speichern und herausgeben.*

Die Bundesregierung hat heute den Gesetzentwurf zur Vorratsdatenspeicherung[1] beschlossen. Das verkünden Justizministerin[2], Innenministerium[3] und Bundesregierung[4]. Damit geht das Gesetz in den Bundestag.

Das Gesetz verpflichtet Internet-Zugangs-Anbieter, IP-Adressen und Port-Nummern sämtlicher Nutzer drei Monate lang zu speichern, ohne Anlass und ohne Verdacht auf eine Straftat.

Behörden dürfen ohne Richtervorbehalt auf die Vorratsdaten zugreifen. Mit dem Gesetz gegen digitale Gewalt[5] sollen auch Privatpersonen in Zivilverfahren auf die Vorratsdaten zugreifen.

Auf Anordnung müssen auch Internet-Dienste wie E-Mail-Anbieter und Messenger Verkehrsdaten drei Monate lang speichern und herausgeben.

Das ist bereits das dritte Gesetz zur Vorratsdatenspeicherung in Deutschland. Sowohl das erste Gesetz von 2007[6] als auch das zweite Gesetz von 2015[7] wurden von höchsten Gerichten gekippt.

Die verfassungswidrigen Vorgänger-Gesetze wurden mit Terrorismus begründet. Die Bundesregierung begründet das neue Gesetz mit Fake-Shops und digitaler Gewalt[8].

Demo gegen VDS und ACTA in Linz Endstation
Foto: a_kep/subtext.at, CC BY 2.0

Mehr Behörden, mehr Fälle

Im Dezember hatte SPD-Justizministerin Stefanie Hubig einen ersten Gesetzentwurf vorgestellt[9]. In den Verhandlungen mit Innen- und Digitalministerium wurden noch ein paar Dinge verändert[10].

Ursprünglich sollten nur Strafverfolgungs- und Polizeibehörden die Vorratsdaten abfragen. Jetzt dürfen auch „andere berechtigte Stellen" die Daten nutzen, darunter Geheimdienste wie Verfassungsschutz, Finanzbehörden und Zoll.

Die Behörden sollen Verkehrsdaten nicht mehr nur abfragen dürfen, wenn eine Ermittlung „auf andere Weise aussichtslos wäre", sondern bereits, wenn sie sonst „wesentlich erschwert wäre".

Der neue Entwurf stellt klar, dass lokale WLANs nicht unter die Speicherpflicht fallen, neben Hotels auch Freifunk. Daten sollen nicht länger als drei Monate gespeichert werden, auch wenn eine Internet-Verbindung länger besteht. Das war im ersten Entwurf noch vorgesehen[11].

Berufsgeheimnisträger sollen nicht geschützt werden, das hatten unter anderem Medien-Vereinigungen[12] vergeblich gefordert.

Hunderttausende Abfragen

Grundrechtseingriffe müssen notwendig und verhältnismäßig sein. Andere Länder wie die USA haben keine Vorratsdatenspeicherung, dort ist sie nicht notwendig. Deutschland hatte schon mal eine Vorratsdatenspeicherung. Damals hat das Max-Planck-Institut für Strafrecht wissenschaftlich untersucht: Es gibt ohne Vorratsdatenspeicherung keine Schutzlücken in der Strafverfolgung[13].

Im Gesetzentwurf versucht die Bundesregierung abzuschätzen, wie oft die Polizei Vorratsdaten abfragen wird. Sie kommen auf 143.000 pro Jahr – 86.000 Abfragen durch das Bundeskriminalamt und 57.000 Abfragen durch die Länder.

Diese Schätzung widerspricht den Daten der Telekom. Ganz ohne Vorratsdatenspeicherung hat die Telekom in einem Jahr fast 290.000 Abfragen zu IP-Adressen[14] bekommen – wegen mutmaßlicher Urheberrechtsverletzungen im Internet.

Tausende Anbieter betroffen

Die Speicherpflicht betrifft „unterschiedslos alle Anbieter von Internetzugangsdiensten", in Deutschland etwa 700. Verbände rechnen mit Kosten von ein bis zwei Millionen Euro für große und 80.000 Euro für kleine Internet-Anbieter.

Die Abfrage von Verkehrsdaten betrifft „alle Anbieter von Telekommunikationsdiensten", also auch Anbieter für E-Mail und Messenger. Die Bundesnetzagentur rechnet mit „rund 3.000 Verpflichteten". Nicht alle Anbieter sind auch kommerzielle Unternehmen, es gibt auch ehrenamtliche und gemeinnützige Anbieter.

Die Bundesregierung schafft also mehr Regulierung und Belastungen für Internet-Dienste, gegen deren Willen[15].

„Rechtswidrig, fehlgeleitet, gefährlich"

Vor 20 Jahren haben zehntausende Menschen gegen die Vorratsdatenspeicherung demonstriert[16]. Auch heute ist der Widerstand breit.

Der Deutsche Anwaltverein kritisierte bereits den Entwurf[17] mit deutlichen Worten: Die Regierung „setzt sich über die europarechtlichen Maßgaben hinweg" und steht „nicht mit den grundrechtsschützenden Intentionen des Gerichtshofs in Einklang". Eine „wirksame Begrenzung der Verwendungszwecke" fehlt, deshalb ist „die vorgeschlagene Vorratsdatenspeicherung europarechtswidrig".

Die Digitale Gesellschaft[18] kritisiert:

> *Die Vorratsdatenspeicherung ist immer noch ein fehlgeleiteter Ansatz. Es gibt keine Evidenz für die Verhältnismäßigkeit dieser radikalen Massenüberwachung. Tatsächlich wären in erheblichem Ausmaß unbescholtene Bürger*innen betroffen.*

Das Zentrum für Digitalrechte und Demokratie[19] kritisiert:

> *In einer Zeit, in der neue Technologien immer stärker in die Privatsphäre eindringen und zugleich autoritäre Kräfte an Macht und Einfluss gewinnen, stellt sich noch die Frage: Was passiert, wenn Regierungen ihre Polizeibehörden dazu anweisen oder ermuntern, ihre Zugriffsmöglichkeiten auf IP-Adressen und Portnummern zu nutzen, um gegen politische Gegner vorzugehen?*

Anwaltverein: „Rechtmäßigkeit fraglich"

Der Deutsche Anwaltverein[20] kritisiert:

> *Auch eine abgespeckte Vorratsdatenspeicherung bleibt eine Vorratsdatenspeicherung. Die anlasslose IP-Adressenspeicherung betrifft die Rechte von Millionen unbescholtener Bürgerinnen und Bürger – während Kriminelle genügend Möglichkeiten kennen, ihre Identität zu verschleiern.*
>
> *Die Speicherdauer von drei Monaten geht deutlich über das erforderliche Maß hinaus. Für die Verwertung ist weder eine richterliche Kontrolle noch eine Beschränkung auf eine Mindestschwere der aufzuklärenden Straftat vorgesehen. Damit ist die Vereinbarkeit mit Verfassungs- und Europarecht fraglich.*

Linke: „Massenüberwachung durch die Hintertür"

Die Linke im Bundestag[21] kritisiert:

> *Dieser Entwurf wird erneut vor den Gerichten krachend scheitern. Ich fordere die Bundesregierung auf, diese Täuschung zu beenden und den Entwurf zurückzuziehen. Als Linke lehnen wir jegliche Vorratsdatenspeicherung ab.*

Internetwirtschaft: „Beschluss hochproblematisch"

Der Verband der Internetwirtschaft eco[22] kritisiert:

> *Auch nach dem Kabinettsbeschluss gilt: Der Entwurf verfehlt die Vorgaben des Europäischen Gerichtshofs und schafft erneut eine anlasslose Datenspeicherung ohne nachweisbaren Mehrwert für die Strafverfolgung. Drei Monate IP-Adressspeicherung bedeuten nicht mehr Sicherheit, sondern mehr Datenspeicherung auf Verdacht.*

Grüne: „Zentrales Bürgerrechtsthema"

Die Grünen im Bundestag[23] kritisieren:

> *Auch die jüngste Vorlage der Bundesregierung mit einer dreimonatigen Speicherfrist begegnet weiterhin erhebli-*

Andre Meister

Andre Meister[24] ist investigativer Journalist. Er hat *netzpolitik.org* mit aufgebaut, Auszeichnungen erhalten und Strafanzeigen gestellt wie kassiert. Andre ist Gründungsmitglied der Vereine *netzpolitik.org*[25], *Gesellschaft für Freiheitsrechte*[26] und *Digitale Gesellschaft*[27], Mitglied im *Chaos Computer Club*[28], Beobachter bei *European Digital Rights*[29] und Beirat beim *Centre for Democracy & Technology Europe*[30]. Nebenbei arbeitet er als System-Administrator.
Kontakt: E-Mail[31] (OpenPGP[32]), Signal[33], Mastodon[34], Bluesky[35], FragDenStaat[36].

chen juristischen Bedenken, bspw. mit Blick auf die Frage, ob die dezidierten Vorgaben höchster Gerichte (die u. a. die Speicherdauer auf das absolute Minimum beschränken) eingehalten werden. Die Gefahr, dass auch diese Regelung nicht lange Bestand haben wird, ist daher sehr real.

Referenz: https://netzpolitik.org/2026/dritter-versuch-bundesregierung-beschliesst-anlasslose-vorratsdatenspeicherung/

Anmerkungen

1 *https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/DE/2025_IP_Speicherung.html*
2 *https://www.bmjv.de/SharedDocs/Pressemitteilungen/DE/2026/0422_Gesetzentwurf_Vorsorgliche_Sicherung_von_IP-Adressen.html*
3 *https://www.bmi.bund.de/SharedDocs/kurzmeldungen/DE/2026/04/ip-adressen.html*
4 *https://www.bundesregierung.de/breg-de/bundesregierung/bundeskanzleramt/kabinett-ip-adressen-2422604*
5 *https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/DE/2026_Gesetz_gegen_digitale_Gewalt.html*
6 *https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2010/03/rs20100302_1bvr025608.html*
7 *https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2023/02/rk20230215_1bvr014116.html*
8 *https://www.bmjv.de/SharedDocs/Pressemitteilungen/DE/2026/0422_Gesetzentwurf_Vorsorgliche_Sicherung_von_IP-Adressen.html*
9 *https://netzpolitik.org/2025/anlasslose-speicherung-justizministerium-veroeffentlicht-gesetzentwurf-zur-vorratsdatenspeicherung/*
10 *https://api.draftable.com/compare/EjtKwzTXQYxd*
11 *https://netzpolitik.org/2026/gesetzentwurf-vorratsdatenspeicherung-deutlich-laenger-als-drei-monate/*
12 *https://www.reporter-ohne-grenzen.de/artikel/pressemitteilungen/4187/reporter-ohne-grenzen-und-medienbundnis-lehnen-vorratsdatenspeicherung-ab*
13 *https://web.archive.org/web/20120216223116/www.mpg.de/5000721/vorratsdatenspeicherung.pdf*
14 *https://www.telekom.com/en/company/data-privacy-and-security/news/germany-363566*
15 *https://www.space.net/aktuelles/artikel/freiheitsrechte-nicht-leichtfertig-opfern/*
16 *https://de.wikipedia.org/wiki/Freiheit_statt_Angst*
17 *https://anwaltverein.de/files/media/news/replicator/stellungnahmen/2026/dav-sn_8-2026.pdf*
18 *https://digitalegesellschaft.de/2026/04/vorratsdatenspeicherung-pressemitteilung/*
19 *https://digitalrechte.de/news/bundesregierung-will-ip-adressen-aller-deutschen-fuer-drei-monate-speichern*
20 *https://anwaltverein.de/newsroom/abgespeckte-vorratsdatenspeicherung-bleibt-vorratsdatenspeicherung*
21 *https://www.dielinkebt.de/presse/pressemitteilungen/detail/massenueberwachung-durch-die-hintertuer-bundesregierung-taeuscht-oeffentlichkeit-bei-vorratsdatenspeicherung/*
22 *https://www.eco.de/presse/nach-kabinettsbeschluss-eco-verband-der-internetwirtschaft-e-v-sieht-erhebliche-risiken-bei-ip-speicherung/*
23 *https://von-notz.de/2026/04/22/anlasslose-datenspeicherung-groko-lernt-aus-ihren-fehlern-nicht/*
24 *https://netzpolitik.org/author/andre/*
25 *https://cdn.netzpolitik.org/wp-upload/2026/03/Satzung_netzpolitikorg_eV.pdf*
26 *https://freiheitsrechte.org/*
27 *https://digitalegesellschaft.de/*
28 *https://ccc.de/*
29 *https://edri.org/*
30 *https://cdt.org/eu/*
31 *mailto:andre@netzpolitik.org*
32 *https://keys.openpgp.org/search?q=andre@netzpolitik.org*
33 *https://signal.me/#eu/2x2EVQTqh8r_fKHn7bCfKUo65239LYxNXcy-ZUeUVNlKfoYsVAk5LA60rfwRKd3KK*
34 *https://chaos.social/@andre_meister*
35 *https://bsky.app/profile/andre.netzpolitik.org*
36 *https://fragdenstaat.de/profil/a.meister/*

Martin Schwarzbeck

Koalitionsvertrag Baden-Württemberg: Kameras sollen prüfen, wer und wie brav du bist

7. Mai 2026 – *Grün-Schwarz will in Baden-Württemberg als erstem Bundesland doppelte KI-Videoüberwachung ausrollen: Kameras, die Menschen auf verdächtiges Verhalten überprüfen und sie gleichzeitig mit Gesichtserkennung analysieren. In Mannheim und zwei weiteren Städten soll das Pilotprojekt starten.*

Gestern haben Cem Özdemir und Manuel Hagel den grün-schwarzen Koalitionsvertrag[1] für Baden-Württemberg vorgestellt. Hier sollen demnach erstmals in Deutschland Kameras eingesetzt werden, die sowohl das Verhalten der Abgebildeten analysieren und bewerten, als auch deren Gesichter vermessen, um per Gesichtserkennung herauszufinden, ob sie von polizeilichem Interesse sind.

Die Verhaltenskontrolle wird bereits seit acht Jahren in Mannheim trainiert[2]. Das Modellprojekt soll nun räumlich ausgeweitet werden, auf zwei weitere, bislang ungenannte Städte. Auch der Umfang wird erweitert, denn zusätzlich zur Verhaltenserkennungs-Technologie sollen künftig auch Objekte und Gesichter von den Kameras erkannt werden.

Live-Gesichtserkennung läuft in Deutschland bislang nur in Frankfurt am Main[3] hinter öffentlichen Überwachungskameras. Die Software vermisst jedes Gesicht im Erfassungsbereich und schlägt Alarm, sobald es einem gesuchten Gesicht sehr ähnlich ist. Gesucht wird damit nach Terrorist*innen, nach vermissten

Menschen, nach Opfern von Entführung, Menschenhandel oder sexueller Ausbeutung. Analysiert und mit den Polizeidatenbanken abgeglichen wird aber jedes Gesicht, das die Kameras aufnehmen.

Zusätzlich zur Echtzeit-Fernidentifizierung wollen Grüne und CDU der Polizei in Baden-Württemberg auch die Suche nach bestimmten Gesichtern im Internet erlauben. Auf Bundesebene[4] gibt es aktuell ebenfalls Bestrebungen, das Tool einzuführen. Damit können Beamt*innen beispielsweise Menschen auf Social Media finden, etwa auf Bildern, die Vereine oder Arbeitgeber ins Netz stellen. Selbst auf Totalaufnahmen von Großveranstaltungen könnten Personen gefunden werden. Wenn die Verhaltensanalyse in einer der Pilotstädte eine Straftat detektiert, kann damit theoretisch auch die tatverdächtige Person retrograd identifiziert werden.

„Schonung der Grundrechte“

Für die Echtzeit-Fernidentifizierung und die Gesichtersuchmaschine muss die Koalition das Polizeigesetz von Baden-Württemberg ändern. Dabei hatte Grün-Schwarz das erst Ende vergangenen Jahres getan. Damals hatte die Landesregierung der Polizei Datenanalyse nach Palantir-Art erlaubt, die diese ohnehin schon lange betrieb[5]. Außerdem genehmigten die alten und neuen Koalitionspartner der Polizei auch das KI-Training mit den persönlichen Daten von Bürger*innen sowie die Weitergabe dieser an externe Stellen.

Nun soll also eine neue Polizeigesetznovelle kommen, die auch Echtzeit-Fernidentifizierung ermöglicht. Niedersachsen, Sachsen und Schleswig-Holstein sind ebenfalls daran, Gesetzesgrundlagen dafür einzuführen. Die Technologie ist in Sicherheitsbehörden ziemlich beliebt, genauso wie der Verhaltensscanner, der in Mannheim trainiert wird. Vergangenes Jahr hat ihn Hamburg übernommen, Berlin folgt wohl als nächstes, Hessen, Niedersachsen, Sachsen, Schleswig-Holstein und Thüringen haben bereits Rechtsgrundlagen dafür oder arbeiten daran.

Bislang hat sich noch niemand getraut, beide Technologien auf einmal einzusetzen. Die Datenschutzbedenken sind bei beiden allein schon sehr hoch[6]. In Baden-Württemberg gibt es nun aber scheinbar keine Scheu mehr. „KI-Videoschutz kann für mehr Sicherheit bei gleichzeitiger Schonung der Grundrechte sorgen“, schreiben Grüne und CDU in ihrem Koalitionsvertrag.

Dass es bei den drei Standorten bleibt, an denen die Koalition die multiple KI-Überwachung pilotieren will, ist vermutlich eher

Aktion gegen Videoüberwachung
Foto: Stefanie Loos, CC BY 2.0

unrealistisch. Bereits vor der Wahl hatten sich Özdemir und Hagel dazu bekannt, den Einsatz von Videoüberwachungskameras entgrenzen zu wollen[7]. Für den Einsatz soll keine erhöhte Kriminalitätsbelastung mehr nötig sein, die Kommunen sollen freihändig darüber entscheiden.

Referenz: https://netzpolitik.org/2026/koalitionsvertrag-baden-wuerttemberg-kameras-sollen-pruefen-wer-und-wie-brav-du-bist/

Anmerkungen

1 *https://www.gruene-bw.de/wp-content/uploads/2026/05/2026-2031_Koalitionsvertrag_GrueneBW_CDUBW.pdf*
2 *https://netzpolitik.org/2025/verhaltensscanner-im-mannheim-hier-wird-die-ueberwachung-getestet-die-so-viele-staedte-wollen/*
3 *https://netzpolitik.org/2026/rotlichtviertel-frankfurt-am-main-hier-analysiert-die-polizei-jedes-gesicht/*
4 *https://netzpolitik.org/2026/faq-das-ueberwachungspaket-der-bundesregierung/*
5 *https://netzpolitik.org/2025/automatisierte-datenanalyse-der-gruene-palantir-spagat/*
6 *https://netzpolitik.org/2026/polizeigesetz-schleswig-holstein-wie-aus-einem-dystopischen-science-fiction-film/*
7 *https://netzpolitik.org/2026/verhaltensscanner-und-palantir-was-das-wahlergebnis-in-baden-wuerttemberg-sicherheitspolitisch-bedeutet/*
8 *https://netzpolitik.org/author/martin-schwarzbeck/*
9 *mailto:martin.schwarzbeck@netzpolitik.org*
10 *https://keys.openpgp.org/search?q=martin.schwarzbeck@netzpolitik.org*
11 *https://kolektiva.social/@YoshiXYZ*

Martin Schwarzbeck

Martin Schwarzbeck[8] ist seit 2024 Redakteur bei *netzpolitik.org*. Er hat Soziologie studiert, als Journalist für zahlreiche Medien gearbeitet, von *ARD* bis *taz*, und war lange Redakteur bei Berliner Stadtmagazinen, wo er oft Digitalthemen aufgegriffen hat. Martin interessiert sich für Machtstrukturen und die Beziehungen zwischen Menschen und Staaten und Menschen und Konzernen. Ein Fokus dabei sind Techniken und Systeme der Überwachung.
Kontakt: E-Mail[9] (OpenPGP[10]), Mastodon[11], Signal: yoshi.42042

Einladung zur Mitgliederversammlung 2026

des Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF e. V.)

Wir laden fristgerecht und satzungsgemäß zur ordentlichen Mitgliederversammlung 2026 ein.

Sie findet am Sonntag, den 1. November 2026, 12:00 – 14:00 Uhr im Theater im Delphi, Gustav-Adolf-Straße 2, 13086 Berlin statt. Eine Möglichkeit, online teilzunehmen, wird angeboten; Details dazu werden auf der Konferenzwebsite und beim FIfF rechtzeitig bekannt gegeben.

Vorläufige Tagesordnung

1. Begrüßung, Feststellung der Beschlussfähigkeit und Festlegung der Protokollführung
2. Beschlussfassung über die Tagesordnung, Geschäftsordnung und Wahlordnung
3. Bericht des Vorstands einschließlich Kassenbericht
4. Bericht der Kassenprüfer
5. Diskussion der Berichte
6. Entlastung des Vorstands
7. Neuwahl der Kassenprüfer:innen
8. Diskussion über Ziele und Arbeit des FIfF, aktuelle Themen, Verabschiedung von Stellungnahmen, Berichte aus den Regionalgruppen
9. Anträge an die Mitgliederversammlung
   Anträge müssen schriftlich bis drei Wochen vor der Mitgliederversammlung bei der FIfF-Geschäftsstelle eingegangen sein
10. Verschiedenes
11. Genehmigung des Beschlussprotokolls

gez. Stefan Hügel
für den Vorstand und die Geschäftsstelle des FIfF

Wissenschaft und Frieden 2/2026

Friedensbewegung(en) heute – Reflexionen und Impulse

Friedensbewegungen gibt es überall auf der Welt – und viele stehen derzeit vor der Herausforderung, dass *Frieden* als Forderung so umstritten und vermeintlich *suspekt* ist wie schon lange nicht mehr. Zudem erscheint zumindest in Europa eine Fragmentierung der Bewegungen vielfach als Hemmnis der Mobilisierungsfähigkeit. Doch zeigt eine Vielzahl an Aktivitäten und Publikationen, dass Friedensbewegungen existieren und sich einmischen. Was also sind die Anliegen dieser Bewegungen heute, wie werden sie formuliert, vor welchen Herausforderungen stehen sie?

Die Bewegungen weltweit ähneln sich und sind doch in ihren Themen, ihren Anliegen, ihren Aktionsformen je nach Kontext sehr unterschiedlich. Protestbanner, Demonstrationen, die Verwendung von international leicht verständlichen Bildern, Gesten, Sprachen gehören zum geteilten Aktionsrepertoire der Bewegungsakteure. Dann aber wieder gibt es deutliche Differenzen: im Gewaltverständnis, in den Zielsetzungen, in der konkreten Betroffenheit von Gewaltverhältnissen. Was also verbindet diese Vielfalt an Bewegungen?

Ein Heft voller Anregungen und Reflexionen, Impulse und Ideen für eine Auseinandersetzung damit, was es heutzutage bedeuten kann, Friedensbewegung zu sein.

Mit Beiträgen von *Andreas Zumach*, *Luise von Scheliha*, *Anna Hauschild* und *Elisabeth Saar*, *Elena Smirnova* und weiteren.

Weitere Texte: *Benedikter* Trumps Iran-Krieg | *Baraki* Belutschistan | *Weller* Wert der Transdisziplinarität

Beilage: Dossier 103 – Land als Schlüssel zum Frieden: Zugang, Nutzung und Resilienz im Fokus.

W&F 2/26 | Mai | 72 Seiten | 15 € (druck) / 12 € (ePUB+PDF)

Dietrich Meyer-Ebrecht

„… es sind nicht mehr die Produktionsmittel,
die die Gesellschaft des 21. Jahrhunderts formen.
Es sind die Kommunikationsformen."
Adrian Kreye[1]

„This Is for Everyone"

Tim Berners-Lee und die Erfindung des World Wide Web – eine Autobiographie

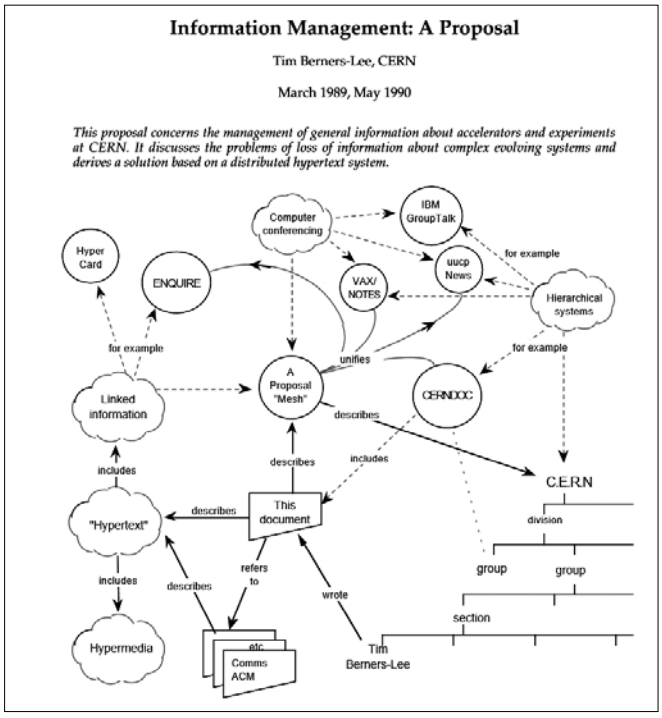
WWW, ein mittlerweile nur noch wenig benutztes Acronym – a *World Wide Web,* so nannte Tim Berners-Lee seine Vision eines weltumspannenden ‚Gewebes' aus Dokumenten, als er in den 1980er-Jahren begann, die Grundelemente für die Vernetzung von Dokumenten zu konzipieren. Seine Entwicklung öffnete das damals noch sehr junge und noch rudimentäre Internet einer breiten Öffentlichkeit. Es sollte allen Menschen über alle Kontinente hinweg ermöglichen, Information miteinander auszutauschen, frei und ohne Einschränkungen – *this is for everybody*, sein Credo. Damit machte Berners-Lee digitale Souveränität zur Prämisse für die Nutzung seines WWW – lange bevor dieser Begriff geprägt und ein Bewusstsein dafür geweckt worden war.

Berners-Lees 2025 erschienene Autobiographie ist zugleich seine Lebensgeschichte und die bis heute eng mit seinem Wirken verbundene Geschichte des World Wide Web, heute kurz das Web oder meist auch synonym das Internet. Eine Erfolgsgeschichte? Nicht nur. Berners-Lees Engagement um die Fortentwicklung seiner Vision eines offenen, unabhängigen Internets wird schon bald zu einem beständigen Ringen gegen Vereinnahmung und Missbrauch, gegen die Erosion der digitalen Souveränität …

Nicht ungewöhnlich war es in den frühen Jahren der Informatik, dass Physikerïnnen sich der Informatik verschrieben, so auch der 1955 geborene britische Physiker Tim Berners-Lee. Bereits in seiner Jungend begeistert er sich für Computer. Nach seinem Physikstudium war er in verschiedenen Software-Projekten tätig. Anfang der 1980er-Jahre fand Berners-Lee ‚seinen' Job im Computer-Center des CERN.

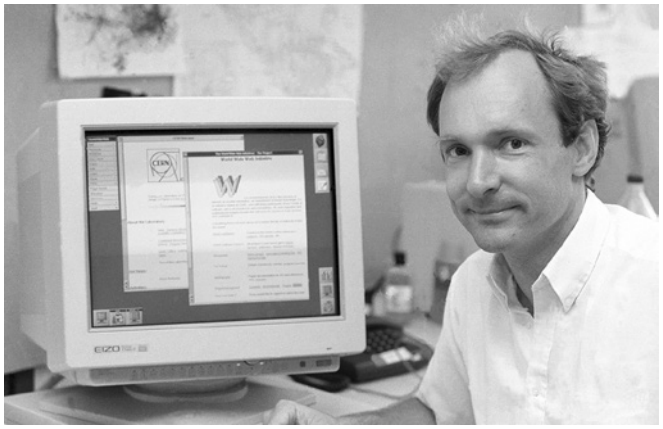
Anfang der 1980er-Jahre entwarf er auch bereits die ersten Visionen seines *world wide web*. Denn zu der Zeit arbeiteten die aus vielen unterschiedlichen Ländern stammenden Arbeitsgruppen im CERN jeweils mit ihren eigenen Computerausrüstungen und speicherten ihre Forschungsberichte, Memoranden, Versuchsdaten etc. auf ihren jeweils proprietären Medien. Ein enormer Arbeitsvorteil wäre es, so Berners-Lee, wenn man von jedem Computer aus auf jedes in einem anderen Computer gespeicherte Dokument zugreifen könnte. Und wenn alle Dokumente einheitlich codiert wären, so dass sie wiederum auf jedem anderen Computer lesbar wären. Und wenn man dann noch von jedem Dokument, von jedem Fragment in einem Dokument auf jedes andere verweisen könnte – „*… information was meaningless in isolation. What truely mattered was the relationship …*", schreibt Berners-Lee.

Die technischen Voraussetzungen für die Umsetzung dieser Wunschvorstellung waren gegeben. Für die Vernetzung von Computern waren standardisierte Hardware- und Software-Lösungen verfügbar, nachdem das damalige US-Verteidigungsministerium im März 1982 das Protokollsystem TCP/IP, entwickelt von Vinton Cerf und Robert Kahn in den 1970er-Jahren, zum Standard für die Vernetzung von Computern erklärt hatte. Mit den Netzwerkdiensten FTP, SMTP und Telnet konnte man bereits Dateien übertragen, E-Mails versenden und auf die Kommandozeilenoberfläche entfernter Computer zugreifen. Und dies nicht nur im Umfeld der eigenen Institution, denn zu dieser Zeit verband ein durch das US-amerikanische ARPAnet initiiertes Datennetz bereits weltweit die Rechenzentren vieler Universitäten und Forschungseinrichtungen. Zu dieser Zeit gewannen auch IBM-PC, Apple Macintosh und andere Kleinrechner rasch an Verbreitung. Modems ermöglichten die Datenübertragung via Telefonleitung. Ein *world wide web* in jedes Haus zu bringen, war technisch möglich.



Picture of World Wide Web proposal (March 1989, May 1990)
Quelle: CERN, CC BY 2.0

Eigentlich waren dazu nur noch zwei ‚kleine' Schritte nötig: Die Textverarbeitung musste so erweitert werden, dass sie Verweise in einem Text, die ‚Links', interpretieren konnte. Berners-Lee



Tim Berners-Lee am CERN, Quelle: CERN, CC BY 2.0

entwarf dafür, basierend auf dem in der Textverarbeitung etablierten Konzept der *mark-up languages*, die *Hypertext Mark-up Language* HTML. Und von einem erkannten Link musste der Zugriff auf das im entfernten Computer gespeicherte Dokument angestoßen werden. Dazu entwarf er ein spezielles Übertragungsprotokoll, das *Hypertext Transport Protocol* HTTP. Im Jahr 1989 gelang ihm endlich, seinen Arbeitgeber CERN von seinen Ideen zu überzeugen. Es kostete dann jedoch noch vier Jahre Entwicklung, bis Sprache und Protokoll ausgestaltet und Schreib- und Leseprogramme – Editor und Browser – prototypisch realisiert waren und dazu eine Betriebssystemergänzung entwickelt war, die aus einem Computer einen Webserver machte. Ein weiterer unverzichtbarer Baustein war der Entwurf einer Konvention für eine einheitliche und eindeutige Adressierung, später *Unified Recource Locator* URL genannt.

Zum Thema Editor und Browser muss noch gesagt werden, dass es ursprünglich Berners-Lees Vision war, alle miteinander zu vernetzenden Dokumente wie Forschungsberichte, Memoranden, Protokolle, Korrespondenz etc. von vornherein als HTML-Dateien zu erstellen. Eigene Inhalte sollten unmittelbar publiziert werden können entsprechend seinem Leitbild *„this is for everyone"*. Das war jedoch noch ein Schritt zu weit in die Zukunft. Es blieb zunächst bei, wie wir heute sagen, statischen Webseiten. Wieder aufgenommen wurden diese Idee in den frühen 2000er-Jahren mit den mittlerweile vielfältig eingesetzten Wikis.

Im August 1991 war ein erster Webserver für eine interne Demonstration implementiert. Am 12. April 1993 veröffentlichte Berners-Lee seine Entwicklung, nachdem er seinem Arbeitgeber den Verzicht auf Patentrechte abgerungen und die Freigabe zur Offenlegung erhalten hatte. Denn Berners-Lee war überzeugt, dass die lizenzfreie Anwendung zusammen mit einer quell-offenen Implementierung der grundlegenden Elemente die Voraussetzung für eine schnelle Verbreitung und einen uneingeschränkten Zugang sein würden – *this is for everyone …*

Schon wenig später musste Berners-Lee ein erstes Mal erleben, wie ihm die Steuerung der Entwicklung aus der Hand genommen wurde. Marc Andreessen, zu der Zeit Student an das University of Illinois, sperrte sich bei der Entwicklung eines neuen Browsers, dem *Mosaic*, gegen eine Abstimmung mit Berners-Lee. Zu offensichtlich war, dass Andreessen seinem Browser mit dem Einbringen proprietärer Sprachelemente ein Alleinstellungsmerkmal verschaffen wollte, um seine Vermarktung vorzubereiten. Die Web-Standards in den Händen gewinnorientierter Unternehmen – das genau kollidierte fundamental mit dem Anspruch auf vollständige Offenheit. Diese Erfahrung war einer der Anstöße, das *World Wide Web Consortium*, kurz W3C zu gründen, das ab Oktober 1994 unter Berners-Lees Leitung die technischen Spezifikationen der Web-Standards im Konsens seiner Mitglieder festlegt.

Ein knappes Jahr später kam die erste Kraftprobe auf das W3C zu, als Microsoft mit seinem Internet Explorer begann, proprietäre Sprachelemente einzuführen. Über mehrere Jahre spaltete Microsoft die Web-Szene mit seiner Marktmacht (Webseiten mussten, wenn diese speziellen IE-Eigenschaften genutzt werden sollten, in unterschiedlichen Versionen erstellt werden) und drohte, dem W3C die Hoheit über die Standardspezifikationen aus der Hand zu nehmen. Mitte der 2000er-Jahre brach interessanterweise zuerst der quell-offene, von der Mozilla Foundation herausgegebene *Firefox* Microsofts Monopolstellung. Die Mozilla Foundation erhielt alsbald einen Sitz im W3C. Denn die Förderung quell-offener Schlüsselkomponenten als Gegengewicht zu den kommerziellen Anbietern war – und ist – Berners-Lee ein besonderes Anliegen.

Monopolbildungen anderer Art konnte Berners-Lee und sein W3C nicht mehr verhindern. Sie betraf zuerst die Suchmaschinen. Einen ersten Ansatz machte die Plattform *Yahoo*, die 1994 zunächst mit einem hierarchischen Katalog startete, der später zu einer Suchmaschine weiterentwickelt wurde. Abgelöst wurde Yahoo alsbald von *Google*, gegründet im September 1998. Mit seinen neuartigen Suchalgorithmen konnten seine Gründer Sergei Brin und Larry Page Yahoo und anderen Plattformen schnell den Rang ablaufen. Verhaltensdaten war das Schlüsselwort, mit ihrer Hilfe konnten die Suchergebnisse nach ihrer wahrscheinlichen Relevanz für die anfragende Person gelistet werden.

Eine entscheidende Wende für Google kam, als Data-Analysten, einer von ihnen Amit Patel, Anfang 2002 auf die *predictive power* dieses mit jeder Suchanfrage wachsenden Datenschatzes aufmerksam wurden. Im selben Jahr holten sich Brin und Page unter dem Druck der Aktionäre und Investoren, die endlich Profit sehen wollten, den in der Unternehmensleitung erfahrenen Ingenieur und Informatiker Eric Schmidt als CEO. Im Anfang, so wollte es der Zufall, musste sich Schmidt ein Arbeitszimmer mit Patel teilen – und heraus kam Googles neues Geschäftsmodell: Profit erzielen mit den gesammelten Daten über das Nutzerverhalten, dem *behavioral surplus*.

Damit hatte das Web seine Unschuld verloren, das Web wurde zur Gelddruckmaschine, gefüttert von seinen Nutzerïnnen. Der Grundstein für den Datenkapitalismus war gelegt. Wie vielfältig und in welchem Umfang aus unseren Datenspuren Profit generiert wird, stellt die US-amerikanische Wirtschaftswissenschaftlerin Shoshana Zuboff in *The Age of Surveillance Capitalism* sehr umfassend dar[2]. Der Buchtitel lässt zugleich anklingen, wie das Web durch das Profit-getriebene ungebremste und perfektionierte Sammeln von Daten von uns und über uns in der Folge zu einem umfassenden Überwachungswerkzeug wird – in den Händen autoritärer Staaten, repressiver Regimes ein Werkzeug, umfassende Macht über ihre Bürgerïnnen auszuüben.

Das W3C – bis 2023 unter Berners-Lees Leitung – gewährleistet die Offenlegung der Web-Standards und Transparenz der Mechanismen. Dies ist die Voraussetzung, um Vorkehrungen gegen missbräuchlichen Datenabfluss aus den Computern der Benutzerïnnen zu schaffen. Mit den Social-Media-Plattformen haben sich die ‚big player' jedoch mittlerweile abgeschlossene Kommunikationsdomains geschaffen, die sich erfolgreich diesen Kontrollmöglichkeiten entziehen. Mit dem gleichen Effekt schotten sich kommerzielle Anbieter ab, wenn sie ihre Dienste von Web-Plattformen zunehmend auf proprietäre Apps umstellen, ein Beispiel die DB-App.

Berners-Lee widmet diesen Entwicklungen, die sein Ideal einer offenen Kommunikationswelt konterkarieren, wenig Raum. Als allerdings Edward Snowden 2013 enthüllt, mit welcher Perfidie und Akribie die NSA das Internet als ein weltumspannendes, alle vernetzten Computer erfassendes Spionagewerkzeug missbraucht, ist auch Berners-Lee alarmiert. In großer Empörung darüber fordert er im März 2014 eine *Bill of Rights* für das Internet. Heute, zwölf Jahre später, brauchten wir eine solche verbindliche Konvention noch viel dringender. Denn mittlerweile befinden sich die wesentlichen Ressourcen des Internets – Technologie, Produktion und Betrieb – in der Hand einiger weniger US-amerikanischer Unternehmen mit einer enormen Finanzmacht, erwirtschaftet zum Großteil aus einer schamlosen Ausbeutung unserer Daten. Und unkontrollierbar missbrauchen sie diese Machtfülle, um in Wirtschaft und Politik einzugreifen. „… es sind nicht mehr die Produktionsmittel, die die Gesellschaft des 21. Jahrhunderts formen. Es sind die Kommunikationsformen", schreibt Adrian Kreye in der SZ. „Und die sind nun mal fest in der Hand der USA, deren Präsident ein Meister ist, sie in Macht zu verwandeln."[1]

Statt gegen diese Entwicklungen auf aussichtsloser Position anzukämpfen, verfolgt Berners-Lee das Konzept eines gänzlich neuen Netzes. Eine durchgängig dezentrale Datenspeicherung soll seinen Benutzerïnnen die volle Souveränität über ihre Daten garantierten. Die Grundlagen dafür – u. a. Standards für eine dezentrale Speicherung und Verlinkung beliebiger Daten – entwickelt er in seinem Projekt *Solid*, das er seit 2006 verfolgt. In Pilotprojekten in Flandern und in Australien fand Solid bereits Anwendung, in den USA fand Berners-Lee einen Kooperationspartner für die Softwareentwicklung. Sehr fraglich ist jedoch, ob sich eine Erfolgsgeschichte wie die des WWW heute in einer vernetzten Welt, in der bereits alle Claims von mächtigen Interessengruppen abgesteckt sind, wiederholen lässt.

Für alle, die sich für die Geschichte des Internets interessieren, ist Berners-Lees Autobiographie auf jeden Fall lesenswert, und gut lesbar ist sie auch. Wer in den 1980ern seine ersten E-Mails an den Terminals der Mainframes schrieb und in den 1990ern seine ersten HTML-Seiten kodierte, wird die Zeit des Aufbruchs noch einmal nacherleben können. Die Geschichte des World Wide Web aus der Feder seines Schöpfers kann auch spannend zu lesen sein für die jüngeren Generationen, die mit dem Internet in Hand- oder Hosentaschen aufgewachsen sind. Vieles erfährt man über die funktionellen, organisatorischen, politischen Mechanismen, über maßgeblich an der Entwicklung und Verbreitung beteiligte Menschen, über die Machtkämpfe hinter den Kulissen, und vor allem, welch langer, mühsamer Weg zurückzulegen war von einer bestechenden Vision mit genialen Ideen für ihre Realisierung bis zur Ausreifung und weltweiten Ausbreitung. Berners-Lee würde sich damit heute vermutlich in die Schar der Tech-Milliardäre einreihen können. Aber Berners-Lee brannte für seine Vision, wichtiger als Profit war ihm – und ist ihm noch immer –, seine Vision zu den Menschen zu bringen, *this is for everybody*. Seine Geschichte sollte ein Maßstab sein.

In der Rückschau wird auch deutlich, welch eminente Rolle Berners-Lees Wirken – die „Hypertext"-Idee, das HTTP/HTML-Konzept, seine prototypischen Implementierungen und sein weltweites Agieren für die Verbreitung – für die Entwicklung des Internets gespielt hat. Der damit ermöglichte komfortable Zugang zu den verteilten Inhalten des Internets hat die Zahl der Nutzerïnnen rasant wachsen lassen, und dies wiederum hat die Entwicklung immer leistungsfähigerer und preisgünstigerer IT-Hardware enorm angekurbelt. Mehr Nutzerïnnen, mehr Dienste, datenintensivere Applikationen, das zusammen hat die Datenmengen, die im Internet bewegt werden, explosionsartig wachsen lassen. Die ökologischen Folgen dieser immer weiter anwachsenden Datenmengen – CO_2-Ausstoß infolge des Leistungsverbrauchs für Verarbeitung, Transport und Speicherung, Wasserverbrauch für die Kühlung der gigantischen *data center* – sind bereits zu einem ernsthaften, viel zu wenig beachteten Problem geworden.

Am Ende bleibt die Frage, *quo vadis* World Wide Web. Es ist weniger eine Frage als vielmehr ein Aufruf an die Akteure: Ihr habt eine gesellschaftliche Verantwortung, werdet euch dieser Verantwortung bewusst! Und ein Aufruf an uns, für ein Web zu werben, zu wirken, zu kämpfen, das uns weiterhin seinen so vielfältigen Nutzen bieten soll, ohne uns jedoch zu manipulieren und auszuspähen und ohne für kriminelle oder kriegerische Zwecke missbraucht zu werden – ein Web, das uns die digitale Souveränität wieder bringt. Denn, so schreibt der Science-Fiction-Autor Murray Leinster in seiner Kurzgeschichte *A Logic Named Joe*[3], in der er vor 80 Jahren die Utopie (oder Dystopie?) eines *world wide web* in einem verblüffenden Maße vorwegnimmt, „If we shut off logics [so nennt Leinster dieses web], we go back to a kind of civilization we have forgotten how to run!"

Tim Berners-Lee (2026)
This is for everyone. The Unfinished Story of the World Wide Web.
London: Macmillan;
in deutscher Übersetzung:
Tim Berners-Lee (2026)
This is for everyone. Die unvollendete Geschichte des World Wide Web.
Hamburg: Rowohlt-Verlag
384 Seiten
Preis 28,00 (Hardcover)
ISBN-13: 978-3498003814

Anmerkungen

1 *Andrian Kreye, SZ No.19, 24./25.01.2026*
2 *Shoshana Zuboff: The Age of Surveillance Capitalism, Profile Books Ltd, London, GB (2019)*
3 *Murray Leinster: A Logic Named Joe, (1946), https://www.baen.com/chapters/W200506/0743499107___2.htm*

30. Grundrechte-Report 2026 der Öffentlichkeit vorgestellt

*Am 21. Mai 2026 wurde der **Grundrechte-Report 2026 – Zur Lage der Bürger- und Menschenrechte in Deutschland** in der Stiftung Forum Recht in Karlsruhe der Öffentlichkeit vorgestellt.*

Die Jubiläumsausgabe des 30. Grundrechte-Reports behandelt die Gefährdung von Grund- und Menschenrechten im Jahr 2025. Im Angesicht zahlreicher nationaler und internationaler Krisen greifen staatliche Stellen „zu den Waffen": Zum einen bewaffnet sich der Staat durch Sondervermögen mit Rekordausgaben für Militär und durch eine Stärkung der Bundeswehr – und greift dabei in Grundrechte der Bürger:innen ein. Zum anderen weiten Bund und Länder ihre Überwachungs- und Eingriffsbefugnisse für Polizei, Geheimdienste und andere Behörden aus, von Staatstrojanern über Datenanalysen mit Palantirs **Gotham** bis zu biometrischen Abgleichen und automatischer Gesichtserkennung. Daneben verschärfen sich die Krisen für die Menschenrechte mit Blick auf den Wohnungsmangel, den Klimawandel, die Rechte von Geflüchteten und Menschen am Rande des Existenzminimums.

Der Report versteht sich als **alternativer Verfassungsschutzbericht** und bespricht Entscheidungen von Parlamenten, Behörden und Gerichten, aber auch von Privatunternehmen. Er wird von zehn Bürgerrechtsorganisationen herausgegeben.

Herta Däubler-Gmelin, Rechtsanwältin, frühere Bundesministerin der Justiz und langjährige Bundestagsabgeordnete, präsentierte den Grundrechte-Report. Sie hob die aktuell immense Bedeutung des Grundrechtsschutzes hervor: *„In unserer Zeit ist Sorge um die Wirksamkeit der Grund- und Menschenrechte besonders geboten. Nicht allein wegen der Aggressionskriege, Konflikte und immer noch zunehmenden autoritären Tendenzen, sondern auch, weil globale – technische – Standards, z. B. in KI-Systemen, trotz ihrer Nützlichkeit und Bequemlichkeit immer häufiger unsere Freiheitsrechte einengen – oder auch die Mitbestimmungsrechte von Arbeitnehmerinnen und Arbeitnehmern gefährden."*

Leo D'Andola, Schüler, berichtete über die Schulstreiks gegen die Wehrpflicht: *„Oft redet die Bundesregierung, wenn sie beispielsweise über das Wehrdienstmodernisierungsgesetz spricht, über Sicherheit. Aber wir Jugendliche fühlen uns nicht sicher – nicht, wenn wir einen Fragebogen bekommen, den wir für die Bundeswehr ausfüllen müssen; nicht, wenn wir der Bundesregierung mitteilen müssen, wenn wir für längere Zeit ins Ausland gehen; und nicht, wenn wir über die kommenden Maßnahmen nachdenken – über Musterung, Sammlung unserer persönlichen Daten und die mögliche Wiedereinführung der Wehrpflicht."*

Ahmad Mosamem Rahimi, der vor den Taliban fliehen musste, berichtete über den Umgang der Bundesregierung mit ihm und anderen Afghan:innen, denen Deutschland Schutz zugesagt hatte: *„Obwohl ich alle meine Unterlagen hatte und mir versprochen worden war, dass ich nach Deutschland kommen dürfe, wartete ich in Pakistan fast zwei Jahre lang auf mein Visum. Während dieser Zeit wusste ich nicht, ob und wann ich nach Deutschland einreisen könnte oder ob die pakistanische Polizei mich nach Afghanistan zurückschicken würde, wo ich der Verfolgung durch die Taliban ausgesetzt wäre. Während dieser ganzen Zeit musste ich Ausbeutung, Misshandlung und einen tiefen Mangel an Respekt erdulden."*

Athena Möller, Jura-Studentin und Vorstandsmitglied der Internationalen Liga für Menschenrechte, führte für die Redaktion durch die Veranstaltung. Sie stellte fest: *„Es ist zunehmend anmaßend, von der Bevölkerung und insbesondere der jüngeren Generation Loyalität gegenüber dem deutschen Staat zu erwarten, während dieser ihre Grundrechte nicht ausreichend wahrt. Obwohl die Grundrechte 2025 besorgniserregend oft und intensiv verletzt wurden, scheinen Politik und Staatsapparat diesbezüglich kaum Konsequenzen tragen zu müssen. Der Grundrechte-Report nimmt sie in die Pflicht und stellt klar, welche Vorgehensweisen aus welchen Gründen zu beanstanden und zu verurteilen sind."*

Grundrechte-Report 2026 – Zur Lage der Bürger- und Menschenrechte in Deutschland. Herausgegeben von: Peter von Auer, Nina Diarra, Franziska Görlitz, Rolf Gössner, Max Putzer, Rainer Rehak, Theresa Tschenker, Lea Welsch, Rosemarie Will, Michèle Winkler
Fischer Taschenbuch Verlag, Frankfurt/M 2026,
ISBN: 978-3-596-71370-7,
240 Seiten, 15,00 Euro.
E-Book 9,99 Euro

*Der Grundrechte-Report 2026 ist ein gemeinsames Projekt von: Humanistische Union, vereinigt mit der Gustav-Heinemann-Initiative • Bundesarbeitskreis Kritischer Juragruppen • Internationale Liga für Menschenrechte • Komitee für Grundrechte und Demokratie • Neue Richter*innenvereinigung • PRO ASYL • Republikanischer Anwältinnen-und Anwälteverein • Vereinigung Demokratischer Jurist:innen • Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung • Gesellschaft für Freiheitsrechte e. V.*

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung

Wir sind ...

... etwa 700 engagierte Menschen aus Wissenschaft und Praxis. Wir sind Fachleute der Informatik und Informationstechnik. Wir denken bei unserer Arbeit auch über deren Konsequenzen nach. Wir wissen, dass nicht alle Probleme technisch lösbar sind. Wir heißen alle willkommen, die Informationstechnik verwenden und sich Gedanken über deren gesellschaftlichen Auswirkungen machen.

Allen, die sich mit Informatik und Informationstechnik beschäftigen – in der Ausbildung, im Beruf oder danach, in Wissenschaft und Praxis – wollen wir ein Forum für eine kritische und lebendige Auseinandersetzung bieten – offen für alle, die mitarbeiten möchten oder auch einfach nur informiert bleiben wollen.

Unsere Arbeit wird vom FIfF-Vorstand koordiniert – unterstützt durch die FIfF-Geschäftsstelle. In wissenschaftlichen Fragen unterstützt uns der Beirat des FIfF. Wir kooperieren mit vielen in- und ausländischen Initiativen und Organisationen.

FIfF online

Website: Aktuelles, Regionalgruppen, Publikationen, Aktivitäten, Texte und Themen
https://www.fiff.de

Mitmachen:
https://www.fiff.de/mitmachen

Regionalgruppen:
https://www.fiff.de/regionalgruppen

Videos und Vorträge:
https://video.fiffkon.de

Social Media:
Mastodon: *https://mastodon.bits-und-baeume.org/@fiff_de*

Mitglieder-Wiki und IT-Handbuch:
https://www.fiff.de

FIfF-Mailinglisten

Überblick: *https://www.fiff.de/mailinglisten*

Allgemeine FIfF-Mailingliste:
Anmeldung per Mail: *fiff-l-subscribe@lists.fiff.de*

Newsletter (etwa alle drei Monate):
Anmeldung per Mail: *newsletter-subscribe@lists.fiff.de*

Presseverteiler:
Anmeldung per Mail: *presse-subscribe@lists.fiff.de*

FIfF-Beirat

Ute Bernhardt (Berlin); **Dagmar Boedicker** (München); Dr. **Phillip W. Brunst** (Köln); Prof. Dr. **Christina B. Class** (Jena); Prof. Dr. **Wolfgang Coy** (Berlin); Prof. Dr. **Wolfgang Däubler** (Bremen); Prof. Dr. **Christiane Floyd** (Berlin); Prof. Dr. **Klaus Fuchs-Kittowski** (Berlin); Prof. Dr. **Michael Grütz** (München); Prof. Dr. **Thomas Herrmann** (Bochum); Prof. Dr. **Wolfgang Hesse** (München); Prof. Dr. **Eva Hornecker** (Weimar); **Werner Hülsmann** (München); **Ulrich Klotz** (Frankfurt am Main); Prof. Dr. **Klaus Köhler** (Mannheim); Prof. Dr. **Jochen Koubek** (Bayreuth); Dr. **Constanze Kurz** (Berlin); Prof. Dr**. Klaus-Peter Löhr (†)**; Prof. Dr. **Dietrich Meyer-Ebrecht** (Aachen); **Werner Mühlmann** (Calau); Prof. Dr. **Arno Rolf** (Hamburg); Prof. Dr. **Alexander Rossnagel** (Kassel); **Ingo Ruhmann** (Berlin); Prof. Dr. **Gerhard Sagerer** (Bielefeld); Prof. Dr. **Gabriele Schade** (Erfurt); **Ralf E. Streibl** (Bremen); Prof. Dr. **Marie-Theres Tinnefeld** (München); Prof. Dr. **Eberhard Zehendner** (Jena)

FIfF-Vorstand

Stefan Hügel (Vorsitzender) – Frankfurt am Main
Dr. **Rainer Rehak** (stellv. Vorsitzender) – Berlin
Michael Ahlmann – Kiel / Blumenthal
Gilbert Assaf – Berlin
Prof. Dr. **Wolfgang Hofkirchner** – Wien
Sylvia Johnigk – München
Siobhan Kraus – Münster
Prof. Dr. **Hans-Jörg Kreowski** – Bremen
Kai Nothdurft – München
Dr. **Friedrich Strauß** – München
Margita Zallmann – Bremen

FIfF-Geschäftsstelle

Ingrid Schlagheck (Geschäftsführung) – Bremen

Impressum

Herausgeber	Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V. (FIfF)
Verlagsadresse	FIfF-Geschäftsstelle Goetheplatz 4 D-28203 Bremen Tel. (0421) 33 65 92 55 *fiff@fiff.de*
Erscheinungsweise	vierteljährlich
Erscheinungsort	Bremen
ISSN	0938-3476
Auflage	1.200 Stück
Heftpreis	7 Euro. Der Bezugspreis für die FIfF-Kommunikation ist für FIfF-Mitglieder im Mitgliedsbeitrag enthalten. Nichtmitglieder können die FIfF-Kommunikation für 28 Euro pro Jahr (inkl. Versand) abonnieren.
Hauptredaktion	Dagmar Boedicker, Stefan Hügel (Koordination), Sylvia Johnigk, Hans-Jörg Kreowski, Ingrid Schlagheck
Schwerpunktredaktion	Ulrike Erb, Karin Vosseberg
V.i.S.d.P.	Stefan Hügel
Retrospektive	Beiträge für diese Rubrik bitte per E-Mail an *redaktion@fiff.de*
Lesen, SchlussFIfF	Beiträge für diese Rubriken bitte per E-Mail an *redaktion@fiff.de*
Layout	Berthold Schroeder, München
Cover	Karin Vosseberg
Druck	BerlinDruck GmbH + Co. KG, 28832 Achim Heftinhalt auf 100 % Altpapier gedruckt.

Verpackung mit finanziellem Klimabeitrag
ClimatePartner.com/11242-2606-1002

Die FIfF-Kommunikation ist die Zeitschrift des „Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V." (FIfF). Die Beiträge sollen die Diskussionen unter Fachleuten anregen und die interessierte Öffentlichkeit informieren. Namentlich gekennzeichnete Artikel geben die jeweilige Autor:innen-Meinung wieder.

Die FIfF-Kommunikation ist das Organ des FIfF und den politischen Zielen und Werten des FIfF verpflichtet. Die Redaktion behält sich vor, in Ausnahmefällen Beiträge abzulehnen.

Nachdruckgenehmigung wird nach Rücksprache mit der Redaktion in der Regel gern erteilt. Voraussetzung hierfür sind die Quellenangabe und die Zusendung von zwei Belegexemplaren. Für unverlangt eingesandte Artikel übernimmt die Redaktion keine Haftung.

Wichtiger Hinweis: Wir bitten alle Mitglieder und Abonnent:innen, Adressänderungen dem FIfF-Büro möglichst umgehend mitzuteilen.

Aktuelle Ankündigungen

FIfF-Konferenz 2026: 30.10. bis 1.11.2026
im Theater im Delphi, Gustav-Adolf-Straße 2, 13086 Berlin
Keine Panik! Resilienz in der Polykrise

FIfF-Mitgliederversammlung 2026
im Theater im Delphi, Gustav-Adolf-Straße 2, 13086 Berlin
Sonntag, 1. November 2026, 12:00 – 14:00 Uhr

FIfF-Kommunikation

3/2026 Künstliche Intelligenz und digitale Medien in der Bildung
Margita Zallmann, Bernard Robben
Redaktionsschluss: 7. August 2026

Zuletzt erschienen:

2/2025 Informatik und Gesellschaft
3/2025 KI, Arbeit, Bildung, Frieden
4/2025 Big Tech und drumherum – Die Gier nach Macht und Geld
1/2026 FIfF-Konferenz 2025: Digitaler Humanismus für eine techno-öko-soziale Transformation der Weltgesellschaft

W&F – Wissenschaft & Frieden

3/25 Ära der Aufrüstung
4/25 Autoritäre Wende
1/26 See der Inseln / Ozeanien
2/26 Friedensbewegung(en) heute – Reflexionen und Impulse

vorgänge – Zeitschrift für Bürgerrechte und Gesellschaftspolitik

#252 Demokratisierung
#253 Einengung der Diskursräume
#254 Menschenrechte in Lieferketten
#255 Wohnungslosigkeit

DANA – Datenschutz-Nachrichten

2/25 Social Media
3/25 Datenschutz in der Roulette-Koalition
4/25 Das Internet der Dinge
1/26 Biometrie

Das FIfF-Büro

Geschäftsstelle FIfF e. V.
Ingrid Schlagheck (Geschäftsführung)
Goetheplatz 4, D-28203 Bremen
Tel.: (0421) 33 65 92 55
E-Mail: fiff@fiff.de
Die Bürozeiten finden Sie unter *www.fiff.de*

Bankverbindung
Bank für Sozialwirtschaft (BFS) Köln
Spendenkonto:
IBAN: DE79 3702 0500 0001 3828 03
BIC: BFSWDE33XXX

Kontakt zur Redaktion der FIfF-Kommunikation:
redaktion@fiff.de
PGP-Key: *https://www.fiff.de/pgp*

Schluss FIfF

„Als zum erstenmal das Wort ‚Friede‘ ausgesprochen wurde, entstand auf der Börse eine Panik. Sie schrien auf im Schmerz: Wir haben verdient! Lasst uns den Krieg! Wir haben den Krieg verdient“

Karl Kraus (1874–1936)

Geeignete Texte für den SchlussFIfF bitte mit Quellenangabe an *redaktion@fiff.de* senden.