erschienen in der FIfF-Kommunikation,
herausgegeben von FIfF e.V. - ISSN 0938-3476
www.fiff.de

Manuel Atug und Caroline Krohn

Nachhaltige Digitalisierung –

Zur Komplexität nachhaltiger Vergabe- und Förderpraxis für die digitale Transformation

Deutschland hinkt in der Digitalisierung hinterher und glänzt nicht als Vorbild: Überall scheitern Digitalisierungsprojekte. Interessant daran ist: Staatliche Projekte scheitern auch unter Mitwirkung von Wirtschaftsunternehmen und wissenschaftlichen Einrichtungen. Haben wir es hier in der Zusammenarbeit von staatlichen, semistaatlichen oder privaten Stellen mit einem strukturellen Problem zu tun? Was müsste passieren, um nachhaltigere Digitalisierungserfolge zu erzielen?

Der vorliegende Beitrag ist eine fachliche Einschätzung und Bewertung der AG Nachhaltige Digitalisierung (AGND). Auch wenn auf Gesetze eingegangen wird, handelt es sich hierbei nicht um einen juristischen Fachbeitrag, sondern um einen zivilgesellschaftlichen Debattenbeitrag. Die AGND ist eine Initiative, die es sich zum Ziel gesetzt hat, Digitalisierungsmaßnahmen in Politik, Wirtschaft, Wissenschaft und Gesellschaft in ihren Langzeitwirkungen zu betrachten und dabei die Selbstbestimmungsbedürfnisse des Menschen in den Mittelpunkt der Analysen stellt. Die Risikobetrachtung basiert auf dem Ansatz der Vermeidung von Technologieschulden für nachfolgende Generationen durch die Vernachlässigung der IT-Sicherheit.

Es gibt ein Phänomen, das sich „pervertierter Anreiz" (engl.: *perverse incentive*) nennt. Perversion ist ein lateinischer Begriff, der eine Verkehrung beschreibt, also mehr als eine Abweichung, im weitesten Sinne eine Umkehr. Wenn beispielsweise ein Mittel zum Zweck wird und gleichzeitig der Zweck das eigentliche Mittel, dann spricht man hier von einer Perversion. Eine Verkehrung eines Anreizes ist folglich eine Fehlleitung einer Anreizabsicht. Bekannt ist hier die Geschichte des sogenannten *Kobra-Effekts*, in der eine Inzentivierung eines Ziels dazu geführt hat, das Gegenteil zu erreichen: Als die Briten Indien kolonialisierten, riefen sie ein Kopfgeld auf jede getötete Kobra aus. Ziel war, die Anzahl der Kobras im Land zu reduzieren. Dies führte jedoch dazu, dass lokale Bauern anfingen, Kobras zu züchten, um diese dann zu töten und dadurch ihren Profit zu maximieren. Als die britische Administration dies erfuhr, strich sie das Kopfgeld und die Bauern ließen ihre Kobras lebend wieder frei. Im Ergebnis führte der Anreiz also zum Gegenteil dessen, worauf er ausgelegt wurde: Anstatt Kobras nachhaltig zu reduzieren, hat man sie sogar vermehrt (Dubner 2012).

Dieses Anreizsystem kann nicht als nachhaltig gewertet werden. Denn Nachhaltigkeit bedeutet, die langfristigen Effekte im Blick zu haben (Hauff 1987) – und Hebelwirkungen so zu setzen, dass die wirklich gewünschten Wirkungen erzielt werden können. Dies zu erzielen ist die Kernkompetenz politischer Rahmensetzung: Durch Finanzierungen unterschiedlicher Art Anreize zu setzen, gesellschaftliche Normen zu steuern und bestimmte Trends zu honorieren. Ein Beispiel hierfür sind öffentliche Ausschreibungen – sei es für Beschaffungen, Vergaben oder auch Förderungen.

Im Vergaberecht ist seit einigen Jahren eine besondere Bemühung zu beobachten, öffentliche Vergabe an konkrete Bedingungen zu knüpfen (HMWEVW 2021 u. a.). Auch dies ist unter anderem ein Anreizsystem: Wenn öffentliche Gelder beantragt werden, so müssen die Beantragenden beispielsweise Nachhaltigkeits- oder Diversitätsnachweise erbringen, die der politischen Linie der öffentlichen Hand entsprechen. Auf diese Weise setzt der Staat Impulse in die Wirtschaft und belohnt Privatunternehmen, die sich rechtskonform aufstellen – zunächst einmal nicht durch die Vergabe selbst, sondern vor allem bereits durch den Zugang zum Vergabeverfahren. Wer die genannten Nachhaltigkeits- und Diversitätskriterien nicht erfüllt, kann gar nicht erst an der Ausschreibung teilnehmen. Diese Kriterien anzusetzen, ist schwierig: So haben es Konzerne mit umfangreichen administrativen Strukturen leicht, bürokratischen Hürden dieser Art schnell gerecht zu werden, während kleinere Akteure, die am Markt zwar flexibler sein mögen, in der Unternehmensadministration solche Strukturen allerdings nicht so schnell schaffen können. Das ist ein Problem und kann zu einer Benachteiligung kleinerer und mittlerer Unternehmen in öffentlichen Ausschreibungen führen.

Was an Vergaben im Digitalen – beispielsweise im Bereich des Onlinezugangsgesetzes (OZG) und anderer Verwaltungsdigitalisierungs-Projekte – gänzlich fehlt, ist bislang ein Nachweis über *digitale* Sorgfaltspflichten, wie z. B. die Prävention von Supply-Chain-Attacken (Lieferkettenangriffe), den BSI Grundschutz für betriebene IT-Infrastrukturen etc. Wenn die BSI Grundschutz- oder eine ISO 27001-Zertifizierung der Dienstleistenden gelegentlich doch eingefordert wird, so fehlen dennoch fast durchgehend entsprechende Kontrollen und Sanktionen.

Mindestsicherheitsstandards als strukturelle Sicherung der Nachhaltigkeit in der Digitalisierung

Abseits der Vergabe: Durch Förderung als Steuerungsinstrument hat die Bundesregierung in hohem Umfang Wagniskapitalunterstützung für digitale Startups in Aussicht gestellt (BMWK 2022) – abermals jedoch ohne jegliche Auflage für Mindestsicherheitsstandards – weder in Bezug auf den Schutz von personenbezogenen Daten, noch in Bezug auf Informationssicherheit, beispielsweise in sensiblen politischen Vorgängen, geheimen Forschungsbereichen oder proprietären Geschäftsgeheimnissen. Im guten Willen, dem Trend zu entsprechen und sich agil und flexibel zu zeigen, transferieren also künftig Behörden, die Politik und die Wirtschaft sensible Geschäftsprozesse in wenig regulierte Startups, denen der Zugang zu Kapital oder zu Beauftragungen durch den Staat aus politischem Willen der Innovationsförderung heraus erleichtert werden soll.

Nur wenn wir eine Kultur des Wohlwollens gegenüber Gründer:innen zeigen – so die Logik – sind wir als Gesellschaft nachhaltig, weil: Fortschrittlich.

Ist es denn aber wirklich nachhaltig, wenn ein Staat Zugänge zu Finanzierungen, Förderungen oder Beschaffungen erleichtert, ohne darauf zu achten, dass ein Mindestmaß an digitaler Sicherheit eingehalten wird und ohne sicherzustellen, dass Daten nicht abfließen können und/oder abgegriffen werden?

Mit dem Inkrafttreten der EU-Datenschutzgrundverordnung (DSGVO) sollte es einen sehr stark an den Bürger:innenrechten orientierten Mindeststandard gerade für elektronische Datenverarbeitung geben. Auch wenn Unternehmen und Organisationen über Jahre den Erstellungsprozess beobachtet und begleitet hatten, kam die tatsächliche Implementierung wie ein Donnerhall über die inner- und außereuropäische Wirtschaft. Die Regelungen betreffen nämlich nicht nur die Unternehmen, deren Herkunft und Hauptsitz die Europäische Union ist, sondern alle, die im Europäischen Markt wirken.

Gleichzeitig wurde festgelegt, dass nicht Verbraucher:innen die Nachweispflicht über mögliche Datenschutzverletzungen erbringen müssen, damit die Aufsicht aktiv wird. Sondern Unternehmen müssen nachweisen, dass sie alles tun, das mögliche Datenabflüsse verhindert werden, dass Grundsätze der Datensparsamkeit und Datenvermeidungen sowie strenge Zweckgebundenheit der Datenverarbeitung eingehalten werden, dass es Offenlegungspflichten und zuverlässige Löschkonzepte gibt.

Anstatt dass die DSGVO in der europäischen Gesellschaft als Faktor der Nachhaltigkeit in der Digitalisierung gesehen wird, kämpft sie mit einer Reputation als Bürokratiemonster und Innovationshemmnis. Ganz unschuldig daran ist der Regulator selbst nicht: Die Rechtsprechung bzw. Rechtsdurchsetzung der DSGVO ist nicht zuletzt dadurch geschwächt, weil sie unter den 17 Aufsichtsbehörden unterschiedlich ausgelegt und entsprechend umgesetzt wird.

Für die technische und organisatorische Seite indes sind Risikobetrachtungen im Sinne und im Geiste der DSGVO durchaus eindeutiger: Ist eine IT-Infrastruktur für Kompromittierungen aller Art anfällig, so ist es wahrscheinlich, dass personenbezogene Daten in irgendeiner Form abhanden kommen, verfälscht und zweckentfremdet werden können. Und es gilt als sicher, dass durch das Potenzial an sich das Ziel des Datenschutzes durch mangelhafte Datensicherheit nicht garantiert werden kann, auch wenn Dokumentations- und Vertragspflichten formal erfüllt sind.

Der Nachweis, der hier im Hinblick auf Datensicherheit als Garant für den Datenschutz zu erbringen ist, ist im Artikel 32 der DSGVO verfasst: Es handelt sich dabei um die Dokumentation und die Verifizierbarkeit der *technischen und organisatorischen Maßnahmen* (TOMs). Hier befindet sich die DSGVO außerhalb des Juristischen und tief in den technischen Anforderungen des Informationsschutzes. Unternehmen und Organisationen müssen erklären, wie sie Daten verschlüsseln (sowohl bei der Übertragung als auch bei der Speicherung); sie müssen zeigen, wie sie die Berechtigungs- und Authentifizierungsprozesse steuern und vieles mehr.

Dass in einem Vergabeverfahren oder Förderungsverfahren die Einreichung der TOMs als Minimalnachweis verpflichtend wäre, wäre kein zusätzlicher bürokratischer Aufwand – wenn die Unternehmen denn ihre gesetzlich ohnehin schon geforderten Hausaufgaben tatsächlich machen.

Verhindert dies Innovationen? Nein, denn Innovationen – also Erneuerungen – bedeuten nicht Unbekümmertheit oder Nachlässigkeit. Neues, das Potenziale aufzeigt, das Probleme andersartig löst, das kreativ mit Herausforderungen umgeht – ist gut. Nachhaltig ist das Neue dann, wenn dies auch in einer Art geschieht, die verantwortungsvoll mit den treuhänderisch verwerteten Daten umgeht. Wir brauchen keine Problemlösung, die neue Probleme aufwirft. Eine Gesellschaft, in der Menschen durch Datenverlust und -missbrauch gefährdet werden, ist keine fortschrittliche.

Selbstverständlich bedeutet eine solche Forderung aber, dass es nicht nur darum gehen kann, die TOMs in einem Vergabeverfahren einzubringen. Der öffentliche Auftraggeber darf hier kein zahnloser Tiger sein. Es ist selbstverständlich erforderlich, dass die staatlichen Stellen von ihren Kontrollrechten Gebrauch machen. Strenggenommen verarbeiten Auftragnehmer:innen des Staates ja schließlich Daten in seinem Auftrag. Fahrlässigkeiten bis hin zu Missbrauch von Daten würden damit der Verantwortung des Auftraggebers zufallen.

Was ist zu tun? – Ein Vorschlag für einen Forderungskatalog zur nachhaltigen Digitalisierung im staatlichen Auftrag

Wie lassen sich also die Digitalisierung der Verwaltung, die Digitalisierung der Politik, die Digitalisierung der Wirtschaft, die Digitalisierung der Forschung und die Digitalisierung der Gesellschaft nachhaltig gestalten? Welche Stellschrauben müssten angefasst werden, um ein Selbstverständnis zu erzeugen, so dass Digitalisierungsvorhaben, die staatlich finanziert werden, den Standards entsprechen, die der Gesetzgeber in allen Sektoren legislativ fordert?

1. ***Das Vergaberecht anpassen***: Unternehmen und Institutionen, die ein digitales Produkt anbieten, um der öffentlichen

Hand zu dienen, müssen bei der Beantragung nachweisen, dass sie gewissenhaft mit ihrer IT-Infrastruktur, mit ihrer Software und mit ihren Datenbeständen (inklusive zukünftiger Datenbestände) sorgsam umgehen, also im Sinne der Datenvermeidung, Datensparsamkeit und des Datenschutzes. Dies gilt auch für die IT-Infrastruktur, die Software und die Datenbestände, die kundenseitig im öffentlichen Sektor betreut oder installiert werden.

2. ***Die Vergabepraxis anpassen:*** Auftragnehmer:innen des Staates müssen nicht nur proaktiv die Integrität ihrer Software, IT-Systeme und Daten nachweisen, sie müssen auch regelmäßig und effektiv kontrolliert werden. Hierfür braucht es Personal und Kontrollprozessstrukturen im öffentlichen Sektor, wie z. B. die Kartellämter oder die Rechnungshöfe. Diese müssen personell ausgestattet und befähigt werden, digitale Prozesse bei den Auftragnehmer:innen des Staates zu prüfen und zu bewerten (GDC 2021 & Stolton 2020).

3. ***Förderungen von Startups*** müssen an die Bereitschaft gebunden werden, einen erheblichen Anteil ihrer Ressourcen für Sicherheit und Datenschutz, besser noch: für Security-by-Design und Privacy-by-Design zu verwenden. Auch hier braucht der Staat eine weitreichende Begleitungs- und Kontrollbereitschaft. Die Digitalisierung von Geschäftsmodellen ist nur dann qualitativ hochwertig und damit schlussendlich auch nachhaltig, wenn sie eine deutliche Verbesserung der Datenintegrität herbeiführen als die Unternehmen und Organisationen, denen sie am Markt den Kampf ansagen. Nicht nur die Möglichkeit, in nichtregulierten Segmenten operieren zu können, sondern auch die Möglichkeit der staatlichen Zuwendungen sind Wettbewerbsvorteile, die an gesellschaftliche Verpflichtungen geknüpft sein müssen.

4. ***Forschungsförderung*** ist dann nachhaltig, wenn die Zusage von Projekten zur Förderung gesellschaftlich relevanter Digitalisierungsforschung nicht nur großen Populärtrends, wie KI oder Blockchain entsprechen, sondern allesamt durch den Filter der Informationssicherheit betrachtet werden. Die öffentliche Hand muss nicht nach Wirtschaftlichkeitskriterien agieren. Im Gegenteil: Dort, wo Wirtschaftlichkeit nicht greifen kann, wohl aber das öffentliche Interesse im gesamtgesellschaftlichen Sinne, ist der Staat gefragt. Hierzu gehört Grundlagenforschung. Hierzu gehören Vergabekriterien, die nicht Popularitätskriterien entsprechen müssen – und damit eine solide Grundlagenarbeit im Bereich der Digitalforschung.

5. ***Projektträgerschaften:*** Projektträger des Bundes sind Unternehmen, die im Auftrag der öffentlichen Hand Projektförderungen verwalten und teilweise sogar selbst in hoheitlicher Aufgabe Förderungen im Namen von Ministerien und anderen behördlichen Einrichtungen vergeben. Hier findet ein Auslagerung vom öffentlichen Sektor an diese Projektträger statt, die den Auftrag haben, nach den Förderkriterien des Staates einerseits – und im Rahmen ihrer Expertisen in Wirtschaftlichkeit und Fachlichkeit andererseits, Förderprojekte zu koordinieren und zu steuern (Fincompare 2019). Die Logik ist ein Offenbarungseid unzureichender digitalpolitischer Expertise – oder auch nur der mangelnden Digitalexpertise an sich – der öffentlichen Verwaltung. Man erhofft

sich nicht nur einen Effizienzgewinn in der Abwicklung der Vergabevorschriften, sondern auch eine Beurteilungsfähigkeit, die staatliche Stellen weder haben, noch sich mit den Bezugstabellen der öffentlichen Hand zunehmend leisten könnten. Von Breitbandausbau bis Digitalbildungsprojekten an Schulen ist alles dabei. Nachhaltigkeit wird hier nicht gewährleistet, denn nicht nur ist in der Kontrolle der Vergabemittel- oder Fördermittelempfänger:innen eine Stelle zwischengeschaltet (auf deren Kontrollpraxis man sich behördlich zu verlassen scheint), sondern auch die Projektträger an sich werden bestenfalls in der Ausschreibung nach Sicherheitsgesichtspunkten mit ausgewählt – hiernach jedoch nie wieder geprüft – auch dann nicht, wenn sie hoheitlich im Auftrag der öffentlichen Stelle agieren und tatsächlich selbst Gelder vergeben. Die Nachhaltigkeit geböte also, eine eigene staatliche Kompetenz aufzubauen und marktgerecht zu entlohnen, um sich die Steuerungs- und Kontrollfähigkeiten nicht von Einrichtungen abnehmen zu lassen (und sich dabei von diesen abhängig zu machen), die eben nicht das öffentliche Interesse bzw. das Gemeinwohlinteresse priorisiert im Blick haben.

6. ***Nachhaltigkeit in der Digitalisierung*** *der öffentlichen Verwaltung und in deren Zusammenarbeit mit Wirtschaftsunternehmen* krankt an der mangelnden (zeitlichen und fachlichen) *Kompetenz* und entsprechend den mangelnden *Handlungsfähigkeiten* des *Personals*. Nicht nur muss die richtige Digitalisierungsexpertise massiv eingekauft und aufgestockt werden – was nur mit kompetitiven Gehältern zu regeln ist – sondern die richtigen Expert:innen an den richtigen Stellen sind kontinuierlich weiterzubilden und es ist auf sie zu hören. Natürlich reicht es nicht, Digitalisierung und ihre Auswirkungen zu verstehen. Ohne Verfahrensfachexpertise im behördlichen Bereich fehlt ein erheblicher Teil zum

Gelingen digitaler Projekte – sei es in Verwaltungsstrukturen oder durch Verwaltungsstrukturen bestellt oder gefördert.

7. ***Das Aufbauen und Vorhalten digitaler Expertise*** ist darum schwierig, weil eine digitale Perspektive technisch sein kann, nicht aber zwingend sein muss. Digitalexpertise besteht auch darin, *Technologiefolgen* soziologisch, psychologisch, kulturell, etc. zu betrachten. Hier sind interdisziplinäre Planungsteams hilfreich – auch interministeriell. Wichtig ist aber hier eindeutig die institutionalisierte Verflechtung mit der *Zivilgesellschaft*, die ihrerseits zwar ebensowenig hoheitliche Aufgaben haben darf wie Projektträger. Doch hält die Zivilgesellschaft gemeinwohlorientierte Expertisen vor, die in Anhörungen und Ausschüssen in noch stärkerem Maße als heute Einzug finden müssen, um auch rein wirtschaftlich orientierten Partikularinteressen an Digitalisierungs-Maßnahmen entgegenwirken zu können. Den Expert:innen der Verwaltung käme dann eine orchestrierende Funktion zu, die die Eingaben evaluiert und mit Blick auf die politischen Vorgaben zusammenbringt.

8. ***Im Sicherheitsbereich*** ist das Zusammenwirken von privaten und öffentlichen Akteuren besonders sensibel und gefährdet die Nachhaltigkeit in jedwedem Digitalisierungsbestreben stark. Sicherheit ist sowohl außen als auch innen eine hoheitliche Aufgabe des Staates. Gleichzeitig ist jedoch die Abhängigkeit von wirtschaftlicher Forschung und ihrer gewinnorientierten Vermarktung besonders hoch. Die Abhängigkeit ergibt sich dabei aus der Dringlichkeit zu handeln, um das öffentliche Bedürfnis nach physischer Sicherheit, also der Unversehrtheit, zu gewährleisten. Gleichzeitig ist der Sicherheitssektor einer, in dem die Beamt:innen im Staatsauftrag ihrerseits bereits nicht gut bezahlt werden und berufsmäßig durchaus ihre eigene physische und mentale Unversehrtheit riskieren, was verständlicherweise ein weiteres Kriterium für verheißungsvolle Digitallösungen ist. Nachhaltigkeit besteht hier dezidiert darin, die staatliche Selbstmäßigung im Blick zu behalten, um Bürger:innenrechte den Investigations- und Verbrechensbekämpfungsinteressen nicht unterzuordnen. Die gesellschaftsnormative und dann auch rechtliche Aushandlung der Verhältnismäßigkeit muss abermals auf interdisziplinäre Strukturen gestützt werden, um Kontrolleur:innen kontrollieren zu können, allerdings ohne allzu große Effizienzeinbußen in Kauf zu nehmen. Der Unterschied zur nicht-nachhaltigen Gesellschaft besteht darin, dass wir heute die Rechte zukünftiger Generationen nicht beeinträchtigen dürfen. Und weitreichende Zugriffskompetenzen des Staates lassen sich nun einmal schwer wieder zurückfahren. Wo Daten entstehen, entsteht Begehren. Die organisierte Kriminalität ist den Sicherheitskräften in demokratischen Ländern leider oftmals einen Schritt voraus (Schönbohm 2013) – und hat leichtere Bedingungen, Menschen zu kompromittieren, als diejenigen, die dies zu verhindern suchen. Gleichsam achten der nachhaltige Staat und die nachhaltige Gesellschaft darauf, die Freiheit und Selbstbestimmung der unbescholtenen Bürger:innen möglichst weit zu erhalten.

9. ***Im Bereich Kritischer Infrastrukturen*** kann nur dann eine wirklich nachhaltige Digitalisierung gewährleistet werden, wenn verstanden wird, dass IT-Sicherheit – bedingt durch die fortschreitende Digitalisierung in Industriesteueranlagen – immer wesentlicher für die Safety wird, also den Schutz des Menschen vor der Maschine. Mit der Digitalisierung wird das Einwirken der IT-Sicherheit, und insbesondere das Ausbleiben selbiger, auf die Safety immer relevanter. Schlussendlich wird also die IT-Sicherheit – und damit Security-by-Design und Privacy-by-Design – zur Frage des Menschenschutz in der Prozessautomatisierung und in Produktionsumgebungen von kritischen Infrastrukturen (Atug 2020).

10. ***Nachhaltige Digitalisierung*** in der *Interaktion zwischen der Politik, der öffentlichen Verwaltung auf allen horizontalen und vertikalen Ebenen, der Wirtschaft, der Forschung und der Zivilgesellschaft* gelingt nur dann, wenn alle Anspruchsgruppen im Aushandlungsprozess ihre jeweiligen Rollen kennen und pflegen. Es muss klar sein, wer Entscheidungen trifft, nach welchen Kriterien sie getroffen werden; welche Kriterien angesetzt werden müssen, um am Geschehen teilzunehmen; wer wie kontrollieren darf und muss, etc. Das Hauptkriterium für gemeinwohlorientierte und damit nachhaltige Digitalisierung ist es, jeden Menschen zu mehr und einfacherer Teilhabe zu befähigen und gleichzeitig vor jedwedem Missbrauch, vor allem durch die Kompromittierung seiner Daten, zu schützen.

Fazit

Die Nachhaltigkeit im Bemühen, Deutschland, seine Politik, seine Verwaltung und seine gesamtgesellschaftlichen Strukturen dem Zeitalter der Digitalisierung zuzuführen, kann nur darin bestehen, alle Anspruchsgruppen einzubinden und den Blick auf die Langzeitfolgen einer digitalen Maßnahme zu richten. Datenbestände sind toxisch, also ein Sicherheits- und ein Haftungsrisiko bergend, wenn sie nicht zielgerichtet gespeichert und verarbeitet werden (Adshead 2017 und Greene 2017). Ihr Vorhalten mag für staatliche, akademische oder wirtschaftliche Fragestellungen praktisch sein, doch gefährdet dies in letzter Konsequenz den Schutz des Menschen. Menschen zu schützen, indem man der möglichen Kompromittierung ihrer personenbezogenen Daten oder ihrer digitalen intellektuellen Werte frühzeitig beikommt, ist die Essenz digitaler Nachhaltigkeit.

Nachhaltige Digitalisierung lässt sich von staatlicher Seite nur dann mit Beständigkeit durchsetzen, wenn die öffentliche Hand bei sich selbst anfängt, das heißt: wenn sie ihre Vergabepraxis in allen Fragen öffentlich-privater Maßnahmen in allen digitalisierten Bereichen nachhaltig, also mit Blick auf den Menschenschutz gestaltet. Wenn also jede Förderung die Sicherheit von Infrastruktur, Software und Datenverkehr als unumstößliche Kernbedingung enthält – sei es für Förderprojekte, für Forschungsprojekte, für Startupförderungen oder auch Unternehmensrettungen, dann wäre im Hinblick auf die Nachhaltigkeit all dieser digitalen Maßnahmen und Komponenten viel gewonnen.

Unabdingbar für den öffentlichen Sektor ist die radikale Erhöhung von Expert:innenwissen innerhalb der Verwaltung, um die Urteilsfähigkeit über digitale Maßnahmen nicht länger auslagern zu müssen. Hierzu gehört auch die kontinuierliche Weiterbildung der Staatsangestellten und Beamt:innen und die Definition des orchestrierenden Auftrags ministerieller Expert:innen.

Eine Zusammenarbeit mit dem privaten Sektor muss geschehen, doch müssen hoheitliche Aufgaben allein bei der staatlichen Seite verbleiben.

Nachhaltig zu digitalisieren bedeutet, sich bei jeder Maßnahme, bei jedem Hebel und jedem Anreizsystem zu fragen, ob gesichert ist, dass wir durch technische Nachlässigkeiten, toxische Datenbestände und Schwachstellenschulden zukünftige Generationen beeinträchtigen. Die Beeinträchtigung erfolgt durch Netzwerkeffekte: jede Komponente kann zu einer Schwächung gesellschaftlicher und individueller Resilienz beitragen. Darum muss der Staat zuallererst in seinem Agieren dafür Sorge tragen, dass Sicherheit stets und zwingend mitgedacht wird.

Referenzen

Adshead Antony (2017) Toxic data: What it is and how to find it and deal with it, in: Computer Weekly, 16. Mai 2017, URL https://www.computerweekly.com/podcast/Toxic-data-What-it-is-and-how-to-find-it-and-deal-with-it, abgerufen am 10. August 2022.

Atug Manuel (2020) Ohne Security keine Safety in Kritischen Infrastrukturen – Begriffliche Trennung und Zusammenführung, in: AG KRITIS Blog, 03. April 2020, URL https://ag.kritis.info/2020/04/03/ohne-security-keine-safety-in-kritischen-infrastrukturen-begriffliche-trennung-und-zusammenfuehrung/, abgerufen am 10. August 2022.

Bundesministerium für Wirtschaft und Klimaschutz (BMWK) (2022) Die Start-up-Strategie der Bundesregierung, 27. Juli 2022, URL https://www.bmwk.de/Redaktion/DE/Dossier/Digitalisierung/start-up-strategie.html, abgerufen am 10. August 2022.

Detsch Claudia (2021) Interview mit Prof. Dr. Arndt Sinn: „Drogen können wir. Geldwäsche nicht.“, in: IPG-Journal, 01. März 2021, URL https://www.ipg-journal.de/interviews/artikel/organisierte-kriminalitaet-4990/, abgerufen am 10. August 2022.

Dubner Stephen J (2012) The Cobra Effect: A New Freakonomics Radio Podcast, 11. Oktober 2012, URL https://freakonomics.com/podcast/the-cobra-effect-2/, abgerufen am 10. August 2022.

FinCompare (2019) Projektträger – wer sind sie und was ist ihre Aufgabe?, 30. April 2019, URL https://fincompare.de/projekttraeger, abgerufen am 10. August 2022.

Hauff Volker Hg. (1987) Unsere gemeinsame Zukunft : der Brundtland-Bericht der Weltkommission für Umwelt und Entwicklung, 1. Auflage, Greven: Eggenkamp.

Hessisches Ministerium für Wirtschaft, Energie, Verkehr und Wohnen (2021) HVTG – Vergabe von öffentlichen Aufträgen in Hessen erleichtert, Pressemitteilung vom 06.07.2021, URL https://wirtschaft.hessen.de/Presse/Vergabe-von-oeffentlichen-Auftraegen-in-Hessen-erleichtert, abgerufen am 10. August 2022.

Humer Stephan (2014) Kriminalität im Netz: Wie das organisierte Verbrechen das Internet nutzt, in: golem.de, 4. Dezember 2014, URL https://www.golem.de/news/kriminalitaet-im-netz-wie-das-organisierte-verbrechen-das-internet-nutzt-1412-110899.html, abgerufen am 10. August 2022.

Gesellschaft für Datenschutz und Compliance (2021) Kelber fordert mehr Ressourcen für die Datenschutzaufsichtsbehörden, August 2021, URL https://www.forum-dc.de/2020/08/30/kelber-fordert-mehr-ressourcen-fuer-die-datenschutzaufsichtsbehoerden/, abgerufen am 10. August 2022.

Greene Travis (2017) Rethinking Toxic Data in Light of GDPR, in: Security Week. Cybersecurity News, Insights and Analytics, 01. Februar 2017,URL https://www.securityweek.com/rethinking-toxic-data-light-gdpr, abgerufen am 10. August 2022.

Schönbohm Arne (2013) Cybercrime: Lukratives Geschäft für die Organisierte Kriminalität, in: Aus Politik und Zeitgeschichte, 12. September 2013, URL https://www.bpb.de/shop/zeitschriften/apuz/168916/cybercrime-lukratives-geschaeft-fuer-die-organisierte-kriminalitaet/, abgerufen 10. August 2022.

Stolton Samuel (2020) Zu wenig Mittel: Die Durchsetzung der DSGVO ist ausbaufähig, in: EURACTIV.com, 25. Mai 2020, URL https://www.euractiv.de/section/digitale-agenda/news/zu-wenig-mittel-die-durchsetzung-der-dsgvo-ist-ausbaufaehig/, abgerufen am 10. August 2022.

Upadek Carsten (2014) Organisierte Kriminalität. Cybercrime, in: WDR Nachrichten, Erstveröffentlichung: 2014, letzte Aktualisierung: 31. Januar 2018, URL https://www1.wdr.de/nachrichten/landespolitik/pwiecybercrime100.html, abgerufen am 10. August 2022.

Wikipedia (2021) „Projektträger“, in: Wikipedia – Die freie Enzyklopädie, Bearbeitungsstand: 30. November 2021, URL https://de.wikipedia.org/wiki/Projekttr%C3%A4ger, abgerufen am 10. August 2022.

Caroline Krohn und Manuel Atug

Caroline Krohn ist IT-Sicherheitsexpertin für nachhaltige Wirtschaft und sichere Digitalisierung. Krohn ist unter anderem Gründerin und Sprecherin der *Arbeitsgemeinschaft Nachhaltige Digitalisierung* (AGND).

Manuel Atug ist IT-Sicherheitsexperte für kritische Infrastrukturen und unter anderem als *@HonkHase* im Netz aktiv.