GESELLSCHAFT
FÜR INFORMATIK

ARBEITSPAPIER

SCHLÜSSELASPEKTE DIGITALER SOUVERÄNITÄT

MAI 2020

WWW.GI.DE

INHALTSVERZEICHNIS

VORWORT

Digitale Souveränität ist innerhalb der letzten Jahre zu einem der zentralen Begriffe in der Digitalpolitik geworden. Es wird zunehmend klar, dass es für verschiedene Stakeholder entscheidend ist, digital souverän entscheiden und handeln zu können. Es geht um den Staat und um Behörden, um Unternehmen und Bürger*innen. Wir sprechen über die Souveränität von Infrastruktur, Daten, Algorithmen, Hardware, Software, Bildung – letztlich geht es um die Unabhängigkeit und Selbstbestimmtheit unserer Gesellschaft.

Es ist ein Kernziel der Gesellschaft für Informatik e.V. (GI) und die Verantwortung von uns Informatiker*innen, in der Debatte um digitale Souveränität fundierte und präzise Beiträge zu leisten. Wir sind als Fachgesellschaft thematisch breit aufgestellt und unsere 20.000 Mitglieder in 14 Fachbereichen haben Expertise zu vielen zentralen Fragestellungen digitaler Souveränität. Mit unseren Projekten leisten wir gemeinsam mit Partnern aus der Wissenschaft, Wirtschaft und Zivilgesellschaft kontinuierliche Arbeit und möchten einen Beitrag zur Versachlichung des Themas leisten. Besonders hervorheben möchte ich hier das Kompetenzzentrum Digitale Souveränität, das wir mit Unterstützung des Bundesministeriums für Bildung und Forschung in den kommenden Jahren aufbauen werden.

Wir freuen uns auf die Aufgabe, den Themenkomplex digitale Souveränität kontinuierlich zu begleiten. Das Fachgespräch des GI-Wirtschaftsbeirats „Schlüssel digitaler Souveränität“, welches im Februar 2020 in Berlin stattfand, war für die Gesellschaft für Informatik ein Startpunkt in diesem Diskussionsprozess. Die Referent*innen lassen uns in der vorliegenden Publikation nun auch verschriftlicht an ihrer Expertise zu digitaler Bildung, wirtschaftlicher Entwicklung und politischer Zusammenarbeit für mehr digitale Souveränität teilhaben. Ich danke allen Expert*innen für ihre Beiträge und hoffe, Sie, liebe Leser*innen, finden darin spannende Denk- und Diskussionsanstöße!

Viel Spaß bei der Lektüre und spannende Einsichten,

Ihr Hannes Federrath

EDITORIAL

DIMENSIONEN DIGITALER SOUVERÄNITÄT – EIN ÜBERBLICK

Daniel Krupka, Gesellschaft für Informatik

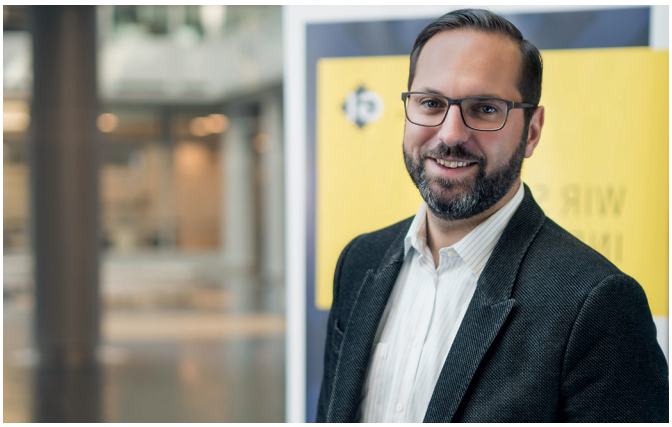
Die Begrifflichkeit der „digitalen Souveränität“ hat sich in den letzten Jahren zu einem zentralen Motiv in politischen Debatten zur Digitalisierung entwickelt. Autoritäre und semi-autoritäre Länder wie China und Russland streben schon lange nach mehr Souveränität im digitalen Raum und spätestens seit den Snowden-Enthüllungen in Jahr 2013 wollen auch die Europäische Kommission und europäische Regierungen die digitale Souveränität der einzelnen Länder bzw. ihrer Wirtschaft und Bürger*innen stärken.[1]

Für das Kompetenzzentrum Öffentliche IT ist digitale Souveränität „die Summe aller Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können.“[2] Die Fokusgruppe „Digitale Souveränität in einer vernetzten Wirtschaft“ des Digital-Gipfels hat diese Sichtweise um die staatliche Dimension erweitert. Demnach ist Digitale Souveränität unverzichtbare Voraussetzung für unabhängiges staatliches und wirtschaftliches Handeln.[3] Unter digitaler Souveränität wird also das selbstbestimmte Handeln und Entscheiden von (1) Individuen, (2) Unternehmen und anderen Institutionen sowie (3) von ganzen Staaten oder transnationalen Institutionen wie der Europäischen Union im digitalen Raum verstanden.

Diese Publikation soll einige Aspekte digitaler Souveränität näher beleuchten. Bei dem Versuch der Strukturierung der Diskussion und der Argumente hilft die Unterscheidung von vier Dimensionen, die diesen weitreichenden und mitunter etwas diffus angewendeten Begriff der digitalen Souveränität[4] ausfüllen: (1) Kompetenzen, (2) Daten, (3) Software- und Hardware-Technologien sowie (4) Governance-Systeme.

(1) Stärkung der individuellen digitalen Kompetenzen

Ausgangspunkt und eines der zentralen Argumente zur Förderung einer digitalen Souveränität ist das Individuum und dessen Kenntnisse im Umgang und Verständnis für digitale Technologien. Mit der Charta Digitale Bildung[5] werben wir als



Daniel Krupka © GI

Gesellschaft für Informatik für ein ganzheitliches Verständnis digitaler Bildung. Jede Person soll die Phänomene, Gegenstände und Prozesse der durch Digitalisierung geprägten Welt sowohl aus gesellschaftlich-kultureller Perspektive („Wie wirkt das?“), aus anwendungsbezogener Perspektive („Wie nutze ich das?“) sowie insbesondere auch aus technologisch-informatischer Perspektive („Wie funktioniert das?“) systematisch reflektieren, ergründen und gestalten können.

Aus Sicht der Gesellschaft für Informatik ist das im Wesentlichen dadurch zu erreichen, indem der informatischen Bildung – insbesondere dem Fach Informatik – in der Schule mehr Platz eingeräumt wird, um das vielbeschworene algorithmische Denken („computational thinking“) schon früh zu vermitteln. Während die technische Perspektive beispielsweise durch flächendeckenden Informatik-Unterricht adressiert werden kann, existieren auch für Herausbildung von Anwendungsfähigkeiten Werkzeuge wie das „International Certificate for Digitale Literacy“ (ICDL), das einen internationalen Standard im Bereich der IT-Skills darstellt.

---

1 *Pohle, Julia (2020): Digitale Souveränität. In: Klenk T., Nullmeier F., Wewer G. (eds) Handbuch Digitalisierung in Staat und Verwaltung. Springer VS, Wiesbaden*

2 *Goldacker, Gabriele (2017): Digitale Souveränität, Kompetenzzentrum Öffentliche IT (ÖFIT), https://www.oeffentliche-it.de/documents/10181/14412/Digitale+Souveränität*

3 *Digital-Gipfel, Fokusgruppe „Digitale Souveränität“ (2019): Digitale Souveränität im Kontext plattformbasierter Ökosysteme, https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2019/p2-digitale-souveraenitaet-plattformbasierter-oekosysteme.pdf?__blob=publicationFile&v=4*

4 *Diese Strukturierung ist angelehnt an die drei Handlungsfeldern Kompetenzen, Technologie und Regulierung aus dem Gutachten „Digitale Souveränität“ des Sachverständigenrat für Verbraucherfragen (https://www.svr-verbraucherfragen.de/wp-content/uploads/Gutachten_Digitale_Souveränität_.pdf) sowie den acht Kategorien digitaler Souveränität der Fokusgruppe „Digitale Souveränität“ der Plattform „Innovative Digitalisierung der Wirtschaft“ des Digitalgipfels.*

5 *www.charta-digitale-bildung.de*

In dieser Publikation gehen insbesondere *Tankred Schipanski, Manuel Höferlin* und *Jens Zimmermann* in ihren Beiträgen auf die Bildungsaspekte in der Diskussion um die digitale Souveränität ein.

(2) Datensouveränität und Souveränität im Umgang mit Daten

Dieser zweite Aspekt rückt angesichts der zunehmenden Wirkkraft von Technologien der Künstlichen Intelligenz und insbesondere maschineller Lernverfahren in den Fokus. Die Bundesregierung hat im November 2019 die Eckpunkte einer Datenstrategie veröffentlicht und vier Handlungsfelder identifiziert. So soll erstens die Datenbereitstellung verbessert und der Datenzugang gesichert werden, zweitens soll die verantwortungsvolle Datennutzung befördert und Innovationpotenziale gehoben werden, drittens soll die Datenkompetenz erhöht und eine Datenkultur etabliert werden und viertens soll der Staat zum Vorreiter in diesem Bereich werden.[6]

Nach dem Papier des Digital-Gipfel ist Datensouveränität gewährleistet, „wenn die Verfügungs- und Nutzungsrechte an Daten, das heißt der Zugriff, der Transfer, die Verarbeitung und die Analyse auf jeder Wertschöpfungsebene ein selbstbestimmtes Handeln gewährleisten. Dies schließt etwa die Möglichkeit ein, auf vertraglicher Grundlage Dritte vom Zugriff auf Daten ein- oder auszuschließen, die Verknüpfung unterschiedlicher Daten sowie die Verarbeitung und Analyse von Daten zu ermöglichen oder zu unterbinden."

Eng verbunden sind auch diese Aspekte mit dem ersten Punkt und der Herausbildung der Kompetenzen im Umgang mit Daten, sowohl in Form grundlegende Kompetenzen in Form einer Data Literacy[7] als auch im Aufbau von Data-Science-Kompetenzen. Hier sind insbesondere die Hochschulen und Universitäten gefragt.[8] Die Gesellschaft für Informatik hat im Dezember 2019 ein Arbeitspapier zur Ausgestaltung von Studiengängen sowie von Aus- und Weiterbildungsangeboten im Bereich Data Science veröffentlicht.[9]

In dieser Publikation geht insbesondere *Karl Steinacker* in seinem Beitrag auf den Datenaspekt in ein und plädiert für ein Recht auf individuelle Datenkonten, um Datenhoheit, Interoperabilität und Portabilität zu gewährleisten. Thomas Bendig plädiert dafür verteilte und von zentralen Instanzen unabhängige Datenhaltung und die freie Nutzung selbst generierter Daten zu fördern. Dadurch würden Markteintrittsbarrieren gesenkt, Innovationspotentiale gesichert und die bei digitalen Plattformen verbreitete „Winner-takes-it-all"-Effekte gemindert. Insbesondere würden so eher mittelständisch geprägte, von Wettbewerb und Innovation bestimmte Wirtschaftssysteme gefördert, ohne dass sie die großen, mit Plattformen verbundenen Chancen, in Bezug etwa auf Wachstum und Schaffung neuer Märkte und Technologien einschränken.

(3) Digitale Souveränität braucht technologische Souveränität in den Bereichen Software, Hardware und Architekturen

Eng mit dem Aspekt der Datensouveränität verknüpft ist die Frage nach technologischer Souveränität im Software- und im Hardware-Bereich. Im Zentrum nahezu aller digitalen Innovationen steht heute Software. „Software eats the world" heißt es nicht erst, seit insbesondere die maschinellen Lernverfahren der sogenannten künstlichen Intelligenz zu neuer Popularität verholfen haben. Digitale Souveränität wird Deutschland und Europa nur mit einer signifikanten Stärkung des Software-Standorts gelingen. Davon ist der Wirtschaftsbeirat der GI überzeugt.[10]

Digitale Souveränität bedeutet auch, bei den benötigen Hard- und Softwarekomponenten mehrere Lösungen mit ähnlicher Leistungsfähigkeit zur Auswahl zu haben. Sie müssen von bekannten, vertrauenswürdigen Instanzen bereitgestellt werden und durch vollständige Dokumentation die Transparenz und Nachvollziehbarkeit der enthaltenen Funktionen sowie der zugrundeliegenden Technologien ermöglichen. Dabei erhöhen Open-Source-Angebote, bei denen der Quellcode eingesehen und genutzt werden kann, konkrete Architektur- und Schnittstellenbeschreibungen sowie die

---

6 https://www.bundesregierung.de/resource/blob/997532/1693626/e617eb58f3464ed13b8ded65c7d3d5a1/2019-11-18-pdf-datenstrategie-data.pdf

7 Data Literacy ist die Fähigkeit des planvollen Umgangs mit Daten. In Ergänzung zu spezialisierten Fachkräften – den Data Scientists – liegt der Fokus auf der bedarfsgerechten, Disziplinen übergreifendem Know-how, um datengestützt arbeiten und entscheiden können.

8 https://gi.de/fileadmin/GI/Hauptseite/Aktuelles/Aktionen/Data_Literacy/GI_DataScience_2018-04-20_FINAL.pdf

9 Gesellschaft für Informatik (2019): Data Science: Lern- und Ausbildungsinhalte, https://gi.de/fileadmin/GI/Allgemein/PDF/GI_Arbeitspapier_Data-Science_2019-12_01.pdf

10 Gesellschaft für Informatik (2020): Positionspapier: Den Software-Standort Deutschland stärken, https://gi.de/fileadmin/GI/Allgemein/PDF/2020_10_02_GI_Positionspapier_Softwarestandort.pdf

Nutzung von etablierten und offenen Standards in der Regel die digitale Souveränität.

Dass Software-Anwendungen auch zu einer Stärkung der digitalen Souveränität auf der Ebene der Individuen und der Unternehmen sein können, zeigt der Beitrag von *Elisabeth Schauermann* und *Nikolas Becker*, der ein Projekt vorstellt, in dem die GI mit einer Reihe an Forschungspartnerinnen erarbeiten wird, welches Potenzial interaktive Datenschutzlösungen zur Steigerung der Souveränität von Smart-Wearables-Nutzerinnen haben. Besonders im Umgang mit sensiblen, persönlichen Gesundheitsdaten sollen Lösungen für informierte und reflektierte Nutzungsentscheidungen entwickelt und bereitstellt werden.
Ein weiteres Beispiel stellen *Bernhard Waltl* und *Georg Schmidt*, die mit Unterstützung der Klaus-Tschira-Stiftung eine Software für die Erstellung laienverständlicher Unterlagen zur informierten Einwilligung im Rahmen wissenschaftlicher Studien entwickeln und so die Souveränität von Patient*innen bzw. Proband*innen mit Hilfe digitaler Werkzeuge stärken.

In einer Ende Januar 2020 veröffentlichten Studie knüpft der VDE den Erhalt und den Ausbau der technologischen Souveränität des Standortes eng an die Frage, ob es gelingt führend in den Technologiefeldern und Fachdisziplinen Innovationsführer zu bleiben oder zu werden: Informations- und Kommunikationstechnik (IKT), Künstliche Intelligenz und Mikroelektronik mit der für die für den flächendeckenden Ausbau der Breitbandinfrastrukturen so wichtigen 5G-Technologie.

In der IKT bedarf es demnach „einer ausgeprägten Befähigung zu souveränem Handeln, indem wir selbst über das technische Detailwissen verfügen, international relevante Forschung betreiben sowie eigene Infrastrukturen konzipieren, aufbauen und nutzen können. Da wir in der IKT die Komponenten überwiegend von internationalen Herstellern beziehen, müssen wir in der Lage sein, deren Vertrauenswürdigkeit selbst zu validieren und die Infrastrukturen umfassend selbst zu betreiben und zu warten.“[11]

Die Diskussion um die Abhängigkeit von außereuropäischen Anbietern insbesondere beim Aufbau der 5G-Infrastrukturen ist auch in diesem Papier sehr präsent: *Jörg Bienert* betont die Gefahr von Lock-In-Effekten von Anwendern bei großen Cloud-Service-Anbietern. *Jens Zimmerman* betont, dass insbesondere Anbieter aus autoritären Ländern ein Sicherheitsproblem darstellen. Deshalb umfasse digitale Souveränität auch die Souveränität über die europäische digitale Infrastruktur.

Zum Erhalt der digitalen Souveränität ist der Aufbau einer europäischen Cloud-Infrastruktur erforderlich. Das betont *Jörg Bienert* in seinem Beitrag. Dabei gehe es nicht um einen Gegenentwurf zu den proprietären Standards internationaler Hyperscaler, sondern darum, zusätzliche, bessere Alternativen („Föderierte Multi-Cloud-Lösungen“) und einen europäischen Hyperscaler auf Basis europäischer Sicherheits- und Wertestandards. Er verweist dabei auf Gaia-X als eine mit großen Hoffnungen verbundene Initiative.
Ziel von Gaia-X sei es, „gemeinsam mit weiteren europäischen Ländern für Europa, seine Staaten, seine Unternehmen und seine Bürgerinnen und Bürger die nächste Generation einer vernetzten Dateninfrastruktur zu schaffen, die den höchsten Ansprüchen an digitale Souveränität genügt und Innovationen fördert.“[12]

Insbesondere die Leitprinzipien, die sich an den europäischen Werten orientieren, sind ein vielversprechender Ansatz. Europäischer Datenschutz, Offenheit und Transparenz, Authentizität und Vertrauen, Souveränität und Selbstbestimmtheit, freier Marktzugang und europäische Wertschöpfung, Modularität und Interoperabilität und Nutzerfreundlichkeit sind wichtige Prinzipien zur Wahrung einer digitalen Souveränität.

Eine wichtige Komponente, die derzeit in der Diskussion um Gaia-X noch etwas zu kurz kommt, ist der Zugang insbesondere für kleine und mittlere Unternehmen – das Rückgrat der deutschen und der europäischen Wirtschaft. Aufbauend auf der dezentralen Plattforminfrastruktur Gaia-X wäre es sinnvoll insbesondere den mittelständischen Innovator*innen eine neue Verwertungsperspektive für ihre Innovationen im Bereich „Künstliche Intelligenz“ zu eröffnen und künftigen Innovator*innen den effizienten Aufbau intelligenter Lösungen auf Basis existierender Komponenten zu erleichtern.
Für mittelständische Anwender sollten die für sie relevanten KI-Komponenten auffindbar gemacht und so der Zugang zur KI erleichtert werden. Die entstehenden Netzwerkeffekte

11 https://www.vde.com/de/presse/pressemitteilungen/technologische-souveraenitaet

12 https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/das-projekt-gaia-x-executive-summary.pdf?__blob=publicationFile&v=16

steigern die branchenübergreifende Integration der neuen Technologien und verringern die Einstiegshürden. Der Erfolg des Austauschs sollte durch intelligente Beschreibungs-, Such- und Empfehlungs-Assistenten gewährleistet werden. Diese sollten die effiziente Auffindbarkeit von Komponenten ermöglichen und somit den souveränen Innovationstransfer in einem offenen, modularen und transparenten Ökosystem fördern. Die Gesellschaft für Informatik wird sich in dieser Fragestellung auch künftig einbringen.

(4) Governance-Strukturen für eine digitale Souveränität

Die Diskussion um den Governance Strukturen zur Bewahrung oder Erreichung einer digitalen Souveränität komplettiert dieses Arbeitspapier. So stellt das Positionspapier der Fokusgruppe „Digitale Souveränität" fest, dass es im EU-Binnenmarkt gelingen muss, faire und gleiche Bedingungen für alle Akteure sicherzustellen und einer Fragmentierung entgegenzuwirken. Dazu seien „regulatorische Rahmenbedingungen erforderlich – im nationalen, europäischen und auch internationalen Maßstab. Dabei gilt es Governance-Regeln zu verankern sowie das Innovationssystem weiterzuentwickeln, aber auch Aspekte der Datensouveränität und -sicherheit ebenso abzubilden wie Interessen der Beschäftigten und des Individuums allgemein. Private Investitionen dürfen jedoch nicht von einem Übermaß an staatlichem Interventionismus unterdrückt werden."[13]

Dazu müssten grundsätzlich der rechtliche Rahmen zu einer besseren Datenportabilität sowie zur Interoperabilität geschaffen werden. Demnach erforderten verstärkte Konzentrationstendenzen auf digitalen Plattformmärkten zügigere Verfahren in der Missbrauchsaufsicht mit einem stärkeren Fokus auf konglomeraten Effekten. Eine Weiterentwicklung der Missbrauchsaufsicht sei unabkömmlich, „um eine stabile und aktuelle Grundlage für verbesserte und beschleunigte Entscheidungen zu schaffen. In Fällen von Marktmissbrauch oder Marktversagen ist ergänzend zu bestehenden wettbewerbsrechtlichen Bestimmungen zu erwägen, ob und in welchem Umfang auf dann regulatorischem Wege eine weitergehende Datenportabilität erforderlich ist, um u. a. kleineren, innovativen Anbietern im Wettbewerb eine Chance zu bieten."

Thomas Bendig weist in seinem Beitrag darauf hin, dass im Sinne der digitalen Souveränität im Kontext plattformbasierter Ökosysteme eine Stärkung der europäischen Anbieterlandschaft ebenso erforderlich sei wie ein Ausbau des Marktortprinzips. Demnach sei für den Erfolg plattformbasierter Ökosysteme ein ausgewogener Regulierungsrahmen erforderlich, der einerseits das Entstehen von Digitalplattformen in der EU fördert und gleichzeitig Marktmachtmissbrauch verhindert.

Manuel Höferlin unterstreicht in seinem Beitrag wie IT-Sicherheit „made in Europe" einen wichtigen Beitrag zur digitalen Souveränität leisten kann, weil es die physische Resilienz der Systeme stärkt. Demnach sei IT-Sicherheit die wirksamste Grundlage für digitale Souveränität. Zudem plädiert Höferlin dafür eine zentrale staatliche Stelle zur Koordinierung staatlicher Digitalisierungsmaßnahmen zu schaffen: Ein Digitalministerium auf Bundesebene.

Den Rahmen der Publikation bilden ein Beitrag von *Luise Kranich*, die insbesondere die Entscheidungssouveränität betont. Um digitale Souveränität einschätzen und gestalten zu können, bedarf es wissenschaftlicher Methoden, denn nur wenn klar ist, worüber wir gesprochen wird, können auch wirkungsvolle Maßnahmen entwickelt und deren Umsetzung sinnvoll evaluiert werden.

Christine Regitz und *Anja Schaar-Goldapp* geben einen Ausblick, wie insbesondere die aktuellen Entwicklungen in der Corona-Krise auch eine Chance sein können.Um digitale Souveränität einschätzen und gestalten zu können, benötigen wir wissenschaftliche Methoden – nur wenn wir uns einig sind, worüber wir genau sprechen, können wir Maßnahmen entwickeln und deren Umsetzung sinnvoll evaluieren.

13 *Seite 13: https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2019/digitale-souveraenitaet.pdf?__blob=publicationFile&v=3*

EINFÜHRUNG

DER MARATHON AUF DEM DRAHTSEIL: KOMPETENZEN FÜR EINE DIGITALE SOUVERÄNITÄT

Luise Kranich, FZI Forschungszentrum Informatik

Um digitale Souveränität einschätzen und gestalten zu können, benötigen wir wissenschaftliche Methoden – nur wenn wir uns einig sind, worüber wir genau sprechen, können wir Maßnahmen entwickeln und deren Umsetzung sinnvoll evaluieren.

Für alle Institutionen in Deutschland und Europa stellt sich digitale Souveränität als Gratwanderung zwischen Fremdbestimmung und Abschottung dar: Wie kann ich mir Fortschritte Dritter zunutze machen ohne davon zu abhängig zu werden? Welche konkreten Entwicklungs- und Herstellungskompetenzen benötigen wir, um in relevanten Technologiefeldern Vorreiter zu sein? Welche konkreten Prüf- und Veredelungskompetenzen benötigen wir, um Technologien Dritter selbstbestimmt einsetzen zu können?

Diese Fragen hat das FZI gemeinsam mit Accenture und Bitkom Research im Rahmen der durch das Bundesministerium für Wirtschaft und Energie beauftragten und im Jahr 2017 veröffentlichten Studie „Kompetenzen für eine digitale Souveränität“14 adressiert. Viele der Erkenntnisse sind auch heute noch aktuell. Der Themenkomplex „digitale Souveränität“ erlebt nun – drei Jahre später – eine kleine Renaissance. Steigende Abhängigkeiten von IT-Lösungen führen dazu, dass der Ruf nach digitaler Souveränität lauter wird. Das nährt einerseits die Debatte, führt aber auch dazu, dass der Begriff droht, zum leeren Buzzword zu werden. Dies erschwert und verlangsamt den Diskurs wiederum.

Drei Jahre nach Veröffentlichung der Studie15 werden einige darin angesprochenen Aktionsfelder bereits mit Hochdruck bearbeitet und die wichtige Zielsetzung der digitalen Souveränität wird von verschiedensten Akteur*innen intensiv beleuchtet. Nichtsdestotrotz gibt es neben dem Wunsch nach Versachlichung und Konkretisierung der Debatte auch einige Hinweise an die handelnden Institutionen und Personen:

1. Nicht „Wir gegen die“ sondern „Wir gemeinsam“ – und zwar koordiniert:
In vielen Diskussionen wird ein Spannungsfeld zwischen Europa, den USA und China aufgezeigt, das von Konkurrenz und Abgrenzung gekennzeichnet ist. Doch diese und viele andere Volkswirtschaften verbindet mehr als sie trennt. So sollten auch in der öffentlichen Kommunikation gemeinsame Wert-

Luise Kranich © privat

vorstellungen von „like-minded nations“ in den Vordergrund gestellt werden.

2. Besonderheiten in Deutschland und Europa anerkennen und Stärken fördern:
Unsere Wirtschaft ist strukturell anders als die in anderen Regionen der Welt. Die Heterogenität im Mittelstand ist Herausforderung und Chance zugleich und erfordert spezifische Maßnahmen. Wirtschafts- und Innovationspolitik hat daher den Auftrag, kleine und mittlere Unternehmen aktiv einzubeziehen.

3. Auf konkreten Nutzen konzentrieren, anstatt ziellose Debatten zu führen:
Um den Mittelstand für Digitalisierungsvorhaben zu begeistern, muss er überzeugt werden. Dies geht am besten durch klare Beispiele: Was wird durch diese Innovation besser? Welche wirklichen Probleme lösen wir damit?

4. Ehrgeizig und selbstbewusst eigene Wege gehen:
Deutschland mag auf der internationalen Bühne nicht immer besonders cool oder innovativ wirken, aber wir sind in Vielem besser als wir selbst glauben. Wir müssen und dürfen uns nicht verstecken. Wir sollten also nicht nur versuchen, in Puncto Datensouveränität mit den großen Playern mitzuhalten, sondern direkt darüber nachdenken, was wir besser können als diese.

---

14 https://www.bmwi.de/Redaktion/DE/Publikationen/Studien/kompetenzen-fuer-eine-digitale-souveraenitaet.html

15 S.o., Kompetenzen für eine digitale Souveränität

Der Schlüssel digitaler Souveränität ist die Entscheidungssouveränität. Neben gesellschaftlichen Veränderungen müssen wir auch zu jeder Zeit die großen technologischen Entwicklungen vorhersehen und mitgestalten. Hierfür brauchen wir einen gemeinsamen Plan, den Wissenschaft, Wirtschaft, Politik und Zivilgesellschaft engagiert umsetzen.

Luise Kranich leitet am FZI Forschungszentrum Informatik die Berliner Außenstelle und den Bereich „Innovation, Strategie und Transfer". Mit ihrem Team forscht sie an technologischen, ökonomischen und gesellschaftlichen Fragen der Digitalisierung und wie diese sinnstiftend und unter Wahrung der digitalen Souveränität eingesetzt werden kann.

1. KOMPETENZBILDUNG FÜR DIGITALE SOUVERÄNITÄT

DIGITALE SOUVERÄNITÄT BEGINNT MIT GUTER DIGITALER BILDUNG

Tankred Schipanski, MdB

Digitale Souveränität entsteht durch verschiedene Faktoren. Zentral ist der Erwerb von Technik- und Medienkompetenz im Schulalter. Hierzu muss sich die Schulbildung in Deutschland neu aufstellen und der Bund Hilfestellung leisten.

Ich verstehe unter Digitaler Souveränität, dass der*die einzelne Bürger*in, Unternehmen oder die öffentliche Verwaltung selbstständig, selbstbestimmt und sicher in der digitalen Welt handeln und entscheiden können. Dazu gehören beispielsweise Fähigkeiten wie Medienkompetenz sowie Rahmenbedingungen, die es mir ermöglichen, meine Sicherheits- und Datenschutzinteressen kontrollieren zu können (z.B. DSGVO). Nicht zuletzt benötigen wir auch die technologischen Fähigkeiten, um bei der rasanten Entwicklung digitaler Schlüsseltechnologien, entsprechenden Diensten und Plattformen, verantwortungsvoll handeln zu können. Dazu gehört auch, bei technischen Produkten selbstbestimmt beurteilen zu können, ob der Anbieter leistungsfähig und vertrauenswürdig ist und diese Produkte entsprechend einzusetzen.

Um Medien- und Technikkompetenzen zu fördern bedarf es eines Ausbaus unserer Bildungseinrichtungen zu qualitätsvollen Vermittlern digitaler Kompetenz. Das föderal organisierte Bildungssystem ist den Herausforderungen der Digitalisierung an manchen Stellen nicht gewachsen. Die Möglichkeiten, aber auch die Gefahren, die Digitalisierung im Bildungsbereich mit sich bringt, dürfen wir nicht unterschätzen: Das Grundproblem umschreibe ich mit meiner Forderung: aus der Informationsflut darf keine Wissensdürre werden! Unsere Bildungseinrichtungen sind inhaltlich und

Tankred Schipanski © Tobias Koch

methodisch auf die Herausforderungen der digitalen Gesell schaft nicht ausreichend vorbereitet. Weder die mäßigen Bemühungen der Kultusministerkonferenz, noch ein Bildungsstaatvertrag werden diese Problematik lösen.

Schülerinnen und Schüler müssen die grundlegenden Strukturen und Zusammenhänge von Naturwissenschaften, Technikwissenschaften, Informatik und Mathematik erlernen und ein Verständnis für wirtschaftliche, politische und soziale Zusammenhänge entwickeln. Deshalb muss die Vermittlung von Fach- und Methodenkompetenz einen besonderen Schwerpunkt einnehmen. Detailkenntnisse können aus Datenbanken abgerufen werden.

Gleichzeitig ist die Lehrerfortbildung Schlüssel zum Erfolg. Diese ist mit Blick auf die digitale Bildung unzureichend. Es muss sichergestellt sein, dass die Lehrkräfte auf höchstem

Niveau in den Bereichen Informationstechnik, Informationssicherheit und Medienkompetenz fortgebildet werden. Ich halte ein stärkeres Engagement des Bundes für notwendig, ähnlich wie der Bund dies für „Gute Lehre“ an unseren Hochschulen organisiert.

Hochschulen und Universitäten müssen außerdem auf den steigenden Fachkräftebedarf eingehen und entsprechende Studiengänge entwickeln und anbieten. Dazu zähle ich beispielsweise die Studiengänge IT-Sicherheit, Data Engineering und Data Science. Nur so können wir sicherstellen, dass Deutschland befähigt ist im Auf- und Ausbau von Schlüsseltechnologien der Zukunft wettbewerbsfähig und damit digital souverän zu bleiben. Zudem muss das Bundesamt für Sicherheit in der Informationstechnik (BSI) zu einer zentralen Anlaufstelle für Fragen der IT-, Internet- und Cybersicherheit weiterentwickelt werden. Auch dies stärkt die Digitale Souveränität aller Bürgerinnen und Bürger.

Tankred Schipanski ist seit 2009 Mitglied des Deutschen Bundestages. Er ist Vorsitzender und Sprecher der Arbeitsgruppe Digitale Agenda der CDU/CSU-Bundestagsfraktion und ordentliches Mitglied der Ausschüsse Digitale Agenda sowie Bildung, Forschung und Technikfolgenabschätzung

2. DATENSOUVERÄNITÄT

DIGITALE SOUVERÄNITÄT IM KONTEXT PLATTFORMBASIERTER ÖKOSYSTEME

Thomas Bendig, Fraunhofer-Verbund IUK-Technologie

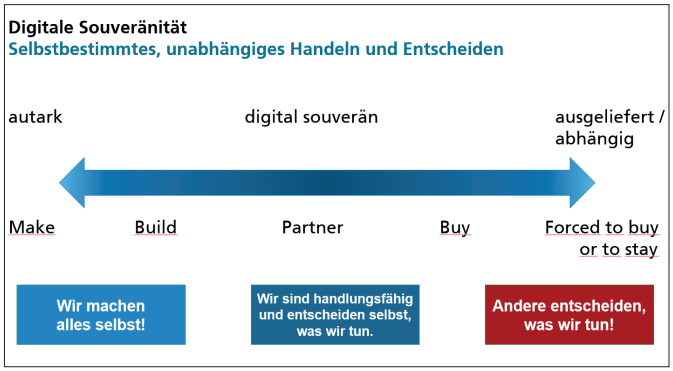
Digitale Souveränität wird meist als ein Begriff verwendet, der vermittelt an welcher Stelle zwischen Autarkie und wirtschaftlicher Abhängigkeit man sich mit seinem digitalen Geschäftsmodell bewegt. Im Kontext plattformbasierter Ökosysteme wird schnell deutlich, wie vielschichtig dieser Begriff im realen Anwendungskontext ist.

Digitale Plattformen sind wichtiger Bestandteil von Wirtschaft, Medien, Politik und Gesellschaft. Sie haben sich zu komplexen Ökosystemen entwickelt und können Märkte in neuer Form beflügeln, gefährden oder völlig neue Märkte schaffen. Allerdings scheinen Deutschland und Europa angesichts starker US-Plattformen und asiatischer Unternehmen die „digitale Anschlussfähigkeit“ an globale Entwicklungen verloren zu haben. Mit steigender Bedeutung digitaler Plattformen und ihrem wachsenden Einfluss auf die Fähigkeit von Staat, Unternehmen und Gesellschaft kommunizieren zu können, Geschäfte miteinander abzuwickeln und im weitesten Sinne innovativ zu sein, steigt einerseits die Notwendigkeit zur Sicherung der Digitalen Souveränität der Plattformnutzer (i. d. R. Individuen, staatliche Stellen, Unternehmen).

Andererseits ist die grundsätzliche Fähigkeit, digitale Plattformen selbst zu entwickeln und zu betreiben, ebenso Ausdruck digitaler Souveränität. Ohne sie verliert Europa in

Thomas Bending © Die Hoffotografen

vielen Feldern der digitalen Transformation die Möglichkeit, Datenströme und Wertschöpfungspotentiale zu steuern, was mit fundamentalen Folgen für Wertschöpfung und Prosperität einherzugehen droht. Auch demokratische Werte und die Stabilität unseres politischen Systems sind angesichts der sich stark verändernden und teils fast unberechenbaren geopolitischen Verschiebungen potentiell in Gefahr, wenn für Kommunikation, Waren- oder Informationsaustausch ausschließlich Plattformen genutzt werden, die in Europa nicht kontrolliert werden können.



Allerdings besteht die Chance für Deutschland und Europa darin, proaktiv zu bestimmen, in welchen gesellschaftlichen, wissenschaftlichen und/oder wirtschaftlichen Bereichen plattformbasierte Ökosysteme technisch entwickelt und betrieben werden sollen bzw. sogar müssen. Insbesondere für diese Bereiche gilt es Marktbedingungen zu schaffen, welche die digitale Souveränität des Einzelnen, von Unternehmen und Forschungseinrichtungen sowie des Staates in den Mittelpunkt stellen und schützen.

Diese Marktbedingungen müssen in der humanistischen und föderalen Tradition Europas stehen und die digitale Selbstbestimmtheit als Grundpfeiler verankern. Sie müssen verteilte und von zentralen Instanzen unabhängige Datenhaltung und die freie Nutzung selbst generierter Daten fördern. Dadurch senken sie Markteintrittsbarrieren, sichern Innovationspotentiale und mildern die bei digitalen Plattformen verbreitete „Winner-takes-it-all"-Effekte. Sie bevorzugen eher mittelständisch geprägte, von Wettbewerb und Innovation bestimmte Wirtschaftssysteme, ohne dass sie die großen, mit Plattformen verbundenen Chancen, in Bezug etwa auf Wachstum und Schaffung neuer Märkte und Technologien einschränken.

Wesentliche Bestandteile solcher Marktbedingungen sind das unmittelbare Selbstbestimmungsrecht über die durch Interaktion mit einer Plattform generierten Daten sowie die Möglichkeit, solche Daten selbst zu nutzen oder Dritten einfach zur Verfügung zu stellen. Das wiederum erfordert Transparenz sowie Vorherseh- und Nachprüfbarkeit der Prozesse, in die Daten eingehen und aus denen neue Daten entstehen.

Datensouveränität ist ein elementarer Wegbereiter für Plattformen „made in Europe". Grundsätzlich ist für den Erfolg plattformbasierter Ökosysteme ein ausgewogener Regulierungsrahmen erforderlich, der einerseits das Entstehen von Digitalplattformen in der EU fördert und gleichzeitig Marktmachtmissbrauch verhindert. Im Sinne einer globalen Wirtschaftsfähigkeit braucht es zudem Erleichterungen von Kooperationsmodellen auch und gerade mit Wettbewerber*innen. Im Bereich von Plattformen zur Interaktion von Unternehmen untereinander sind außerdem partizipative Prozesse zur Gestaltung der Plattformregeln erforderlich sowie – analog zum Internet – der föderierte Aufbau, der es ermöglicht, Teile von Plattformen unter der eigenen Kontrolle zu betreiben, ohne dabei von anderen Teilen und damit vom Gesamtnutzen der Plattform ausgeschlossen zu sein.

Solche Bedingungen bieten die Chance, durch föderiert aufgebaute Multi-Cloud-Technologien in Europa Plattformen zu schaffen, die spätestens mittelfristig zu etablierten großen Plattformen kompetitiv sind. Im Sinne der digitalen Souveränität ist eine Stärkung der europäischen Anbieterlandschaft ebenso erforderlich wie ein Ausbau des Marktortprinzips. Zur Umsetzung dieser Ziele ist es im Sinne der digitalen Souveränität Europas unerlässlich, dass der Staat selbst als Leitnachfrager entsprechender Lösungen fungiert.

Dieser Beitrag basiert auf dem Beitrag der Fokusgruppe Digitale Souveränität im Rahmen des Digitalgipfels 2019.[16]

Thomas Bendig ist Forschungskoordinator des Fraunhofer-Verbundes IUK-Technologie. Neben der strategischen Koordination der 21 Fraunhofer-Institute, zählt der Technologie-Transfer aus der Forschung in die Wirtschaft zu seinen Aufgaben.

16 *„Digitale Souveränität im Kontext plattformbasierter Ökosysteme", Fokusgruppe Digitale Souveränität im Rahmen des Digitalgipfels 2019, https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2019/digitale-souveraenitaet.pdf?__blob=publicationFile&v=3*

INDIVIDUELLE DATENKONTEN – ODER WAS MEIN STAUBSAUGER MIT DIGITALER SOUVERÄNITÄT ZU TUN HAT

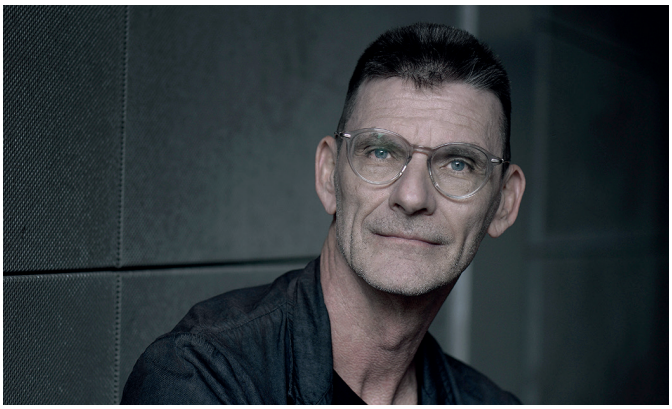
Karl Steinacker

Digitalisierung macht Spaß: Ich sitze auf dem Sofa und lese ein Buch. Derweil surrt der selbstfahrende Staubsauger-Roboter durch die Wohnung. So entspannt muss es sein, demnächst zeitungslesend im selbstfahrenden Auto durch die Landschaft zu fahren!

Als ich den Roboter kaufte, wusste ich allerdings nicht, dass dadurch auch meine Wohnung regelmäßig vermessen wird: Nach jeder Fahrt wird ein neuer Grundriss meiner Wohnung als Arbeitsnachweis produziert. Die Bedienungsanleitung des Staubsaugers nimmt – und es war nicht anders zu erwarten – keinen Bezug auf das Grundgesetz, und die Prinzipien der Unverletzlichkeit der Wohnung (Artikel 13 GG) und der Volkssouveränität (Artikel 20 GG). Denn es liegt an uns, dem Souverän, die Digitalisierung nach den Maßstäben unser Rechts- und Werteordnung zu gestalten.

Deshalb sollten Informatiker, Manager und Politiker sich mit den Analysen und Empfehlungen von Wissenschaftlern wie Nick Srnicek[17], José van Dijck[18], Peter F. Cowhey und Jonathan D. Aronson[19] und anderer, die soziologische und demokratietheoretische Ansätze verfolgen, auseinandersetzen. Danach trägt das neoliberale Modell einer sich selbst-regulierenden digitalen Transformation nicht: „States can guarantee a level playing field where actors are held to conform to democratically agreed upon public values “[20].

Was heißt das konkret für unsere Staubsauger und Autos? Die Daten, die diese generieren gehören auf ein persönliches Datenkonto und nicht auf die Server der Hersteller*innen. Ein persönliches Datenkonto ist der Grundstein für eine effektive individuelle Datensouveränität und informationelle Selbstbestimmung, denn ich kann nur das kontrollieren wozu ich exklusiven Zugriff habe. Analog zu meinem Geld und Aktien gehören meine persönlichen Daten auf mein Konto.



Karl Steinacker © Gerlind Klemens Fotodesign

Der Gesetzgeber hat allen Bürger*innen das Recht auf ein Bankkonto eingeräumt. Jetzt ist der nächste Schritt fällig: Das Recht auf ein individuelles Datenkonto und damit zum mobilen Internet und Cloudcomputing. Die digitale Infrastruktur gehört zur staatlichen Daseinsvorsorge ebenso wie die Bereitstellung von Elektrizität und Straßen, Schulen, öffentlichen Verkehrsmitteln usw. Das Zusammenspiel von privatwirtschaftlichen Banken und staatlicher Bankenaufsicht könnte zum Modell für die Verwaltung der digitalen Privatsphäre werden: Private Anbieter*innen verfolgen rentable Geschäftsmodelle für Vertrauens- und Identifikationsdienste und einer Wertschöpfung, die auf dem Respekt des Privaten beruht.

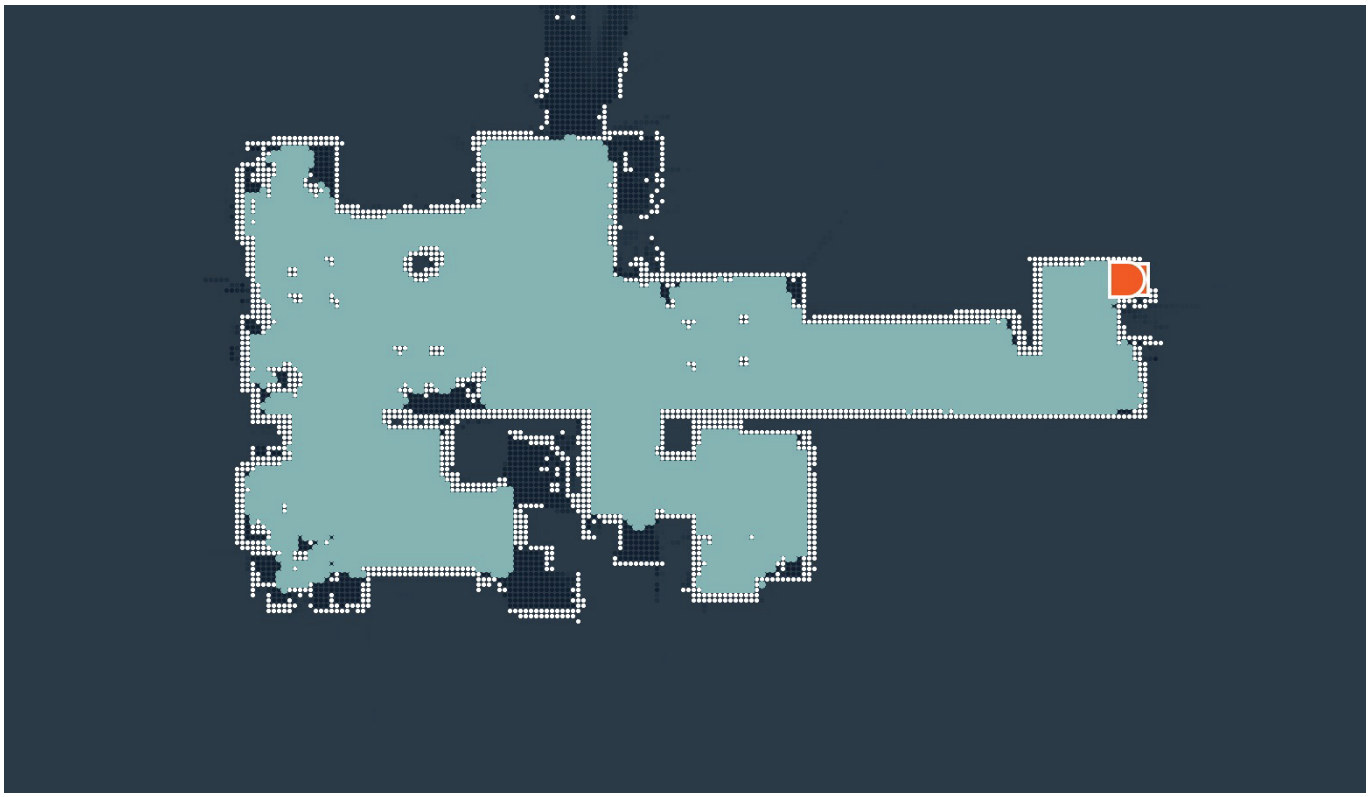
Geschäftsmodelle bei den der*die Einzelne mit seinen Daten zahlt, gehören unterbunden. Stattdessen sollten neue Plattformen, zum Beispiel im Mobilitätssektor, den zivilgesellschaftlichen Forderungen nach individueller Datenhoheit, Interoperabilität und Portabilität entsprechen.
Die Partnerin von Politik und Wirtschaft für dieses Projekt ist die Zivilgesellschaft. Das zeigt auch das Beispiel aus Kanada. Dort arbeitet seit 2014 der Digital ID & Authentication

17 *Nick Srnicek, Platform Capitalism, 2017*

18 *José van Dijck et al., The Platform Society, 2018*

19 *Peter F. Cowhey/Jonathan D. Aronson, Digital DNA, 2017*

20 *José van Dijck, S. 187*



Der Grundriss meiner Wohnung, wie ihn der Roboter sieht

Council of Canada[21] an einem informationellen Vertrauenssystem, welches das Land in seiner ganzen Weite und Vielfalt umfasst.

Für die Wirtschaft ist der*die Einzelne Kunde*in, für die Zivilgesellschaft selbstbestimmte*r Bürger*in. Dies ist kein Widerspruch. Wirtschaft, Politik, und Zivilgesellschaft können gemeinsam die Spielregeln der digitalen Welt so gestalten, dass Wohlstand und Freiheitsrechte auch für die Zukunft bewahrt werden.

Karl Steinacker ist Digitaler Berater des International Civil Society Centres in Berlin. Zuvor hat er für die Vereinten Nationen viele Jahre das Personenstandsystem für Flüchtlinge und die Entwicklung Konzepte digitaler Identität geleitet.

21 https://diacc.ca

3. TECHNISCHE SOUVERÄNITÄT

DIGITALE SOUVERÄNITÄT BRAUCHT AUFKLÄRUNG

Dr. Jens Zimmermann, MdB

Aufklärung ist der Ausgang des Menschen aus seiner selbstverschuldeten Unmündigkeit“[22], schrieb Kant bereits 1784. Die digitale Mündigkeit aller Bürgerinnen und Bürger ist Grundlage für die digitale Souveränität unserer Gesellschaft heute. Wir sprechen zu oft nur von Wirtschaft, Monopolen, von China, den USA, von Abhängigkeiten und Technologievorreitern. Doch digitale Souveränität beginnt in den Köpfen der Einzelnen.

Dr. Jens Zimmermann © Marlene Bleicher

Digitale Souveränität beginnt bei Programmierkursen in der Schule, Kampagnenarbeit zu digitalen Rechten und einem Grundverständnis von Datenschutz. Sie benötigt gute digitale Bildungsarbeit.

Nur wenn Bürgerinnen und Bürger verstehen, was der Staat reguliert, können wir digitale Souveränität erreichen. Und regulieren müssen wir die digitale Welt. Wir müssen den Big Techs deutlich Grenzen setzen, wenn sie einen Markt nach dem anderen monopolisieren. Doch digitale Souveränität erreichen wir nicht nur durch die Eingrenzung der digitalen Monopole, sie braucht auch die Förderung eigener europäischer Alternativen. Oft ist die Rede von einem „digitalen Airbus.“ Genau dies brauchen wir in Europa.

Am Beispiel der Debatte um den 5G Ausbau lässt sich das Aufzeigen. Natürlich sind Anbieter*innen aus autoritären Ländern ein Sicherheitsproblem. Denn selbstverständlich sind sie im Zweifel gezwungen Informationen an den entsprechenden Staat weiterzugeben. Deshalb umfasst digitale Souveränität auch die Souveränität über die europäische digitale Infrastruktur. Den Zugriff außereuropäischer Mächte auf kritische europäische Infrastruktur müssen wir gegenwärtig und zukünftig unterbinden. Die Frage um den 5G Ausbau ist letztendlich auch eine Frage der wirtschaftlichen Souveränität. Setzen wir jetzt nicht auf europäische Anbieter*innen, dann laufen wir Gefahr Fehler der Vergangenheit zu wiederholen. Gerne erinnere ich an das Thema Photovoltaik, bei dem wir nur auf Technologien aus einem außereuropäischen Land gesetzt haben. Mit welchem Ergebnis? Europäische Wettbewerber gibt es in diesem Sektor heute nicht mehr. Das darf uns beim Thema 5G nicht passieren. Dafür ist diese Infrastruktur zu kritisch und zentral für unsere Zukunft.

Was bedeutet das für unsere digitale Souveränität? Es bedeutet, dass wir sie komplex denken müssen. Aus dem Blickwinkel der Gesellschaft, der Wirtschaft und unserer Sicherheit.
Die Grundlage bleibt die Befreiung des Menschen aus der digitalen Unmündigkeit. Wir brauchen Regeln für die digitale Welt, wir brauchen gute digitale Bildung, wir brauchen Mut für unseren europäischen Weg einzustehen.

Dr. Jens Zimmermann ist seit 2013 Mitglied des Deutschen Bundestags. Seit 2018 ist er digitalpolitischer Sprecher der SPD-Bundestagsfraktion. In Ingolstadt und London hat er Betriebswirtschaftslehre studiert und 2013 promoviert.

---

22 *Immanuel Kant, Beantwortung der Frage: Was ist Aufklärung? in: Berlinische Monatsschrift, Dezember 1784, 481-494.*

INFORMED CONSENT: VON DER UTOPIE ZUM NORMALFALL

Dr. Bernhard Waltl, GI/ PD Dr. Katharina M. Huster/Prof. Dr. Georg Schmidt

Die informierte Einwilligung ist eine akzeptierte Maßnahmen um Bürger und Bürgerinnen über für sie relevante Abläufe und Entscheidungen aufzuklären. Dies setzt voraus, dass die bereitgestellte Information verständlich ist und von der Zielgruppe erfasst werden kann. In der Praxis zeigen sich hier große Mängel. Von einem ethischen Standpunkt kann dies nicht hingenommen werden. Die Digitalisierung bietet uns Möglichkeiten die Souveränität wieder zurückzugewinnen. Eine Chance für die Menschen und die Gesellschaft, die hier am Beispiel der Medizin dargestellt wird.

Unmittelbar vom Grundgesetz leitet sich des Persönlichkeits- und Selbstbestimmungsrechts jedes einzelnen Menschen ab. Für die medizinische Forschung, deren Grundlage klinische Studien am Menschen sind, ergeben sich daraus einige Konsequenzen: Trotz sorgfältiger Vorbereitungen und Planungen sind Risiken bei Klinischen Studien, an denen Verfahren am Menschen getestet werden, nie ganz auszuschließen. Die Weltärztekammer hat dazu in der Deklaration von Helsinki[23] ethische Richtlinien verabschiedet, die besagt, dass „potentielle Versuchsperson angemessen über die Ziele, Methoden, [...] die potentiellen Risiken der Studie, möglicherweise damit verbundenen Unannehmlichkeiten, [...] informiert werden." Darüber legt die Deklaration fest, dass sicherzustellen ist, dass „die potentielle Versuchsperson diese Informationen verstanden hat, [...]."

In der Praxis fasst die schriftliche Patienteninformation die Hauptinhalte des Aufklärungsgesprächs zusammen und dokumentiert dieses. Die Patienteninformation weist jedoch oft erhebliche Mängel auf, sodass von einem „informed consent" eigentlich nicht mehr ausgegangen werden kann. Sie sind schlecht strukturiert, sprachlich unzulänglich und für die Zielgruppe damit schwer verständlich. Oft wird mehr Wert auf die Erfüllung der gesetzlichen Anforderungen und den Schutz der Institution der Wissenschaftler*innen gelegt als auf die Verständlichkeit der Dokumente. Eine aufgeklärte und wirklich selbstbestimmte Entscheidung für oder gegen die Teilnahme an der wissenschaftlichen Studie ist daher in vielen Fällen nicht gegeben. Dies ist unethisch und nicht akzeptabel.

Dieses Phänomen beschränkt sich allerdings nicht nur auf die Medizin, sondern zieht sich damit wie ein roter Faden durch die immer komplexer werdende Welt und findet sich auch in vielen digitalen Bereichen wieder, z. B. Geschäftsbedingungen von Online-Plattformen (AGBs), Information zu Datenschutz und automatisierte Datenverarbeitung, oder Einwilligung bei Kreditauskunft und Bonitätsprüfung, etc. beobachten.

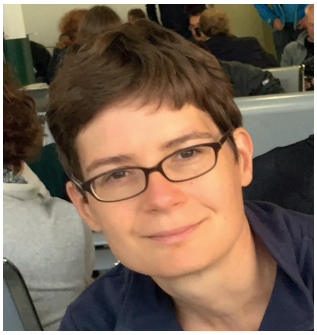
Prof. Dr. Georg Schmidt ©privat

Fortschritte im Bereich Künstliche Intelligenz und der algorithmischen Verarbeitung natürlicher Sprache geben uns die Möglichkeit, Mängel bei Patienteninformation sehr schnell und objektiv nachzuweisen und aufzudecken. Nach erfolgter Anpassung auf die jeweilige Domäne kann man Antragstellern konstruktive Hinweise zur Verbesserung und Korrektur geben, sodass die sprachliche Richtigkeit sichergestellt und deutlich lesbarere und verständlichere Texte entstehen. Damit kann man viele der oben genannte Probleme lösen. Die Selbstbestimmung des Menschen bleibt durch eine echte informierte Einwilligung erhalten. Informed Consent wird durch die Digitalisierung ermöglicht, verliert den Status der Utopie und wird – zum Wohle des Menschen und der Gesellschaft - wieder zum Normalfall.

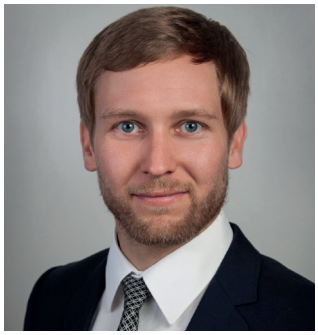
Dr. Bernhard Waltl hat an der TU München im Bereich Informatik promoviert, ist Mitglied der Fachgruppe GI Rechtsinformatik und beschäftigt sich mit der semantischen Analyse von Dokumenten mithilfe von künstlicher Intelligenz und Natural Language Processing.

Dr. Katharina M. Huster hat an der TU München promoviert und habilitiert. Sie ist Privatdozentin für Immunologie und Fachärztin für Mikrobiologie, Virologie und Infektionsepidemiologie und hat im Rahmen eines von der Tschira-Stiftung geförderten Projektes eTIC, ein elektronisches Tool für die Erstellung von Informed Consent Unterlagen entwickelt.

Prof. Dr. Georg Schmidt ist Kardiologe am Klinikum rechts der Isar, Vorsitzender der Ethikkommission der TU München und stellvertretender Vorsitzender des Arbeitskreises Medizinischer Ethikkommissionen in Deutschland.



Dr. Katharina M. Huster © privat



Dr. Bernhard Waltl ©privat

---

23 https://www.wma.net/policies-post/wma-declaration-of-helsinki-ethical-principles-for-medical-research-involving-human-subjects/

4 GOVERNANCE-STRUKTUREN FÜR DIGITALE SOUVERÄNITÄT

IT-SICHERHEIT ALS GRUNDLAGE DIGITALER SOUVERÄNITÄT

Manuel Höferlin, MdB

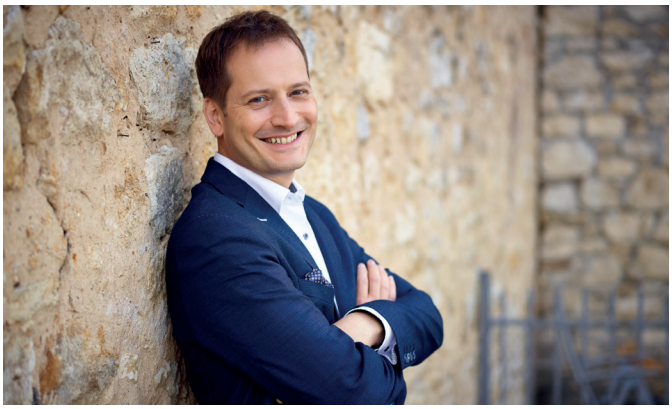
Digitale Souveränität ist komplex und weitreichend. Sie fußt in wesentlichen Teilen auf Rahmenbedingungen, die der Staat schaffen muss. Eine der wichtigsten davon ist IT-Sicherheit. Warum das so ist, erläutert der Vorsitzende des Bundestagsausschusses Digitale Agenda und digitalpolitischer Sprecher der FDP-Fraktion im Bundestag, Manuel Höferlin im folgenden Beitrag.

Im Zeitalter der digitalen Transformation gewinnt digitale Souveränität zunehmend an Bedeutung – auch in der Politik. Und das ist gut so. Denn das selbstbestimmte Entscheiden und Handeln von Menschen, Betrieben und Institutionen im digitalen Raum fußt zu einem erheblichen Teil auf Rahmenbedingungen, die auch der Staat schaffen kann. In meinen Augen spielt IT-Sicherheit hierbei eine zentrale Rolle. Denn richtig eingesetzt, bildet ein hohes Maß an IT-Sicherheit die beste Grundlage für digitale Souveränität.

Welche Maßnahmen können dafür also ergriffen werden? Am Anfang stehen da für mich die infrastrukturellen Grundlagen. Denn nicht erst seit den aktuellen Debatten um Huawei oder Gaia-X steht die Frage im Raum: Wie machen wir uns möglichst unabhängig? Und wie schaffen wir es im globalen Wettbewerb mitzuhalten? Ich finde, wir sollten hierbei unseren innovativen Mittelstand und unser eigenes Know-How – denn daran mangelt es uns nicht – für IT-Sicherheit „made in Europe“ zur globalen Standardsetzung nutzen.

Darüber hinaus leistet IT-Sicherheit „made in Europe“ auch einen wichtigen Beitrag zur physischen Resilienz unserer Systeme. Dabei darf es aber nicht bleiben. Denn der zweite große Risikofaktor für Resilienz ist und bleibt der Mensch (vgl. Phishing, Social Engineering, etc). Deshalb ist es für mich ebenfalls staatliche Aufgabe, eine resiliente Gesellschaft zu fördern und den Menschen von Kindesbeinen an entsprechende digitale Kompetenzen mit an die Hand zu geben.

Neben den Kompetenzen, sind aber auch handfeste Instrumente, wie ein Recht auf Verschlüsselung, wichtig. Denn kryptographische Systeme sollen zunehmend zugunsten von mehr Überwachung aufgeweicht werden. Damit soll angeblich mehr Sicherheit im Cyberspace erzeugt werden. Davor warne ich. Sichere Systeme dürfen nicht künstlich geschwächt werden. Eine effektive Verschlüsselung ist ein Grundpfeiler für die IT-Sicherheit und damit auch für die digitale Souveränität der Menschen und der Wirtschaft.



Manuel Höferlin © Christian Kuhlmann

Im nächsten Schritt stellt sich dann natürlich auch die Frage nach einer Weiterentwicklung des Datenschutzes. Denn im Sinne der digitalen Souveränität sollen – vereinfacht gesagt – die Menschen geschützt und befähigt werden – nicht abstrakte Daten. Datenschutz nach dem heutigen Verständnis kann das nicht leisten. Denn umfassender Datenschutz heißt nicht, nur der Verwendung von Daten zu widersprechen. Stattdessen muss die Souveränität des Einzelnen über seine Daten im Mittelpunkt stehen. Deshalb brauchen wir ein Bekenntnis für mehr Selbstbestimmung des Einzelnen über seine Daten, einen konsequenten Anonymisierungs-Ansatz für maschinengenerierte Daten und einen europäischen Rechtsrahmen für Datentreuhänder.

Das alles verdeutlicht: Digitale Souveränität ist komplex und weitreichend. IT-Sicherheit die wirksamste Grundlage dafür. Um alle Aspekte handhaben und koordinieren zu können, braucht es daher, nicht zuletzt als Grundvoraussetzung für den gesamten Prozess, eine zentrale Stelle, die sich der Aufgabe annimmt. Deshalb plädiere ich seit Jahren für ein Digitalministerium auf Bundesebene. Als Digital- und Innenpolitiker der Freien Demokraten werde ich mich auf jeden Fall weiter dafür einsetzen, die entsprechenden Rahmenbedingungen zu schaffen.

Manuel Höferlin ist Vorsitzender des Bundestagsausschusses Digitale Agenda und digitalpolitischer Sprecher der FDP-Bundestagsfraktion. Er zählt zu den Digitalpolitikern der ersten Stunde im Bundestag, dem er von 2009 bis 2013 und seit 2017 angehört.

KI-ENTWICKLUNG BRAUCHT UNABHÄNGIGE INFRASTRUKTUREN

Dr. Jörg Bienert, KI-Bundesverband

Künstliche Intelligenz ist eine zentrale Komponente für zukünftige Innovation in vielen Bereichen und damit Grundlage für zukünftiges Wirtschaftswachstum. Für eine leistungsfähige europäische KI-Industrie ist eine eigene Cloud-Infrastruktur eine wichtige Voraussetzung.

Eine wesentliche Voraussetzung für die erfolgreiche Transformationen hin zu einer digitalisierten, KI-gestützten Wirtschaft ist der Erhalt der digitalen Souveränität.

Wir erleben derzeit einen gewaltigen Umbruch im Bereich der IT. Unternehmen fast aller Branchen transferieren ihre zentralen Computer-Infrastrukturen hin zu Cloud Services. Dies geschieht aus Gründen der Gesamtkosten, flexiblen Skalierbarkeit aber auch wieder aus einem zu erwartenden Mangel an Fachkräften. Gerade der Mittelstand wird es zukünftig immer schwerer haben, ausreichend Systemadministrator*innen zum Betrieb eigener Infrastruktur zu rekrutieren.

Dominiert wird der Markt von den amerikanischen Diensten Amazon Webservices (AWS), Microsoft Azure und Google Cloud Services, doch stehen chinesische Anbieter wie Alibaba oder Tencent in den Startlöchern. Es ist faszinierend, welches Portfolio an Diensten und Services diese Anbieter in den letzten Jahren aufgebaut haben auf den verschiedenen Ebenen Infrastructure as a Services (IaaS), Platform as a Service (PaaS) und Software as a Service (SaaS). Dieser Segen ist gleichzeitig auch ein Fluch. Unternehmen gegeben sich mit der Nutzung dieser Services zunehmend in eine wachsende Abhängigkeit von diesen Anbietern. Einmal getätigte Investitionen in Software, Infrastruktur und Prozesse lassen sich nur bedingt zu einem alternativen Anbieter transferieren, es kommt zum Lock-In.

Berücksichtigt man, dass im Jahr 2025 schätzungsweise bereits 80% der deutschen Unternehmen die Cloud-Services nutzen, so wird aus dem betriebswirtschaftlichen ein volkswirtschaftliches Problem. Die Funktionsfähigkeit vieler Unternehmen und damit der deutschen Wirtschaft ist direkt abhängig von einigen wenigen Dienstleistern. Hinzu kommt eine durchaus ernstzunehmende politische Komponente, wie das von Washington durchgesetzte Verbot der Android-Nutzung durch Huawei oder die Abschaltung der Adobe Cloud in Venezuela gezeigt haben.

Es wird also dringend eine deutsche oder europäische Alternative benötigt. Das Bundeswirtschaftsministerium hat hier unter der Leitung von Marco-Alexander Breit mit Gaia-X eine Initiative gestartet, die Standards für einen virtuellen Hyperscaler erarbeitet, auf deren Basis Marktteilnehmer*innen einheitliche, transparent migrierbare Cloud Services anbieten können. Wichtig ist hierbei jedoch, dass dieses Angebot von großen Playern zu attraktiven Preisen auf den Markt kommen. Auch darf sich das Angebot nicht auf die Bereitstellung von Infrastruktur beschränken, sondern muss einen umfassenden Katalog von Services auf allen Ebenen entwickeln. Erfolgt dies nicht, oder sind die Umsetzungsversuche zu zaghaft, so werden kaum Kund*innen gewonnen werden, und es wird bei Konzepten bleiben.

Dr. Jörg Bienert © Jörg Bienert

Gerade für die aufkommende europäische KI-Industrie wäre das fatal, da die Cloud-Anbieter auf Basis Ihrer Rechenkapazität und vorhandenen Datenmassen immer mehr KI-Dienste out-of-the box als leistungsfähige Services bereitstellen und somit immer kleinere Nischen übrigbleiben.

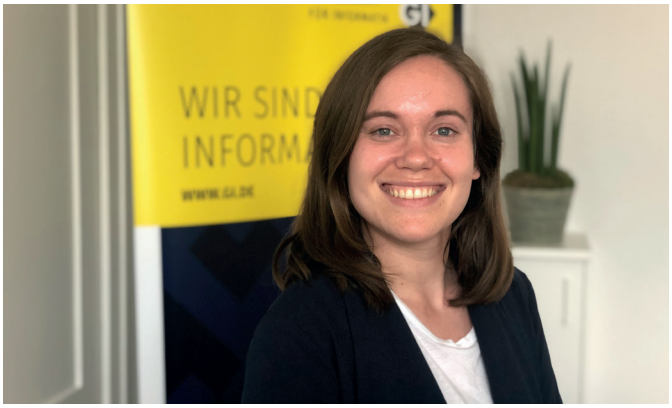
Dr. Jörg Bienert ist Mitgründer und Vorsitzender des Bundesverbandes Künstliche Intelligenz e.V. Gleichzeitig ist er Partner und CPO der Alexander Thamm GmbH, Deutschlands führendem Unternehmen für Data Science und KI. Davor war er u.a. Gründer von ParStream, ein Big-Data Startup mit Sitz im Silicon Valley, das 2015 von Cisco übernommen wurde.

AUSBLICK

MENSCH-TECHNIK-INTERAKTION FÜR DIGITALE SOUVERÄNITÄT

Nikolas Becker / Elisabeth Schauermann, Gesellschaft für Informatik

„Sind sie hiermit einverstanden?“ Internetnutzer*innen geben auf solche Fragen häufig ihr „OK“ ohne nur einen Blick in die Datennutzungserklärungen der jeweiligen Dienste zu werfen. Die Konsequenzen – umfangreiche Datensammlungen und die Einwilligung in die Verarbeitung ihrer personenbezogenen Daten – sind ihnen dabei häufig nicht klar. Warum ist das ein gesellschaftliches Problem und wie gehen wir es an?



Elisabeth Schauermann © GI

Nikolas Becker © GI

2018 etablierte die europäische Datenschutzgrundverordnung das Konzept der „informierten Einwilligung“ als Rechtsgrundlage für die Verarbeitung personenbezogener Daten. Sie reglementiert so die Rechte und Pflichten in der Interaktion von Datenverarbeitenden und Datensubjekten. In der Praxis stellen sich jedoch vielfältige Fragen zur konkreten technischen Ausgestaltung einer solchen Einwilligung, damit diese der Zuschreibung „informiert“ auch ernsthaft gerecht wird. Als Gesellschaft für Informatik nähern wir uns in zwei Forschungsprojekten der Beantwortung dieser Fragen an. Im Forschungsprogramm „Technik zum Menschen bringen“ hat sich das Bundesministerium für Bildung und Forschung (BMBF) daher zum Ziel gesetzt, Innovationen in der Mensch-Technik-Interaktion zu fördern, welche Nutzer*innen darin unterstützen, digitale Inhalte und ihre eigenen Daten informiert und mündig nutzen und verwalten zu können.

Auf Seiten der Nutzenden kann es zudem zu Akzeptanzproblemen kommen, weil sie in der Interaktion mit den Systemen nicht verstehen, welche personenbezogenen Daten über sie erfasst werden und welche Konsequenzen dies für sie mitbringt. Digitale Souveränität im Kontext der Mensch-Technik-Interaktion soll jedoch über die rechtliche Basis hinausgehen – es geht um die Steigerung von Kompetenzen im digitalen Raum und Instrumente, die Nachvollziehbarkeit erhöhen und dazu beitragen, kompetente Entscheidungen zu treffen. Die Gesellschaft für Informatik (GI) eint in ihren 20.000 Mitgliedern und 14 Fachbereichen enorme Expertise zu diesen Fragestellungen. Wir wollen seit 50 Jahren wissen, welche Antworten die Informatik auf die drängenden Fragen unserer Zeit bereithält.

Aus dieser Position wird sich die GI in den kommenden Jahren im Themenkomplex digitale Souveränität mit Projekten zur Mensch-Technik-Interaktion verorten. In einem interdisziplinären Verbund mit Partnern von der RWTH Aachen, der Universität Bremen, der Otto-Friedrich-Universität Bamberg, der Stiftung Digitale Chancen und Garmin Würzburg GmbH wollen wir untersuchen, welches Potenzial interaktive Datenschutzlösungen zur Steigerung der Souveränität von Smart-Wearables-Nutzer*innen haben.

Immer mehr Menschen nutzen Fitnesstracker, Smart Watches und ähnliche Technologien, die Bewegungsmuster und Vitalfunktionen aufzeichnen und auswerten. Besonders im Umgang mit sensiblen, persönlichen Gesundheitsdaten wollen wir Lösungen für informierte und reflektierte Nutzungsentscheidungen entwickeln und bereitstellen. Die Diskussionen um Tracking-Anwendungen und die „Datenspende-App“ des Robert Koch-Instituts zur Eindämmung der pandemischen Ausbreitung des Corona-Virus im Frühjahr 2020 zeigt einerseits, welcher gesellschaftliche Nutzen von derartigen Technologien ausgehen kann und andererseits, die Wichtigkeit informierter Nutzungsentscheidungen für eine sichere

und datenschutzkonforme Lösung.[24] Neben dem Bereich Gesundheit stehen auch Mobilität und „digitale Gesellschaft" im Fokus des Programms. Letztendlich soll bei allen Forschungsprojekten der Mensch im Mittelpunkt stehen.

Auch in der Arbeitswelt, insbesondere im Personalmanagement stellen sich viele Fragen zum digital-souveränen Umgang mit algorithmischen Entscheidungssystemen. In einem weiteren Forschungsprojekt werden wir daher Handlungsempfehlungen zur Verbesserung von Nachvollziehbarkeit und Beherrschbarkeit in KI-basierten Systemen am Beispiel der Steuerung kollaborativer Produktionsprozesse und individueller Arbeitskarrieren entwickeln. Die Studie wird durch das Bundesministerium für Arbeit und Soziales (BMAS) finanziert und entsteht in Zusammenarbeit mit dem Algorithm Accountability Lab an der TU Kaiserslautern, dem Institut für Rechtsinformatik an der Universität des Saarlandes, dem Fraunhofer-Institut für Experimentelles Software Engineering sowie der Stiftung Neue Verantwortung.[25]

Um diese vielfältigen Fragestellungen und noch zu entwickelnden Lösungsansätze zu integrieren, wollen wir gemeinsam mit der AlgorithmWatch gGmbH das „Netzwerk Digitale Souveränität" ins Leben rufen, in dem wir spannende Erkenntnisse für die interessierte Öffentlichkeit, die Politik und die Wirtschaft aufbereiten werden. Wir wollen den öffentlichen Diskurs fachlich fundiert anreichern und gleichzeitig eine Demokratisierung der entstehenden Information erreichen. Denn: In einer digitalisierten Gesellschaft brauchen wir vielfältige Lösungen und klare Ziele. Eines davon ist die Mündigkeit von Nutzer*innen.

Elisabeth Schauermann ist Referentin für Politik bei der GI, sie leitet das Projekt InViDas im Rahmen des Förderprogramms „Mensch-Technik-Interaktion für eine digitale Souveränität" des BMBF und ist Expertin in den Bereichen Internet Governance und partizipative Prozessgestaltung.

Nikolas Becker ist Referent für Politik bei der GI, er leitet das Projekt „Testing und Auditing von KI-Systemen" des BMAS und ist Experte in den Bereichen Digitalisierung und Nachhaltigkeit, Datenschutz und IT-Sicherheit.

24 Vgl. die Pressemitteilung der GI vom 09.04.2020: „GI kritisiert ‚Datenspende-App' des Robert-Koch-Instituts" https://gi.de/meldung/gi-kritisiert-datenspende-app-des-robert-koch-instituts

25 Weitere Informationen zum Projekt unter https://testing-ai.gi.de

DIGITALE SOUVERÄNITÄT IN ZEITEN EINER PANDEMIE

Christine Regitz / Anja Schaar-Goldapp, Sprecherinnen GI-Wirtschaftsbeirat

Wie ein Brennglas verdeutlicht uns die Corona-Krise 2020 die Zukunfts-Herausforderung für unsere Wirtschaft: Für viele Betriebe entscheidet die digitale Souveränität ihrer Mitarbeiter*innen maßgeblich darüber, wie hoch Produktivitätsverluste ausfallen, ob das Unternehmen dem internationalen Wettbewerb standhalten kann und ob es die Krise überstehen wird.

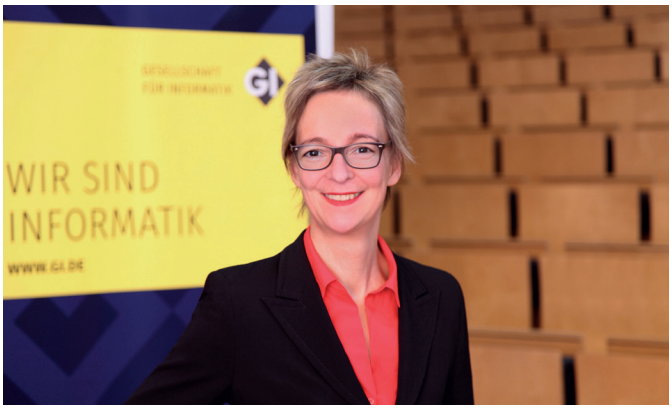
Ohne Vorwarnung werden Deutschlands Unternehmen im Frühjahr 2020 gezwungen, sich mit Fragen digitaler Arbeit auseinanderzusetzen. Um die Maßnahmen der Regierung gegen das Corona-Virus zu unterstützen und ihre Belegschaft zu schützen, ordnen zahlreiche Unternehmen kurzfristig die Einrichtung von Homeoffice-Arbeitsplätze an. Doch während die Kommunikation via E-Mail für viele mittlerweile zum normalen Büroalltag gehört, zeigt sich im permanenten Homeoffice schnell, dass wir digitalen Kompetenzen bisher zu wenig Bedeutung beimessen.

Reibungsverluste im Homeoffice

So sind digitale Tools der Arbeitsorganisation und Zusammenarbeit für viele noch Fremdworte. Stattdessen werden tausende E-Mails mit angehängten Textdateien versendet – Effizienz sieht anders aus. Und es stellen sich Fragen: Wie lassen sich die Kundendaten datenschutzkonform an die Kollegin zu Hause übermitteln? Und lässt sich die nervig-repetitive Aufgabe nicht mit wenigen Handgriffen automatisieren? Die Sprachlosigkeit, die diese Fragen selbst in den Chefetagen noch häufig hervorruft, verdeutlicht uns: In Deutschland besteht noch immer ein enormer Mangel an IT-Kompetenzen.

Eine Frage der IT-Sicherheit

Dabei ist digitale Souveränität auch eine Frage der IT-Sicherheit. Wenn Unwissen über die (Un)-Sicherheit unverschlüsselter Mailkommunikation herrscht, wenn der Umgang mit einem Passwortmanager nicht geübt ist und Firmengeheimnisse durch Metadaten nach draußen gelangen, dann wird deutlich, dass selbst eine gute IT-Abteilung wenig gegen fehlende Digitalkompetenz in der Breite ausrichten kann. Ob Signal, PGP oder MD5 – digitale Souveränität, verstanden als Fähigkeit zum selbstbestimmten Handeln und Entscheiden im digitalen Raum, erlaubt uns, Sicherheitsprobleme zu erkennen und die richtigen Werkzeuge auszuwählen. Ihr Mangel bedeutet hingegen ein permanentes Sicherheitsrisiko.



Christine Regitz © GI

Anja Schaar-Goldapp © GI

Digitale Souveränität ermöglicht Innovation

Doch es gibt Hoffnungsschimmer: Ebenfalls im Zuge der Corona-Krise veranstaltete die Bundesregierung den Online-Hackathon „Wir vs. Virus“. Ehrenamtliche Programmierer*innen, Hacker und Haecksen waren ein Wochenende lang aufgerufen, die Pandemie mit den Mitteln der Informatik zu bekämpfen. Im Rahmen des Wettbewerbs entstanden beispielsweise Apps, die lokale Gewerbetreibende in der Krise unterstützen oder selbstgebaute Beatmungsmaschinen für den heimischen 3D-Druck. Insgesamt beteiligten sich unglaubliche 28.000 Freiwillige an der gesellschaftlichen Hau-Ruck-Aktion. Das enorme Innovationspotenzial, das hier deutlich wird, könnte sich auch in deutschen Firmen und Organisationen wiederfinden. Denn digitale Souveränität bedeutet auch die Kompetenz, digitale Werkzeuge und Software-Bausteine in neuer Art und Weise zusammenfügen zu können.

Unser Bildungssystem ist gefragt

Um digitale Souveränität zu erreichen, müssen wir den Informatik-Unterricht in der Schule stärken und außerschulische Informatik-Bildungsangebote ausbauen. Mit dem Projekt Turing-Bus haben GI und Open Knowledge Foundation hier in den letzten Jahren gezeigt, wie sich Informatik-Grundlagen und ein selbstbestimmt-kritischer Umgang mit IT mit Spaß und Engagement vermitteln lassen. Lassen Sie uns hier ansetzen, und digitale Souveränität in unserem Bildungssystem verankern.

Christine Regitz ist Sprecherin des Wirtschaftsbeirats der GI du bei SAP weltweit verantwortlich für das Programm „Women in Tech“ sowie Mitglied des Aufsichtsrats.

Anja Schaar-Goldapp ist stellvertretende Sprecherin des GI-Wirtschaftsbeirats und Geschäftsführerin des Beratungsunternehmens Schaar-Goldapp Consulting GmbH.

IMPRESSUM

HERAUSGABE
Gesellschaft für Informatik e.V.
Spreepalais am Dom, Anna-Louisa-Karsch-Str. 2, 10178 Berlin

REDAKTION / GESTALTUNG
Geschäftsstelle Berlin der Gesellschaft für Informatik e.V.

STAND
Mai 2020

ÜBER DIE GESELLSCHAFT FÜR INFORMATIK E. V.

Die Gesellschaft für Informatik e.V. (GI) ist mit rund 20.000 persönlichen und 250 korporativen Mitgliedern die größte und wichtigste Fachgesellschaft für Informatik im deutschsprachigen Raum. Seit 1969 vertritt sie die Interessen der Informatikerinnen und Informatiker in Wissenschaft, Wirtschaft, öffentlicher Verwaltung, Gesellschaft und Politik. Mit 14 Fachbereichen, über 30 aktiven Regionalgruppen und unzähligen Fachgruppen ist die GI Plattform und Sprachrohr für alle Disziplinen in der Informatik. Die GI-Mitglieder binden sich an die Ethischen Leitlinien für Informatikerinnen und Informatiker der Gesellschaft für Informatik e.V. Weitere Informationen finden Sie unter www.gi.de.

GESELLSCHAFT FÜR
INFORMATIK E. V. (GI)

Geschäftsstelle Bonn

Wissenschaftszentrum

Ahrstr. 45

53175 Bonn

Tel.: +49 228 302-145

Fax: +49 228 302-167

E-Mail: bonn@gi.de

Geschäftsstelle Berlin

Spreepalais am Dom

Anna-Louisa-Karsch-Str. 2

10178 Berlin

Tel.: +49 30 7261 566-15

Fax: +49 30 7261 566-19

E-Mail: berlin@gi.de

gs-berlin@gi.de

www.gi.de

/informatikradar

/company/gesellschaft-fuer-informatik

/net/gi