Kompetenzzentrum
Öffentliche IT

KOMPETENZZENTRUM ÖFFENTLICHE INFORMATIONSTECHNOLOGIE

DIGITALE SOUVERÄNITÄT

Gabriele Goldacker

IMPRESSUM

Autoren:
Gabriele Goldacker

Gestaltung:
Reiko Kammer

Herausgeber:
Kompetenzzentrum Öffentliche IT
Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS
Kaiserin-Augusta-Allee 31, 10589 Berlin
Telefon: +49-30-3463-7173
Telefax: +49-30-3463-99-7173
info@oeffentliche-it.de
www.oeffentliche-it.de
www.fokus.fraunhofer.de

ISBN: 978-3-9818892-2-2

1. Auflage November 2017

Dieses Werk steht unter einer Creative Commons Namensnennung 3.0 Deutschland (CC BY 3.0) Lizenz.
Es ist erlaubt, das Werk bzw. den Inhalt zu vervielfältigen, zu verbreiten und öffentlich zugänglich zu machen, Abwandlungen und Bearbeitungen des Werkes bzw. Inhaltes anzufertigen sowie das Werk kommerziell zu nutzen.
Bedingung für die Nutzung ist die Angabe der Namen der Autoren sowie des Herausgebers.

Die Fotografien laufen unter der Lizenz:
https://creativecommons.org/publicdomain/zero/1.0/deed.de

Bildnachweise:

Seite 1: bonoflex
https://pixabay.com/de/paris-d---arc-golden-statue-d-636263/
Seite 6: Bernhard_Staerck
https://pixabay.com/de/reiter-skulptur-lissabon-denkmal-1753885/
Seite 11: strecosa
https://pixabay.com/de/denkmal-statue-menton-frankreich-2920175/
Seite 14: AKuptsova
https://pixabay.com/de/katharina-ii-catherine-2-denkmal-1341811/
Seite: 17: skeeze
https://pixabay.com/de/skulptur-1050387/
Seite 19: HOS70
https://pixabay.com/en/horse-fisherman-fishermen-1320045/
Seite 21: rihaij
https://pixabay.com/de/reiterstandbild-kunst-statue-1522570/
Seite 23: Selomedia
https://pixabay.com/de/august-der-starke-dresden-denkmal-433333/
Seite 24: ErikaWittlieb
https://pixabay.com/de/queen-elizabeth-statue-k%C3%B6nigin-455746/
Seite 26: reginaspics
https://pixabay.com/de/essen-riesenrad-ruhrgebiet-nrw-1999614/
Seite 29: werner22brigitte
https://pixabay.com/de/denkmal-metall-fahrer-pferde-51660/
Seite 30: travelspot
https://pixabay.com/de/potsdam-reiterstandbild-park-pferd-2383813/
Seite 34: Stevebidmead
https://pixabay.com/de/statue-bronze-die-mall-london-357311/

VORWORT

Es gibt viele, sehr unterschiedliche Definitionen für »digitale Souveränität« – und alle haben ihre Berechtigung! Für umfassende digitale Souveränität von Bürgern, Unternehmen, öffentlicher Verwaltung, Parlament, Regierung und der Gesellschaft insgesamt müssen viele verschiedene Voraussetzungen erfüllt sein.

Sinngemäß ist digitale Souveränität unter anderem …

- selbstbestimmtes Handeln und Entscheiden von Menschen, Unternehmen und anderen Institutionen im digitalen Raum, wobei sie die Hoheit über ihre eigenen Sicherheits- und Datenschutzinteressen behalten sollen[1]
- die Möglichkeit eines Menschen, digitale Medien souverän nutzen zu können, was neben der individuellen Fähigkeit (vgl. Medienkompetenz) auch notwendige, äußere Rahmenbedingungen (z. B. sicherer Transportweg, geeignete Angebote, regulatorische Maßnahmen) umfasst[2]
- die Fähigkeit, die Vertrauenswürdigkeit, Integrität, Verfügbarkeit der Datenübertragung, -speicherung und -verarbeitung durchgängig kontrollieren zu können[3]
- die Selbstbestimmung von Dateneigentümern über die Nutzungsbedingungen für ihre Daten[4]
- über eigene Fähigkeiten auf internationalem Spitzenniveau bei digitalen Schlüsseltechnologien, entsprechenden Diensten und Plattformen zu verfügen und darüber hinaus in der Lage zu sein, selbstbestimmt und selbstbewusst zwischen Alternativen leistungsfähiger und vertrauenswürdiger Partner zu entscheiden, sie bewusst und verantwortungsvoll einzusetzen und sie im Bedarfsfall weiterzuentwickeln und zu veredeln[5]

Diese Definitionen zeigen ein breites Spektrum von Voraussetzungen auf, die für digitale Souveränität gegeben sein müssen. Die meisten gesellschaftlichen Gruppen, die sich mit digitaler Souveränität beschäftigen – u. a. Wirtschaftsverbände, Bildungsorganisationen, Forschungsinstitute – fokussieren sich auf eine einzige Definition. Dies führt manchmal auch zu Missverständnissen. Deshalb wollen wir das gesamte Spektrum digitaler Souveränität vorstellen und die teilweise sehr speziellen, teilweise aber auch konvergierenden Voraussetzungen für umfassende digitale Souveränität beleuchten.

Wir fassen die Definitionen in einem Satz zusammen: **Digitale Souveränität ist die Summe aller Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können.**

Mögliche Schwachstellen bei der Umsetzung digitaler Souveränität gibt es viele, Bedrohungen können von Wirtschaftsunternehmen, Kommunikationspartnern oder auch staatlichen Stellen ausgehen. Lassen Sie sich also von uns mitnehmen bei der Betrachtung, was Grundschulcurricula und Geheimdienstaktivitäten gemein haben können.

Ihr Kompetenzzentrum Öffentliche IT

---

[1] https://www.polyas.de/wahllexikon/digitale-souveraenitaet.

[2] https://de.wikipedia.org/wiki/Digitale_Souver%C3%A4nit%C3%A4t.

[3] ZVEI: »Diskussionspapier Digitale Souveränität«, Juni 2015.

[4] Fraunhofer-Gesellschaft: »White Paper Industrial Data Space, Digitale Souveränität über Daten", 17.08.2016.

[5] Bitkom: »Digitale Souveränität, Positionsbestimmung und erste Handlungsempfehlungen für Deutschland und Europa.«, 12.05.2015.

SELBSTSTÄNDIG, SELBSTBESTIMMT UND SICHER IN DER DIGITALEN WELT.

INHALTSVERZEICHNIS

1.	**Thesen**	**5**
2.	**Was macht digitale Souveränität aus?**	7
2.1	Digitale Souveränität individueller IT-Nutzer	7
2.2	Digitale Souveränität institutioneller IT-Nutzer	8
2.3	Digitale Souveränität von IT-Produzenten und -Dienstleistern	9
2.4	Gesamtgesellschaftliche digitale Souveränität	9
3.	**Wie kann mehr digitale Souveränität erreicht werden?**	12
3.1	Individuelle digitale Souveränität	12
3.2	Institutionelle digitale Souveränität	20
3.3	Digitale Souveränität von IT-Produzenten und -Dienstleistern	24
3.4	Gesamtgesellschaftliche digitale Souveränität	27
3.5.	Notwendige Kooperation der Akteure	31
4.	**Handlungsempfehlungen**	**32**

1. THESEN

Digitale Souveränität muss aus vielen Perspektiven betrachtet werden.
Neben Datensouveränität, Cybersicherheit und Beherrschung der digitalen Kerntechnologien ist beispielsweise auch die erfolgreiche IT-Nutzung ein Aspekt digitaler Souveränität.

Digitale Souveränität erreichen wir nur gemeinsam.
Bürgern[6], Wirtschaft und Staat kommen bei der digitalen Souveränität jeweils eigene Rollen und Aufgaben zu, die nicht vollständig durch Leistungen der anderen Akteure kompensiert werden können.

Digital souverän zu handeln bedeutet oft, wohlinformiert einen Kompromiss einzugehen.
Ob bei der Entscheidung, eine Cloud- oder eine autarke Lösung einzusetzen, oder bei der Wahl des Webbrowsers: Meist gibt es nicht die eine, für alle Nutzer und alle Einsatzfälle optimale Lösung, sondern nur solche, die individuell mehr oder weniger Aufwand und höhere oder niedrigere Risiken verursachen. Dann hilft nur, sich zu informieren, zu vergleichen, abzuwägen und die verbleibenden Risiken im Auge zu behalten.

Digital souveränes Verhalten läuft ohne entsprechende (quelloffene) Produkte ins Leere.
Ob Suchmaschine oder Router – bei kommerziellen Anforderungen stehen meist nur sehr wenige und oft keine Produkte mit optimaler Souveränitätsunterstützung zur Verfügung. Bei nicht quelloffener Software nehmen sich auch Nutzer, die selbst nicht in der Lage sind, den Quellcode auf Korrektheit und das Nichtvorhandensein unerwünschter Funktionen zu prüfen, die Möglichkeit, von Dritten auf entsprechende Mängel hingewiesen zu werden.

Technische Entwicklungs- und Produktionskompetenz verpufft ohne Konkurrenzfähigkeit und Kundenakzeptanz.
Die Fähigkeiten, IT-Kerntechnologien zu entwickeln und zu produzieren bzw. als Dienstleistung anzubieten, sind zwar notwendige Voraussetzungen für gesamtgesellschaftliche digitale Souveränität, lassen sich aber entsprechende Ergebnisse nicht erfolgreich am Markt platzieren, bleiben diese Fähigkeiten wirkungslos.

Wer öffentliche Clouds und Plattformen nutzt, gibt digitale Souveränität preis.
Clouds und Plattformen sind mindestens ebenso lohnende Ausspähziele wie Datenleitungen und internationale Router. Unverschlüsselt in einer von Dritten betriebenen Cloud oder Plattform gespeicherte oder verarbeitete Daten sind gegenüber dem Betreiber technisch nicht geschützt. Ein Ausfall der Cloud/Plattform oder der notwendigen Kommunikationsdienste führt zu (temporärer) Unverfügbarkeit der Daten/Dienste.

Schengen-Routing und die Euro-Cloud spiegeln digitale Souveränität nur vor.
Fremde Rechtssysteme können Hersteller und Betreiber trotzdem zur Herausgabe von Daten verpflichten oder Angreifer auch Datenleitungen und -speicher auf EU-Territorium anzapfen. Angriffe auf Datenspeicher finden ohnehin oft via Datenkommunikation von beliebigen Standorten aus statt.

Datensouveränität ist kein Ersatz für Datenschutz – und dieser kein Ersatz für Privatsphäre.
Auch von informierten Bürgern bereitwillig zur Verfügung gestellte Daten müssen geschützt werden. Jedes erfasste oder erhobene personenbezogene Datum stellt selbst bei idealem Datenschutz einen Eingriff in die Privatsphäre der betroffenen Person dar und muss sich daher auf einen objektiven, gesellschaftlich anerkannten Bedarf abstützen.

Echokammern schränken die Informationsfreiheit[7] ein.
Viele Anbieter, die Kenntnisse über den konkreten Nutzer haben, präsentieren ihm z. B. Nachrichten, Meinungsäußerungen oder Werbung, von denen angenommen wird, dass sie ihn besonders ansprechen. Damit kann für den Nutzer der Eindruck entstehen, diese Nachrichten und Meinungen seien repräsentativ bzw. die beworbenen Produkte besonders nachgefragt.

Klassische Programmierkenntnisse tragen nicht zur digitalen Souveränität normaler IT-Nutzer und -Beschaffer bei.
Wichtiger sind Grundkenntnisse zu Konzepten (z. B. serverbasierte Datenverarbeitung), zum Umgang mit eigenen und fremden Inhalten, zur Cybersicherheit und zu den Geschäftsmodellen hinter Diensten und Produkten.

[6] Wenn wir in diesem Dokument von Menschen als Nutzern, Bürgern usw. reden, sind damit stets Personen jedweden Geschlechts gemeint.

[7] In diesem Dokument wird der weiter gefasste Begriff der Informationsfreiheit zugrunde gelegt, der nicht nur Daten der öffentlichen Hand betrifft.

2. WAS BESTIMMT DAS MASS DER DIGITALEN SOUVERÄNITÄT?

Digitale Souveränität ist keine Eigenschaft bzw. kein Zustand, die bzw. der gegeben oder nicht gegeben ist. Vielmehr setzt sich ihr Gesamtmaß aus zahlreichen Facetten zusammen, die wiederum jeweils in unterschiedlichen Abstufungen vorliegen können.

Wie bereits die Thesen zeigen, gibt es viele Perspektiven, um digitale Souveränität zu bewerten. Eine hilfreiche Herangehensweise betrachtet unterschiedliche gesellschaftliche Rollen:

- den einzelnen Menschen (als Privatperson, Bürger oder Arbeitnehmer),
- Unternehmen, Verwaltung und Regierung, wenn sie Nutzer von IT sind,
- IT-Produzenten und -Dienstleister sowie
- das Gemeinwesen als Ganzes.

Bei jeder dieser Rollen stehen zum Teil völlig unterschiedliche Fähigkeiten, Kenntnisse und (Wahl-)Möglichkeiten im Fokus.

2.1 DIGITALE SOUVERÄNITÄT INDIVIDUELLER IT-NUTZER

Die digitale Souveränität des einzelnen Menschen bezieht sich im Wesentlichen auf seine Fähigkeiten und Möglichkeiten bezüglich dreier Aspekte:

Nutzung (und Beschaffung)

- Digitaltechnik, Computeranwendungen und IT-Dienstleistungen (z. B. Internetzugang) zur Erreichung von Primärzielen (z. B. Information, Unterhaltung, Sozialkontakt, Erbringung von Arbeitsleistung) erfolgreich, effizient und rechtssicher einsetzen zu können
- IT sicher nutzen zu können
- einen angemessenen Zugang zu Ressourcen der Digitalisierung (Hardware, Software, Internetzugang …) zu haben

Daten

- über die Herausgabe, Erfassung, Speicherung, Nutzung und Verarbeitung eigener Daten umfassend und qualifiziert entscheiden bzw. mitbestimmen zu können
- sein Recht, sich aus allgemein zugänglichen (digitalen) Quellen ungehindert zu unterrichten[8] (Informationsfreiheit), wirksam ausüben zu können
- die Glaubwürdigkeit[9] und Relevanz digitaler Daten, Informationen, Nachrichten und Dokumente angemessen bewerten zu können

Gesellschaftliche Gestaltung

- sich über die (möglichen) Auswirkungen der Digitalisierung auf vielfältige Aspekte der Gesellschaft – z. B. Arbeit, Freizeit, Einkommensverteilung, Geschlechterrollen … – ein sachliches Bild machen zu können
- sich in die gesellschaftliche Gestaltung der Digitalisierung einbringen zu können

Erfolgreiche IT-Nutzung bedeutet, die angestrebten direkten Ziele der Nutzung (also z. B. eine Websuche oder auch die Gestaltung und Platzierung einer eigenen Website) zu erreichen. Zur effizienten IT-Nutzung gehört, die wesentlichen nützlichen Funktionen der verwendeten Hard- und Software zu kennen und gezielt einzusetzen. Bei der rechtssicheren IT-Nutzung geht es in erster Linie darum, Rechte Dritter nicht unbeabsichtigt zu verletzen und sich der Konsequenzen einer Verletzung bewusst zu sein. Insbesondere bei Internet-Nutzung kann Rechtssicherheit unter anderem Grundkenntnisse der allgemeinen Persönlichkeitsrechte (z. B. Recht Dritter an ihrem eigenen Bild) oder des Urheberrechts erfordern.

Die sichere IT-Nutzung hingegen betrifft den Selbstschutz. Sie umfasst den Schutz gegen materielle Gefahren, die sich direkt aus der IT-Nutzung ergeben, beispielsweise den Schutz gegen versehentliche Datenzerstörung, aber auch gegen betrügerische Internethändler. Ebenso umfasst die sichere IT-Nutzung den Schutz der eigenen Persönlichkeitsrechte, z. B. gegen Ausspähen oder unerwünschte Profilbildung.

---

[8] »Grundgesetz der Bundesrepublik Deutschland«, Artikel 5, Absatz 1.

[9] Zur Vertiefung siehe auch: Petra Hoepner: »Digitale Glaubwürdigkeit«, ÖFIT-Whitepaper, Kompetenzzentrum Öffentliche IT, Fraunhofer FOKUS, Berlin, 1. Auflage Oktober 2017, http://www.oeffentliche-it.de/publikationen?doc=70454&title=Digitale+Glaubw%C3%BCrdigkeit.

Rollen im Zusammenhang mit digitaler Souveränität

Der Schutz eigener Persönlichkeitsrechte hat einen engen Bezug zur Datensouveränität, bei der es um das gezielte, informierte Bereitstellen eigener Daten geht. Auch hier stehen die personenbezogenen bzw. personenbeziehbaren Daten im Vordergrund. Datensouveränität[10] umfasst aber alle eigenen Daten. Dazu gehören die nicht öffentlichen Daten, die die eigene Person betreffen, selbst erzeugte Daten (so z. B. auch die Urlaubsfotos, die nur Landschaft zeigen, aber bei guter Qualität einen materiellen Wert für Kalenderverlage darstellen können) und nicht öffentliche sonstige Daten, die man rechtmäßig erworben bzw. erhalten hat. Nicht immer kann man allerdings über alle eigenen Daten völlig frei verfügen. Um eine öffentliche Leistung zu erhalten oder eine Ware geliefert zu bekommen, müssen bestimmte Daten zur Verfügung gestellt werden. In beiden Fällen eröffnet dies den Empfängern aber nicht das Recht der beliebigen Nutzung dieser Daten.

Der souveräne Umgang mit Daten, Informationen und Dokumenten »aus dem Netz« wird umso wichtiger, je mehr sich die Informationsbeschaffung auf das Internet verlagert. Dies bedeutet, (weitgehend) ungefiltert auf Datenquellen zugreifen zu können, aber auch, bei der expliziten wie impliziten Nutzung von Datenmaklern (z. B. Suchmaschinen bzw. Nachrichtenportalen) ein kritisches Bewusstsein dafür zu haben, was in welchem Umfang und in welcher Rangfolge präsentiert wird. Dazu gehört, in angemessenem Umfang in der Lage zu sein, Falschmeldungen und Ähnliches zu erkennen und die persönliche und gesellschaftliche Bedeutung von Nachrichten einzuordnen.

»Die Digitalisierung durchdringt alle Lebensbereiche« heißt es in vielen Veröffentlichungen. Gerade weil diese Aussage stimmt, ist es wichtig, sich sachlich über die Möglichkeiten und die Auswirkungen der Digitalisierung informieren und den gesellschaftlichen Wandel aktiv mitgestalten zu können. Dazu gehören zunächst angemessen aufbereitete Informationsangebote der Interessengruppen (einschließlich des Staates und seiner Organe). Für die Mitgestaltung sind vielfältige Organisations- und Partizipationsmöglichkeiten bis hin zu offenen politischen Prozessen erforderlich. Diese Möglichkeiten können klassisch gestaltet sein, sollten sich aber zunehmend auch selbst IT zunutze machen.

2.2 DIGITALE SOUVERÄNITÄT INSTITUTIONELLER IT-NUTZER

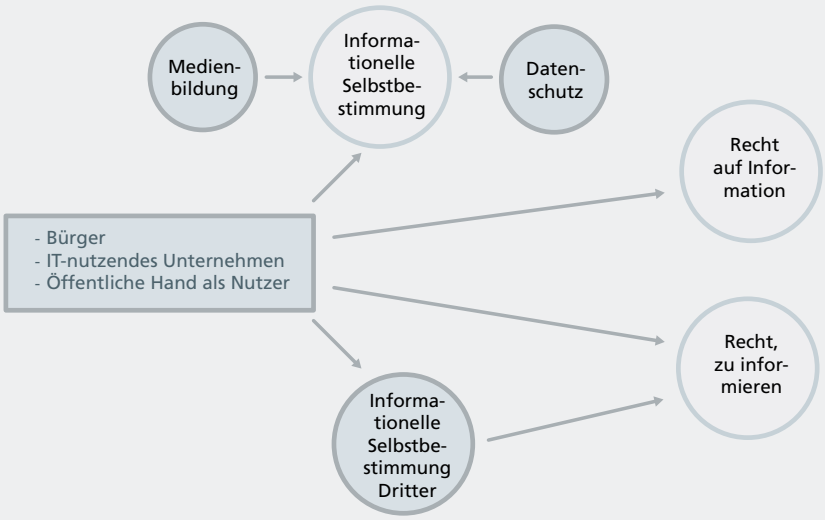
Die digitale Souveränität von Unternehmen, öffentlicher Verwaltung, politischen Gremien und gesellschaftlichen Organisationen[11] in der Rolle als IT-Nutzer umfasst zunächst alle Aspekte der individuellen digitalen Souveränität von IT-Nutzern übertragen auf eine gesamte Institution.

Ein wesentlicher Aspekt institutioneller digitaler Souveränität ist der angemessene Auftritt im Internet, sowohl durch Webseiten und Internetdienste als auch bei der Beteiligung der Mitarbeiter/Mitglieder an der Internetkommunikation. Bei privaten Nutzern entscheiden die Existenz bzw. Nichtexistenz eines Auftritts nur über Bekanntheit und Auffindbarkeit, die Inhalte und die Art der Präsentation über Sympathie oder Ablehnung. Bei Institutionen kann beides für wirtschaftlichen bzw. sonstigen institutionellen Erfolg entscheidend sein.

Beim Aspekt der sicheren Nutzung tritt im Zusammenhang mit möglicher Ausspähung neben den Schutz der Persönlichkeitsrechte der bedienenden Menschen fallweise der Schutz sensibler Daten der Institution: z. B. Arbeitsergebnisse (in Form von Daten und Dokumenten), Umsatzzahlen oder persönliche bzw. wirtschaftliche Daten Dritter (Kundendaten, Mitgliederdaten …).

[10] Datensouveränität ist eine Facette der digitalen Souveränität.

[11] Unter gesellschaftlichen Organisationen werden z. B. Wirtschafts- und Arbeitnehmerverbände oder gemeinnützige Vereine zur Freizeitgestaltung verstanden.



Facetten und Abhängigkeiten der digitalen Souveränität von IT-Nutzern

Hinzu kommt der Aspekt der IT-Steuerung bis hin zur digitalen Governance[12], d. h. die Fähigkeit, die IT-Ausstattung und den IT-Einsatz bedarfsgerecht zu planen und zu organisieren, einen stabilen und effizienten Betrieb zu gewährleisten sowie die Digitalisierung der Institution planen, steuern und bewerten zu können. Dieser Aspekt wird umso wichtiger und betrifft umso mehr Teile und Mitarbeiter der Institution, je stärker IT beispielsweise auch in klassischen industriellen und handwerklichen Produktionsbereichen zum Einsatz kommt.

2.3 DIGITALE SOUVERÄNITÄT VON IT-PRODUZENTEN UND -DIENSTLEISTERN

IT-Produzenten (Hard- und Software) und -Dienstleister tragen mittelbar zur digitalen Souveränität von Personen und Institutionen und unmittelbar zur gesamtgesellschaftlichen digitalen Souveränität bei. Sie sind in der Regel ebenfalls IT-Nutzer, weshalb auch für sie die Aspekte individueller und institutioneller digitaler Souveränität relevant sind.

Einige Aspekte kommen speziell hinzu bzw. erhalten eine erweiterte Bedeutung:

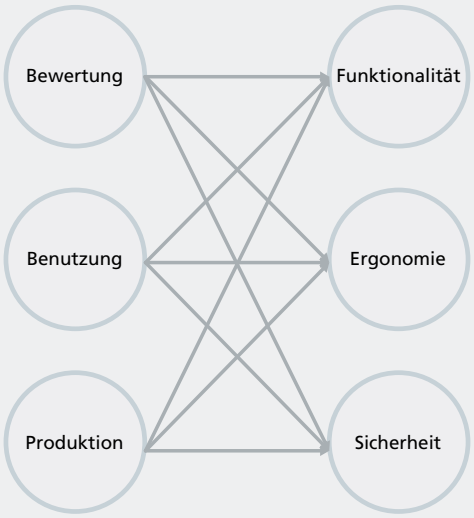
- **Entwurfs- und Produktionssouveränität**: die Fähigkeit und Möglichkeit, die angestrebten Produkte und Dienstleistungen zu realisieren
- **Marktsouveränität**: die Möglichkeit, mit den Produkten und Dienstleistungen im fairen Wettbewerb auf den angestrebten Märkten bestehen zu können

[12] Zu Begriffsbestimmung und vertiefter Betrachtung siehe M. Stemmer: »Digitale Governance. Ein Diskussionspapier«, Kompetenzzentrum Öffentliche IT, Fraunhofer FOKUS, Berlin, Juni 2016, http://www.oeffentliche-it.de/publikationen?doc=45209&title=Digitale+Governance+-+Ein+Diskussionspapier.

2.4 GESAMTGESELLSCHAFTLICHE DIGITALE SOUVERÄNITÄT

Bei der Betrachtung der gesamtgesellschaftlichen digitalen Souveränität müssen verschiedene Aspekte teilweise orthogonal zueinander betrachtet werden, die wir hier zunächst identifizieren und zueinander in Beziehung setzen, um den Umfang des Gesamtkomplexes abzustecken:

- die **innere digitale Souveränität** als Gesamtheit der digitalen Souveränität aus individueller, institutioneller und Produzenten-/Anbieterperspektive aller gesellschaftlichen Teile und Gruppen, gepaart mit der Fähigkeit von Staat und Verwaltung, die digitale Souveränität zielführend zu gestalten (und nötigenfalls auch zu lenken oder zugunsten allgemein akzeptierter höherer Güter teilweise einzuschränken)
- die **nach außen gerichtete digitale Souveränität**, die darauf abzielt, die Gesellschaft gegen Eingriffe in die digitale Souveränität (einschließlich des schleichenden Verlustes derselben) durch wirtschaftliche oder äußere politische Einflüsse zu schützen und möglichst die Abhängigkeit der Gesellschaft von Wirtschaftsunternehmen und anderen Staaten in Bezug auf IT-Komponenten – Hardware und Software – und in Bezug auf IT-Dienstleistungen – insbesondere Plattformen und Clouddienste – zu verringern
- die **digitale Souveränität im technischen bzw. Dienstleistungsbereich**, die beschreibt, in welchem Umfang die Gesellschaft, als Ganzes betrachtet, in der Lage ist, nachgefragte bzw. Erfolg versprechende IT-Komponenten selbst zu entwickeln und zu produzieren bzw. entsprechende IT-Dienstleistungen anzubieten
- die **organisatorische digitale Souveränität**, die bestimmt, in welchem Maß die digitale Souveränität unabhängig von anderen Staaten bzw. marktbestimmenden Wirtschaftsunternehmen durchgesetzt werden kann



- die **wirtschaftlich bestimmte digitale Souveränität** als Maß dafür, ob die digitale Souveränität im technischen und im Dienstleistungsbereich unter wirtschaftlichen Gesichtspunkten konkurrenz- und durchsetzungsfähig ist, aber auch dafür, ob die Gesellschaft sich die selbst gesteckten oder von ihr erwarteten Digitalisierungsziele wirtschaftlich leisten kann
- die **gesellschaftliche Gestaltung der Digitalisierung**, die Chancen und Risiken, Stärken und Herausforderungen für die Gesellschaft durch die Digitalisierung identifiziert und unter Einbeziehung aller gesellschaftliche Gruppen diskutiert, nach fairen Lösungen sucht und die Digitalisierung in einem iterativen, reflektierenden Prozess umsetzt

Wechselbeziehungen gibt es beispielsweise zwischen innerer und nach außen gerichteter digitaler Souveränität, die auch vom jeweiligen Gesichtspunkt abhängen: Befindet sich die Bundesrepublik zum Beispiel bei bestimmten Fragen in Übereinstimmung mit den anderen EU-Staaten, so sind diese Fragen Aspekte der inneren digitalen Souveränität der EU. In anderen Fragen kann ein Dissens mit anderen EU-Mitgliedern bestehen, dann bedarf es gegebenenfalls nationaler Schutzmaßnahmen gegen diese anderen Staaten bzw. gegen das Verhalten von Wirtschaftsunternehmen aus diesen Staaten, um das in Deutschland gewünschte Schutzniveau sicherzustellen.

Auch bei hoher digitaler Souveränität im technischen und im Dienstleistungsbereich kann die organisatorische digitale Souveränität gering sein, wenn z. B. notwendige staatenübergreifende Kommunikation nur bei Verzicht auf bestimmte Datenschutzrechte möglich ist oder wenn eine Kooperation mit fremden Produkten oder Dienstleistungen stets nur durch eigene Anpassungen an diese Produkte bzw. Dienstleistungen ermöglicht werden kann.

3. WIE KANN MEHR DIGITALE SOUVERÄNITÄT ERREICHT WERDEN?

Die gebotenen Maßnahmen zur Schaffung und Erhöhung digitaler Souveränität sind je nach Perspektive teilweise sehr unterschiedlich, ebenso die jeweils verantwortlichen Akteure. Andererseits gibt es aber auch erhebliche Gemeinsamkeiten.

3.1 INDIVIDUELLE DIGITALE SOUVERÄNITÄT

Nur wenn neben Wissen zur guten und sicheren IT- und Mediennutzung sowie zur Datensouveränität auch entsprechende Produkte bzw. Dienstleistungen und ein zeitgemäßer und technikgerechter Rechtsrahmen, treten, die zudem die Informationsfreiheit unterstützen, ist digitale Souveränität tatsächlich umsetzbar.

3.1.1 Allgemeinbildung

In Schule und Berufsausbildung sowie in Einzelaspekten bereits in der vorschulischen Bildung, muss ein breites, altersgerechtes Basiswissen zu Aspekten der Digitalisierung vermittelt werden.[13] Dazu gehören:

- **Techniknutzung:** Handhabung von IT-Komponenten (Hardware, Betriebs- und Anwendungssoftware, Internetdienste), Grundkenntnisse zu Basiskonzepten netzbasierter Kommunikation und Datenverarbeitung (z. B. digitale Identitäten, Verbindungen (Sessions), Client-Server-Systeme …)
- **Mediennutzung:** u. a. zielgruppengerechte Aufbereitung eigener Inhalte; effizientes Suchen nach benötigten Informationen; Beurteilung der Glaubwürdigkeit von Daten bzw. Datenquellen (Stichwort »Fake News«[14]), Beurteilung der persönlichen und gesellschaftlichen Relevanz von Nachrichten, Vertrauenswürdigkeit von Kommunikationspartnern und Datenanbietern (als Vorsorge gegen Phishing[15] oder auch Grooming[16]), Authentizität von Kommunikationspartnern, Datenanbietern und Datenquellen; elementares Urheberrecht, Strafrecht (Mobbing, Verleumdung, Stalking …)
- **Sicherheit und Datensouveränität:** gezielter Selbstschutz z. B. gegen Datenverlust, Daten- und Identitätsdiebstahl[17], Überwachung, Bewegungs-, Gewohnheits- und Neigungsprofiling, soziale und wirtschaftliche Übervorteilung; Datenschutzrecht
- **mögliche gesundheitliche Folgen der IT-Nutzung:** von Schlafmangel und Unkonzentriertheit bis zur Computersucht

Im Hinblick auf Datensouveränität ist es notwendig, ein Grundverständnis zu vermitteln, welche typischen Formen der Verhaltensaufzeichnung (Cookies, Positionslogging …) es gibt und welches Wissen aus den aufgezeichneten Daten gewonnen werden kann.

Besonderes Augenmerk, speziell bei Kindern und Jugendlichen, bedürfen der Aufbau und die Stärkung des Selbstschutzes gegen soziale und wirtschaftliche Übervorteilung, von der sexuellen Ausnutzung in sozialen Netzen bis zu Kostenfallen bei vermeintlich günstigen Online-Spielen.

Für alle sozialen und Altersgruppen jenseits von Schule und Berufsausbildung sind aktuelle, bedarfs- und zielgruppengerechte Schulungsangebote notwendig. So nennen nach einer Erhebung aus 2016[18] 41 Prozent der Privathaushalte ohne Internetzugang »keine ausreichenden Kenntnisse« als einen Grund. Angesichts des sehr unterschiedlichen Einstiegsniveaus sind differenzierte Kurse erforderlich, die an die Alltagswelt und die zu erwartende IT-Nutzung der Adressaten anknüpfen. Je nach der individuellen Situation muss Basiswissen bis hin zu spezifischem berufsbezogenem Wissen vermittelt werden.

---

[13] Siehe dazu auch: Nicole Opiela, Mike Weber: »Digitale Bildung – Ein Diskussionspapier«, Kompetenzzentrum Öffentliche IT, Fraunhofer FOKUS, Berlin, September 2016, http://www.oeffentliche-it.de/publikationen?doc=45209&title=Digitale+Governance+-+Ein+Diskussionspapier.

[14] Fake News: Vorsätzliche Falsch- oder dekontextualisierte Nachrichten, oft zur Meinungsbeeinflussung.

[15] Phishing: Das Erschleichen sensibler Daten zwecks Missbrauchs derselben, z. B. Kontodaten.

[16] Grooming: Das Ansprechen von Kindern und Jugendlichen durch Erwachsene mit dem Ziel sexueller Handlungen.

[17] Identitätsdiebstahl: z. B. Diebstahl von Authentifizierungsinformationen, die es einem Angreifer ermöglichen, Transaktionen (Online-Käufe, -Überweisungen …) im Namen des Opfers durchzuführen.

[18] Statistisches Bundesamt: »Wirtschaftsrechnungen – Private Haushalte in der Informationsgesellschaft -Nutzung von Informations- und Kommunikationstechnologien«, 16.12.2016, https://www.destatis.de/DE/Publikationen/Thematisch/EinkommenKonsumLebensbedingungen/PrivateHaushalte/PrivateHaushalteIKT2150400167004.pdf?__blob=publicationFile.

Besonders bei bildungsfernen Bevölkerungsgruppen und Spät-einsteigern können mittels niederschwelliger Angebote wie Selbsthilfegruppen (»Senioren helfen Senioren«) oder Computerpaten – direkt oder online – auch Menschen erreicht werden, die vor kommerziellen Kursen oder der Volkshochschule zurückschrecken.

Die vielfach geforderten Programmierkenntnisse können heutzutage zu den Kulturtechniken gezählt werden. Für den souveränen und sicheren Umgang mit IT sind sie jedoch für bloße IT-Nutzer ähnlich unbedeutend wie es die Fähigkeit, einen Motor zusammenzubauen, für das erfolgreiche und sichere Fahren eines Automobils ist.

Um die gesellschaftlichen Auswirkungen der Digitalisierung sachgerecht bewerten und die Digitalisierung mitgestalten zu können, sind schulische Angebote, z. B. im gesellschaftswissenschaftlichen Unterricht, notwendig, ebenso aber auch selbstständige Bildung unter Zuhilfenahme digitaler wie analoger Informationsquellen. Wer sich aktiv an der Gestaltung der Digitalisierung beteiligen möchte, braucht dazu auch technisches Basiswissen, vor allem jedoch die Fähigkeit zu argumentieren und sich an den verschiedensten Meinungsbildungs- und Entscheidungsformaten – von der Diskussionsveranstaltung bis zu Online-Abstimmungen – angemessen zu beteiligen.

3.1.2 Nutzungsfreundliche Hard- und Software

Individuelle (und institutionelle) digitale Souveränität kann erheblich gesteigert werden, wenn die eingesetzte Hard- und vor allem die Software nutzungs- und konfigurationsfreundlich gestaltet ist. Beispiele sind:

– Geräteschnittstellen für Energieversorgung und Datentransfer sowie die über letztere verwendeten Datenformate sollten herstellerübergreifend einheitlich (standardisiert) sein, um Interoperabilität zu gewährleisten.[19] Die Anschlüsse sollten zudem eine gut erkennbare und leicht verständliche Kennzeichnung haben. Konfigurationseinstellungen (wie z. B. der Flugmodus) müssen sich schnell und ohne Fehlbedienungsgefahr vornehmen lassen.
– Software muss in erster Linie ergonomisch gestaltet sein, beispielsweise sollte der Nutzer Bedienelemente leicht erkennen können und dort finden, wo er sie erwartet (also den Absenden-Button direkt hinter einem Eingabefeld). Software sollte bei Anforderung durch den Nutzer ausführliche Bedienungshinweise liefern. Sie muss sich leicht entsprechend den Bedürfnissen des Nutzers konfigurieren lassen (z. B. Schriftgröße und -font, Anpassung an Bildschirmgröße), unabhängig davon, ob sie auf dem Gerät des Nutzers oder im Wesentlichen an einem anderem Ort (z. B. »in der Cloud«) ausgeführt wird.

3.1.3 Angemessene und nutzerfreundliche Updates

Für Universalsoftware wie Betriebssysteme und Webbrowser für PCs und Laptops sind Funktions- und Sicherheitsupdates im 2-Wochen-Rhythmus inzwischen der Normalfall. Folgt der Nutzer der an sich sinnvollen Empfehlung, die Software aus Sicherheitsgründen stets aktuell zu halten, ist damit nicht selten erheblicher Aufwand verbunden, wenn beispielsweise Einstellungen des Nutzers nicht automatisch übernommen werden (und dies womöglich nicht einmal dokumentiert ist) oder Zusatzkomponenten (wie Browser Add-ons) nicht mehr kompatibel sind. In beiden Fällen kann die Unterstützung der Privatsphäre durch die Software oder gar die Angriffssicherheit des gesamten Gerätes erheblich sinken und somit die Datensouveränität (weiter) eingeschränkt werden.

[19] Vergleiche (auch zu anderen wesentlichen Aspekten): FZI Forschungszentrum Informatik/Accenture GmbH/Bitkom Research GmbH: »Kompetenzen für eine Digitale Souveränität«, Auftraggeber: Bundesministerium für Wirtschaft und Energie, Juni 2017, https://www.bmwi.de/Redaktion/DE/Publikationen/Studien/kompetenzen-fuer-eine-digitale-souveraenitaet.html.

In erster Linie ist es Aufgabe der Hersteller der Universalsoftware, die Sicherheits- und Privatsphäreeinstellungen der Nutzer zu respektieren und auch über Updates hinweg aufrechtzuerhalten. Da dies nicht immer technisch möglich ist, würde eine Verpflichtung, entsprechende Änderungen zu dokumentieren, den Nutzern zumindest die notwendige Unterstützung für ihr diesbezügliches eigenverantwortliches Handeln bieten.

Für viele preisgünstige mobile Geräte – von Smartphones bis zu den zunehmend eingesetzten IoT[20]-Geräten – werden hingegen gar keine Betriebssystemaktualisierungen erstellt und so die sichere IT-Nutzung verhindert. Hier scheint ein regulativer Eingriff geboten, zumal unsichere Geräte für die weitere Verbreitung von Angriffen benutzt werden können.

3.1.4 Angriffsresistente, Backdoor[21]-freie Komponenten

Je größer die Funktionsvielfalt und die Flexibilität einer Hard- oder Softwarekomponente sind, desto schwieriger ist es, sie schwachstellenfrei zu realisieren. Deshalb kann es vorteilhaft sein, Komponenten einzusetzen, die nur über den notwendigen Funktionsumfang verfügen. Backdoors, seien es für die eigentliche Funktionalität überflüssige Schnittstellen oder konfigurationsunabhängige Nutzerkonten bzw. Passwörter, bieten – selbst wenn sie mit guter Absicht oder gar aufgrund rechtlicher Vorgaben geschaffen wurden – stets zusätzliche Angriffsmöglichkeiten. Angriffsmöglichkeiten über Backdoors können kaum proaktiv eingeschränkt werden. Angriffe hingegen bleiben häufig längere Zeit unentdeckt, da sie nicht zu Auffälligkeits- oder Fehlermeldungen führen.

Quelloffene Software bietet gegenüber nicht quelloffener Software zumindest theoretisch die Möglichkeit einer vollständigen Überprüfung auf programmiertechnisch schwache, überflüssige bzw. nicht funktionsrelevante Teile. Während eine vollständige Überprüfung mit zunehmender Komplexität der Software mehr und mehr an intellektuelle und Aufwandsgrenzen stößt, kann oft bereits eine gezielte Teilüberprüfung kritische Schwachstellen aufdecken.

Bei der Nutzung mehrerer Softwareprodukte desselben Herstellers, die Schnittstellen untereinander besitzen (z. B. zur Erhöhung des Komforts), können Fehler oder unerwünschte Funktionen in bereits einem der Produkte alle diese Produkte kompromittieren.

3.1.5 Technische, organisatorische und rechtliche Unterstützung von Datensouveränität und Informationsfreiheit

Hard-/Software und IT-Dienstleistungen müssen ihren Teil zur Datensouveränität beitragen, indem transparent, zweckgebunden und von den Betroffenen mitbestimmt mit persönlichen Daten umgegangen wird.[22]

Die Unterstützung von Datensouveränität und Informationsfreiheit bedingt vielfältige Elemente, was hier nur exemplarisch gezeigt werden kann.

Wesentlich, insbesondere für ungeübte und wenig IT-affine Nutzer, sind privatsphärenfreundliche Grundeinstellungen[23] bei Hard- und Software auf allen Ebenen (Betriebssystem, Firewall,

[20] IoT: Internet of Things, Internet der Dinge. Geräte, die Umgebungsparameter erfassen oder physische Prozesse steuern und dabei vornehmlich mit anderen IoT-Geräten kommunizieren.

[21] Backdoor: Bewusst geschaffene, zusätzliche, meist undokumentierte und vom Nutzer unerwünschte Funktionalität einer Komponente.

[22] Zur Vertiefung siehe auch: Petra Hoepner: »Datenschutz und Technik – Ein Informationspapier«, Kompetenzzentrum Öffentliche IT, Fraunhofer FOKUS, Berlin, April 2017, http://www.oeffentliche-it.de/publikationen?doc=66590&title=Datenschutz+und+Technik+-+Ein+Informationspapier.

[23] Vgl: Sachverständigenrat für Verbraucherfragen (SVRV): »Digitale Souveränität – Gutachten des Sachverständigenrats für Verbraucherfragen«, Juni 2017, https://www.bmjv.de/SharedDocs/Downloads/DE/PDF/SVRV_Gutachten_Digitale-Souveraenitaet.pdf?__blob=publicationFile&v=2.

Anwendungen …). Zudem ist besonders wichtig, dass für eine Überwachung geeignetes Zubehör wie Kameras, Mikrofone und GPS[24]-Empfänger klare Funktionsanzeigen besitzt und man es nicht unbeabsichtigt einschalten kann. Allerdings werden laufend neue Trackingmechanismen[25] entwickelt, die auch bisher als nicht überwachungsrelevant angenommene Sensoren und Aktuatoren[26] einbeziehen. Zumindest bei älteren Geräten fehlen dann oft die entsprechenden Abschaltmöglichkeiten und Funktionsanzeigen. Browsersoftware sollte komfortable Konfigurationsmöglichkeiten (z. B. direkt über die Symbolleiste) für das domänen-, website- und webseitenspezifische temporäre und permanente Zulassen bzw. Blockieren von Cookies enthalten, ohne dass dafür zusätzliche Module installiert werden müssen.

IT-Komponenten – z. B. Webseiten, Anwendungen, Betriebssysteme –, die persönliche Daten vom Nutzer abfragen oder Verhaltensdaten des Nutzers (z. B. in Cookies) aufzeichnen, müssen die Notwendigkeit dieser Daten erläutern können.[27] Werden bestimmte Daten nur gespeichert, um den Komfort des Nutzers zu erhöhen (beispielsweise, damit er die Daten nicht mehrfach eingeben muss), sollte die eigentliche Funktion auch dann – natürlich mit entsprechendem Komfortverlust – zur Verfügung stehen, wenn der Nutzer die Speicherung dieser Daten nicht zulässt. Die Erfassung von nicht funktions- oder komfortrelevanten Daten darf nur erfolgen, wenn der Nutzer explizit zustimmt. Nur so kann der Nutzer souverän entscheiden, ob er bereit ist, die Daten für die beabsichtigten Zwecke zur Verfügung zu stellen. Dies setzt natürlich auch voraus, dass Daten nicht für andere als die autorisierten Zwecke benutzt (Zweckbindung) oder mit unzulässig erweiterten Nutzungsrechten weitergegeben werden. Anonymisierung oder Pseudonymisierung vor der Verwendung für nicht explizit autorisierte Zwecke ist bei Datensätzen, die eine Vielzahl individueller Merkmale oder ungewöhnliche Merkmalskombinationen enthalten, schwierig. Um Personenbeziehbarkeit dauerhaft auszuschließen, insbesondere wenn eine Verknüpfung mit anderen, dieselbe Person betreffenden Datensätzen nicht ausgeschlossen werden kann, sind komplexe Maßnahmen erforderlich. Insofern kann auch die Verarbeitung anonymisierter oder pseudonymisierter Daten einen Eingriff in die Datensouveränität darstellen.

Problematisch ist, dass meist sehr weitreichende Rechte von den Nutzern eingeholt werden. Im Regelfall ist völlig intransparent, welche Daten und Mechanismen für welchen Zweck benötigt werden. Die Nutzer stimmen dann zu, weil sie ansonsten Nachteile bis hin zum Nichterreichen ihrer Ziele befürchten.

Wird zudem jeweils die Zustimmung der Nutzer zur Erfassung vieler einzelner Daten bzw. zum Einsatz vieler verhaltenserfassender Mechanismen abgefragt, neigen die Nutzer dazu, spätestens nach einigen Abfragen stets ohne Prüfung zuzustimmen, weil sie der Zeitaufwand für die – im Hinblick auf das angestrebte Ziel unproduktiven – Abfragen stört.

---

[24] Global Positioning System: satellitenbasiertes System zur Positionsbestimmung.

[25] Tracking: Verfolgung der Bewegung eines Objektes im geografischen Raum, auf Webseiten, in und zwischen Websites …

[26] Aktuator: Komponente, die ihre Umgebung mechanisch, akustisch … beeinflusst, z. B. ein Lautsprecher.

[27] Siehe dazu »Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz«, »Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr« und »Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)«, http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32009L0136, http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:31995L0046, http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679.

PRIVATSPHÄRE IN DER DIGITALEN WELT AUFRECHTERHALTEN.

Auf diese Weise verkehren sich wohlmeinende Informations- und Schutzmechanismen – wie z. B. nach der Datenschutz-Grundverordnung[28] vorgesehen – in die gegenteilige Wirkung, da im Ergebnis weit mehr Rechte erteilt werden als notwendig.

Noch völlig unbefriedigend gelöst ist die technisch-organisatorische Umsetzung, wenn Nutzer generell oder im Einzelfall der Aufzeichnung personenbezogener Daten nicht zustimmen. Bei der Speicherung entsprechender Daten in Cookies beispielsweise werden die Nutzer oft lediglich informiert, dass Cookies gesetzt werden und dass der bloße Aufruf der Webseiten aus Sicht des Anbieters bereits als Zustimmung gewertet wird. Da gleichzeitig bereits Cookies gesetzt werden, kann sich der Nutzer dieser nur durch eine Umkonfiguration seines Browsers entledigen und dies auch nur dann gezielt tun, wenn er zuvor Namen und Ursprungsdomäne der Cookies in Erfahrung bringen konnte, da vielfach gerade Verhaltensdaten in Cookies anderer Domänen gespeichert werden. Das Setzen der »Do-not-Track«-Browsereinstellung führt nicht in allen Fällen zum gewünschten Erfolg, da die Beachtung freiwillig ist. Das explizite Setzen von Cookies gegen nutzungsbasierte Werbung[29] wird zwar von einer Reihe von Unternehmen unterstützt, ist aber aufwändig und kann weder proaktiv für zukünftig hinzukommende Unternehmen noch generell vorgenommen werden. Zudem kollidiert dieses Verfahren mit dem Wunsch von Nutzern, alle Cookies am Ende der Browsersitzung zu löschen.

Angesichts der Datenflut im digitalen Raum ist jeder ständig auf eine Vorauswahl durch andere angewiesen, seien es Suchmaschinen, (quasi-)journalistische Angebote oder Tagesnachrichten auf den Einstiegsseiten von Dienstanbietern. In der Regel beeinflusst ein wirtschaftliches oder gesellschaftliches Ziel des Anbieters die Datenauswahl und die mehr oder weniger prominente Darstellung der einzelnen Dateneinheiten. Es kann für den Nutzer vorteilhaft sein, wenn für die Auswahl und Platzierung der Suchergebnisse bzw. der Artikel implizites Wissen aus dem bisherigen Nutzerverhalten herangezogen wird. So kann eine Suchfunktion beispielsweise Annahmen über die intendierte Semantik eines mehrdeutigen Suchbegriffes (z. B. »Golf«) machen oder ein journalistisches Angebot im Sportteil Nachrichten zu (vermeintlich) stärker interessierenden Sportarten in den Vordergrund stellen. Trotzdem sollten Nutzer eine einfache Möglichkeit haben, sich gezielt Suchergebnisse und journalistische Angebote so präsentieren zu lassen, wie sie einem Nutzer präsentiert werden, über den kein oder nur sehr rudimentäres Wissen (z. B. über den Aufenthaltsstaat) existiert. Nur so kann ein Nutzer dem Entstehen eigener Echokammern entgegenwirken, ohne andererseits auf für ihn zugeschnittene Angebote verzichten zu müssen.

Werden hingegen Suchergebnisse, journalistische Artikel oder Werbung aufgrund bloßer wirtschaftlicher Interessen (direkt oder aufgrund entsprechender Anzeigenkunden) des Anbieters prominenter platziert, muss zumindest eine deutliche Kennzeichnung der so bevorzugten Objekte erfolgen und relevante Suchergebnisse dürfen dadurch nicht verdrängt werden (z. B. auf weitere, erst durch expliziten Aufruf erreichbare Seiten). Nötigenfalls müssen diese Vorgaben regulativ festgelegt sein.

Einige Kommunikationsdienste verwenden nicht nur personenbezogene Daten für andere Zwecke als die Zielerreichung der Nutzer, sondern behalten sich in ihren AGBs[30] sogar vor, beliebige, nicht im Einzelnen bekanntgegebene Kommunikationsinhalte für solche Zwecke zu benutzen. Eine solche Regelung greift nicht nur massiv in die Datensouveränität der Nutzer ein, sie kann auch – z. B. wenn es sich bei den Kommunikationsin-

[28] »Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)«, http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679.

[29] Z. B. über die Webseite http://www.youronlinechoices.com/de/praferenzmanagement/.

[30] AGBs: Allgemeine Geschäftsbedingungen.

halten um Fotografien Dritter handelt – einen Eingriff zulasten unbeteiligter Nichtvertragspartner bedeuten. Akzeptiert ein Nutzer derartige AGBs nicht, kann er den Dienst generell nicht benutzen, was sich, abhängig von der Verbreitung des Dienstes, eventuell erheblich auf seine Kommunikationsmöglichkeiten auswirkt.

Der Rechtsrahmen muss die Interessen und Rechte der unterschiedlichen Beteiligten zueinander in Beziehung setzen und über den digitalen Raum hinausreichen, beispielsweise um die Digitalisierung und digitale Nutzung ursprünglich analoger Werke zu regeln.

Da es technisch kaum möglich ist, eine unkooperative Institution an der zweckfremden Nutzung von (personenbezogenen oder Inhalts-)Daten zu hindern, in deren Besitz sie gelangt ist, sind angemessene Möglichkeiten zur Ahndung von Datenmissbrauch besonders wichtig. Hier wurde für personenbezogene Daten mit der Datenschutz-Grundverordnung ein deutlicher Fortschritt im Hinblick auf EU-einheitliche Zulässigkeitsregeln erzielt.

Ein weiteres Spannungsfeld, in dem klare rechtliche Regeln erforderlich sind, ist die Erfassung und Auswertung von personenbezogenen bzw. personenbeziehbaren Daten zu Arbeitsleistung und -qualität. Hier kommt zur generellen Datenasymmetrie zwischen einzelnen Beobachteten und häufig großen beobachtenden Institutionen die Abhängigkeit der Arbeitnehmer von ihren Arbeitgebern, die viele Arbeitnehmer veranlasst, mehr Zugeständnisse als notwendig zu machen.

Im Zusammenhang mit Datensouveränität sind auch verschiedene Aspekte der in der öffentlichen Verwaltung flächendeckend geplanten und teilweise bereits genutzten Servicekonten[31] relevant. Es sollte den Bürgern (bzw. bei Unternehmenskonten den Unternehmen) möglich sein, die Zugriffsrechte auf die in einem Servicekonto permanent gespeicherten Daten feingranular festzulegen und gezielt einzelnen Behörden zu gewähren. Personen, die keine Bedenken haben, vielfältige Daten in einem solchen Servicekonto zu speichern und beliebigen Behörden zur Verfügung zu stellen, kann aber ebenso eine einfache generelle Zustimmungsmöglichkeit geboten werden.

3.1.6 Angebotsvielfalt, Interoperabilität und Standardisierung

Digitale Souveränität bemisst sich auch daran, ob es Alternativen bei Hard- und Software sowie deren Herstellern bzw. bei IT-Dienstleistern (z. B. Internetprovidern) gibt. Monopolistische Strukturen bergen ebenso wie monolithische Hard- oder Softwaresysteme die Gefahr, dass digitale Souveränität durch eine nicht (mehr) erwünschte, aber notwendige Bindung an einen Anbieter oder ein Produkt (»Vendor Lock-in«[32]) verloren geht. Zudem kann es bei Kompromittierung zu längeren, flächendeckenden Ausfällen oder größeren Datenverlusten bzw. -diebstählen kommen, was ebenfalls die digitale Souveränität beeinträchtigt.

Erforderlich ist für alle Bedürfnisse eine ausreichende Zahl konkurrierender, aber je nach Funktion interoperabler, kompatibler bzw. koexistenzfähiger[33] Komponenten und Dienstleistungen. Vorteilhaft sind standardisierte Programmier-, Kommunikations- und Bedienschnittstellen, die einen schnellen Austausch einzelner Komponenten – auch über Anbietergrenzen hinweg – ermöglichen. Modular aufgebaute Komponenten mit wiederum standardisierten Schnittstellen zwischen den Modulen erleichtern die gezielte Anpassung an die eigenen Bedürfnisse

[31] Servicekonto: Geschützter Online-Datenspeicher, in dem Bürger persönliche Daten für die Nutzung durch die öffentliche Verwaltung bereithalten können.

[32] Vendor Lock-in: Angewiesensein auf einen bestimmten Hersteller/Anbieter.

[33] Koexistenzfähige IT-Komponenten müssen nicht interoperabel sein (z. B., weil sie nie gemeinsam aktiv benutzt werden), behindern sich aber nicht gegenseitig bei Installation im selben IT-System.

SOUVERÄNITÄTSFREUNDLICHE GESCHÄFTSMODELLE ANBIETEN.

und führen zudem in der Regel zu geringeren Anpassungskosten gegenüber dem Austausch ganzer Komponenten oder sogar Systeme.

Selbst bei guter digitaler Bildung sowie nutzungs- und konfigurationsfreundlichen IT-Komponenten und -Diensten, die Datensouveränität unterstützen, gäbe es individuelle Unterschiede in der Passgenauigkeit. Da jedoch bisher keine dieser Voraussetzungen optimal erfüllt ist, bieten konkurrierende Angebote zumindest die Möglichkeit, dass die Nutzer das am besten für ihre persönlichen Anforderungen geeignete Produkt auswählen können. Zudem setzt die Nutzung von Produkten und Diensten, die die Voraussetzungen besser als andere erfüllen, die Anbieter anderer Produkte/Dienste unter Nachbesserungsdruck.

3.1.7 Offen gelegte Geschäftssmodelle und entsprechende Optionen für die Nutzer

Nutzer sind daran gewöhnt, eine Reihe von Internetdiensten (z. B. Suchmaschinen, Online-Spiele) kostenfrei nutzen zu können. Oft ist den Nutzern derzeit nicht bekannt, wenn sich solche Dienste (teilweise) über die Erfassung, Auswertung oder Weitergabe von Nutzerdaten finanzieren. Entsprechende Entscheidungsmöglichkeiten sind aber wesentlicher Teil der digitalen Souveränität. Sollten Nutzer zukünftig verstärkt dieser Datenverwendung widersprechen bzw. die Datenerfassung verhindern, müssen alternative Geschäftssmodelle angeboten werden.

3.1.8 Neutrale IT-Bewertung und -Zertifizierung, zentrale Sicherheitswarnungen

Zusätzlich zur Vermittlung von Fähigkeiten, um Beschaffungssouveränität zu erreichen, müssen neutrale Informationen über Hard- und Software- sowie Dienstleistungsalternativen angeboten werden. Hilfreich ist auch eine Zertifizierung von Produkten und Dienstleistungen, die bestimmte Mindestanforderungen erfüllen. Dazu gehören insbesondere Datenschutz und Datensicherheit, aber z. B. auch die ergonomische Bedienung.

Selbst einfachste IT-Systeme für den Privatgebrauch umfassen in der Regel Hard- und Softwarekomponenten verschiedener Hersteller, die zudem von Dritten angepasst worden sein können. Der Nutzer hat keinen Überblick über dieses komplexe Komponentengeflecht. Selbst wenn alle Hersteller Sicherheitswarnungen für ihre Produkte zeitnah bekanntgeben würden, wäre der private Nutzer mit der Beobachtung dieser Warnungen überfordert. Eine zentrale, zeitnahe Bereitstellung von Informationen über verfügbare Sicherheitsupdates, wie die Sicherheitshinweise[34] für Bürger vom BSI[35], stellt daher eine unverzichtbare Informationsquelle für eigenverantwortlich handelnde private IT-Nutzer dar.

3.1.9 Eigenverantwortliches Handeln

Neben den Voraussetzungen für individuelle digitale Souveränität, die von Dritten geschaffen werden müssen, verbleibt ein wesentlicher Teil, den nur die Nutzer selbst leisten können.

Hierzu gehören im Bereich der Sicherheit und des Datenschutzes, um nur einige zu nennen, der Einsatz aktueller Softwareversionen und Angriffsschutzsoftware, der sorgfältige Umgang mit Passwörtern, PINs[36] und TANs[37] und gesundes Misstrauen bei der Herausgabe persönlicher Daten (Konto- und Kartennummern …) sowie beim Aufrufen von Weblinks oder der Benutzung von USB-Sticks, die man von Dritten erhalten hat.

[34] https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Buerger-CERT/Sicherheitshinweise/Sicherheitshinweise_node.html.

[35] BSI: Bundesamt für Sicherheit in der Informationstechnik.

[36] PIN: Persönliche Identifikationsnummer.

[37] TAN: Transaktionsnummer.

Will man sich nicht von monolithischen Angeboten bei Hard- und Softwarekomponenten oder Onlinediensten abhängig machen, erfordert dies in der Regel ein gewisses Maß an Eigeninitiative, alternative Angebote zu finden und zum Einsatz zu bringen. Für Basiskomponenten (wie z. B. Webbrowser) gibt es dazu sowohl online als auch häufig auf nachbarschaftlicher Ebene Unterstützung, die dies auch Menschen ermöglicht, die nur IT-Grundkenntnisse besitzen (beispielsweise Cryptopartys).

Bei der Auswahl neuer mobiler Geräte ist auch darauf zu achten, ob regelmäßig Sicherheitsupdates für das eingesetzte Betriebssystem ausgeliefert werden.

Hinter Suchmaschinen und journalistischen Angeboten im Internet stehen oft Institutionen, die nicht den in Deutschland üblichen Erwartungen an Neutralität entsprechen, beispielsweise weil an ihrem Hauptsitz oder bei einem großen Teil ihrer Kunden andere Erwartungen herrschen oder weil es zu ihrem Geschäftsmodell gehört, den Nutzern (vermeintlich) angenehme Angebote zu präsentieren. Deshalb ist es auch an den Nutzern sich dies bewusst zu machen und – analog z. B. zu Printmedien – gegebenenfalls weitere Suchmaschinen bzw. journalistische Angebote zu nutzen, um ein umfänglicheres Bild zu erhalten.

3.1.10 Zeitgemäße Informations- und Beteiligungsmöglichkeiten im Zusammenhang mit der gesamtgesellschaftlichen Digitalisierung

Neben den klassischen Beteiligungsformaten bietet es sich besonders beim Thema Digitalisierung an, digitale Beteiligungsformate wie Online-Diskussionen, Webcasts, Internet-Abstimmungen und Ähnliches einzusetzen und so verstärkt orts- und zeitunabhängige Beteiligung zu ermöglichen. Digitale Formate bedürfen dabei neben neutraler und kontinuierlicher Organisation auch einer vertrauenswürdigen digitalen Plattform, auf der freie Meinungsäußerung möglich ist und die gegen Meinungsmajorisierung (z. B. durch Social Bots) geschützt wird. Während bei den Informationsmöglichkeiten derzeit von einem guten Angebot klassischer wie neuer Medien – von Zeitungen und Fernsehen über Fachveröffentlichungen bis zu Wikipedia – ausgegangen werden kann, sind bei politikrelevanten Fragen evtl. auch direkt von den politischen Gremien betriebene Beteiligungsplattformen notwendig, wie beispielsweise die Online-Umfragen zu den Grünbüchern[38] des BMWi.

3.2 INSTITUTIONELLE DIGITALE SOUVERÄNITÄT

Die digitale Souveränität einer Institution erfordert zunächst die individuelle digitale Souveränität ihrer Mitarbeiter. Besonders wenn eine Institution auf den Einsatz und damit auf das Funktionieren von IT-Komponenten angewiesen ist – was zunehmend selbst für kleine und mittlere Handwerksbetriebe gilt –, kommen weitere Maßnahmen hinzu, die sämtlich in dieselben oder ähnliche Kategorien wie bei der individuellen digitalen Souveränität (siehe Abschnitt 3.1) fallen.

3.2.1 Fachbildung

Um die digitalen Belange einer Institution sachgerecht und effizient bearbeiten zu können, sind in der Regel über die Allgemeinbildung hinausgehende Fachkenntnisse zu Techniknutzung, Mediennutzung und Sicherheit notwendig, deren Zusammensetzung aufgabenabhängig variiert. Angemessene Fachkenntnisse sind dabei nicht nur für IT-Personal, sondern für alle Personen notwendig, die IT-Komponenten nutzen oder Tätigkeiten mit IT-Bezug steuern.

[38] Bundesministerium für Wirtschaft und Energie: »Grünbuch Digitale Plattformen, Mai 2016, https://gruenbuch.de.digital/fileadmin/redaktion/BMWi/gruenbuch-digitale-plattformen.pdf bzw. Bundesministerium für Wirtschaft und Energie: »Grünbuch Energieeffizienz«, August 2016, https://www.gruenbuch-energieeffizienz.de/fileadmin/redaktion/Energieeffizienz/bmwi_bro_gru%CC%88nbuch_energieeffizienz_web_bf.pdf.

Die Fachausbildung erfolgt typischerweise im dualen System und in Hochschulen, wobei die Inhalte ständig an die nach wie vor rasante Technikentwicklung im Bereich der Digitalisierung angepasst werden müssen. Wegen dieses Entwicklungstempos ist auch die Fortbildung von besonderer Bedeutung.

Neben die nutzungsorientierte Bildung muss in einer Institution auch die organisatorische Bildung treten, die vor allem für die digitale Governance der Institution wesentlich ist.

Verbänden, (Groß-)Unternehmen und Behörden kommen wesentliche Aufgaben zu, so die Identifikation notwendiger Fortbildungsinhalte, die Vermittlung dieses Fortbildungsbedarfes an ihre Mitglieder bzw. Abteilungen sowie die Durchführung entsprechender Fortbildungen. Wichtig sind Verbände auch bei der Identifikation und Verbreitung von »Best Practices«, also vorteilhafter Problemlösungen, die oft in den eigenen Reihen entwickelt wurden.

Sowohl klassische Bildungseinrichtungen als auch Verbände, (Groß-)Unternehmen und die öffentliche Hand können und sollten Aus-, Weiter- und Fortbildung durch offene Online-Angebote (Open Educational Resources, OERs) unterstützen und so insbesondere den berufsintegrierten bzw. berufsbegleitenden Auf- und Ausbau von IT-Fähigkeiten fördern.

Alle Institutionen benötigen, unabhängig von ihrer Größe und vorhandener oder nichtvorhandener Gewinnerzielungsabsicht, klare und praxistaugliche Regeln zu Datenschutz, Angriffsschutz, Sicherstellung der Verfügbarkeit von IT-Betriebsmitteln und Daten sowie zum angemessenen Verhalten bei der Internetkommunikation. Diese Regeln müssen situationsgerecht aktualisiert und nachvollziehbar vermittelt werden.

3.2.2 Nutzungsfreundliche Hard- und Software

Bei der Hard- und Software in institutionellen Kontexten kann man in der Regel nicht auf nutzerspezifische Konfigurationsprofile einschließlich sachgerechter Datenzugriffsrechte verzichten. Zudem muss die Einhaltung bestimmter Nutzungsregeln (z. B. zur Aufrechterhaltung des erforderlichen Sicherheitsniveaus) durch zentrale Konfiguration erzwungen werden können.

Spezielle Anforderungen gelten bei der Robustheit, also der Fähigkeit der Hard- und Software, ungewöhnliche Ereignisse (z. B. unerwartete Eingaben) oder Zustände (z. B. die Nichtverfügbarkeit eines externen Datenspeichers) zu erkennen und darauf so zu reagieren, dass die Nutzer insgesamt möglichst wenig beeinträchtigt werden. Beispielsweise können Geräte, die mit zwei Netzteilen ausgestattet und damit an verschiedene Stromkreise angeschlossen sind, sowohl den Ausfall eines Netzteils als auch den eines Stromkreises kompensieren.

3.2.3 Nutzer- und betreiberfreundliche Unterstützung von Softwareinstallationsprozessen

In Institutionen existiert häufig (gegenüber individuellen IT-Nutzern) verstärkter Interoperabilitätsbedarf zwischen Software innerhalb einzelner Geräte, insbesondere aber zwischen verschiedenen Geräten der Institution. Deshalb stellen das »Ausrollen« neuer Software (versionen) sowie die Verteilung und Inbetriebnahme von Softwareupdates (und schlimmstenfalls auch das Rückabwickeln fehlerhafter Updates) regelmäßig eine Herausforderung dar, beispielsweise im Hinblick auf die Synchronisation von Server- und Klientenupdates. Für Institutionen, die neue Software und Updates zunächst einer internen Funktions- oder Interoperabilitätsprüfung unterziehen, sind automatische, unkoordinierte Updates ebenfalls ungeeignet. Einige Softwarehersteller und Drittanbieter bieten für vernetzte Geräte (institutions-)zentrale Komponenten für die Installationsunterstützung an, wobei die Komponenten von Softwareherstellern häufig nur ihre eigene Software unterstützen.

3.2.4 Angriffsresistente, Backdoor-freie Komponenten

Institutionen sind für verschiedene Typen von Angreifern die (z. B. gegenüber privaten Nutzern) »lohnenderen« Ziele und bei erfolgreichen Angriffen droht ein größerer wirtschaftlicher oder Imageschaden. Werden für Angriffe die Schnittstellen und/oder die Kommunikationsformen spezieller Anwendungen (z. B. Produktionssteuerungs- oder Logistiksysteme) ausgenutzt, sind unspezifische Sicherheitssysteme (wie Virenscanner, Firewalls, Intrusion-Prevention[39]- und Intrusion-Dectection-Systeme[40]) oft hilflos, selbst wenn man sie aktuell hält. Mit zunehmender Vernetzung stoßen zudem klassische Konzepte zur Netzwerkabsicherung in jeglicher Hinsicht an ihre Grenzen – weder können alle Komponenten innerhalb eines vermeintlich sicheren Netzes als dauerhaft sicher angenommen werden noch kann jede Kommunikation mit potenziell unsicheren Komponenten unterbunden oder umfänglich geprüft werden. Die beste Abschottung nützt zudem nichts, wenn Nutzer oder Systeme innerhalb der »Schutzmauern« frei agieren können.[41] Deshalb ist es – insbesondere in den zu den kritischen Infrastrukturen zählenden Bereichen – notwendig, dass Software nachweislich und überprüft nur die betriebsnotwendigen Funktionen, Kommunikationsmuster, Schnittstellen und Schnittstellenfähigkeiten besitzt bzw. unterstützt und ungeplante Kommunikationsmuster selbst konsequent erkennt und unterbindet.

[39] Intrusion-Prevention-System: System zur Verhinderung elektronischer Einbrüche z. B. in Firmennetze.

[40] Intrusion-Detection-System: System zur Erkennung elektronischer Einbrüche z. B. in Firmennetze.

[41] Siehe auch: N. Menz, P. Hoepner, J. Tiemann, F. Koußen »S²: Safety und Security aus dem Blickwinkel der öffentlichen IT«, ÖFIT-Whitepaper, Kompetenzzentrum Öffentliche Informationstechnologie, Fraunhofer FOKUS, Berlin, April 2015, http://www.oeffentliche-it.de/publikationen?doc=31236&title=Safety+und+Security+aus+dem+Blickwinkel+der+%C3%B6ffentlichen+IT.

3.2.5 Technische, organisatorische und rechtliche Unterstützung von Datensouveränität und Informationsfreiheit

Datensouveränität von Institutionen bezieht sich einerseits auf die Entscheidungsmöglichkeit, wem welche Daten zur Verfügung gestellt, z. B. welche Unternehmenskennzahlen über die rechtlichen Verpflichtungen hinaus der Öffentlichkeit zugänglich gemacht werden. Hier spielen vor allem technische (z. B. Firewalls) und organisatorische Maßnahmen eine Rolle, die einen unbefugten Zugriff Dritter auf die Daten verhindern.

Andererseits hat die Verfügbarkeit der eigenen Daten, die für den geordneten Geschäftsbetrieb notwendig sind, für die Mitarbeiter der Institution eine hohe Bedeutung. Bei Institutionen ist unter Gesichtspunkten der Datensouveränität z. B. abzuwägen, ob eine Vor-Ort-Speicherung oder eine Speicherung in einer geografisch entfernten und/oder fremdadministrierten Cloud zu bevorzugen ist.

Der Missbrauch solcher in einer Cloud bzw. Plattform gespeicherter Daten durch den Betreiber ist i. d. R. schwer feststellbar und nur mit richterlicher Hilfe – technische Untersuchung der Cloud- bzw. Plattforminfrastruktur – nachweisbar.

Die Datenschutz-Grundverordnung der EU gilt nur für personenbezogene Daten und dient dem Schutz natürlicher Personen. Eine analoge rechtliche Regelung für sensible Daten von Unternehmen und ggf. Behörden wäre vorteilhaft.

Nach der Insolvenz eines Betreibers besteht nicht in allen Rechtssystemen automatisch ein Herausgabe- und Löschungsanspruch für die aufbewahrten Daten, auch beim Rechteübergang an einen neuen Betreiber gilt nicht unbedingt die Pflicht, die Zustimmung der Nutzer zur Übergabe ihrer gespeicherten Daten einzuholen.

Institutionen sind wie individuelle IT-Nutzer durch digitale Echokammern und die Platzierung von Suchergebnissen anhand wirtschaftlicher Erwägungen des Anbieters gefährdet, beispielsweise bei Markterhebungen im Zusammenhang mit Beschaffungen. Auch hier würden eine leicht anwählbare wissensarme Ausprägung der Suchfunktion und klare Vorgaben zur Kennzeichnung werblicher Elemente helfen.

3.2.6 Angebotsvielfalt, Interoperabilität und Standardisierung

Unter Verfügbarkeitsgesichtspunkten sind für manche Institutionen Produktalternativen oder mehrere, voneinander unabhängige Kommunikations- oder Clouddienste, die gleichzeitig genutzt werden können, essenziell.

3.2.7 Neutrale IT-Bewertung und -Zertifizierung, zentrale Sicherheitswarnungen

Institutionen brauchen ebenso wie private IT-Nutzer neutrale Qualitätshinweise zu den von ihnen eingesetzten oder geplanten IT-Komponenten. Lediglich die Gewichtung der Kriterien (wie Ergonomie, Angriffs- und Betriebssicherheit …) fällt oft anders als bei der privaten Nutzung aus. Häufig ist eine Zertifizierung der Produkte wesentliche Grundlage einer Beschaffungsentscheidung.

Eine neutrale, unabhängige Zertifizierung ganzer IT-Installationen und des IT-Managements von Institutionen – z. B. im Hinblick auf Betriebs-, Angriffs oder Datensicherheit – kann ein sinnvolles Mittel sein, um festzustellen, ob sachgerecht und zeitgemäß mit IT und Daten umgegangen wird. Vielfach ist eine freiwillige Zertifizierung auf Veranlassung des Betreibers ausreichend. In speziellen Fällen, z. B. bei Komponenten kritischer Infrastrukturen oder bei der Übertragung staatlicher Aufgaben, kann jedoch auch eine Zertifizierungspflicht angemessen sein.

Tagesaktuelle, zentrale Sicherheitswarnungen sind essenziell, beispielsweise um durch gezieltes präventives Handeln Schäden zu vermeiden. Hierzu sind die vom BSI bereitgestellten CERT-Bund[42]-Meldungen (und die Meldungen weiterer CERTs) ein bedeutendes Hilfsmittel.

3.2.8 Eigenverantwortliches Handeln

Zum eigenverantwortlichen Handeln einer Institution im Zusammenhang mit digitaler Souveränität gehören im Bereich der Sicherheit vor allem sorgfältig geplante und umgesetzte sowie regelmäßig auf ihre Wirksamkeit überprüfte Regeln und technische Maßnahmen im Zusammenhang mit IT-Betriebs- und Angriffssicherheit und zum Umgang mit Personen- und sensiblen Daten der Institution. Entsprechende Regeln können sich sowohl auf das Verhalten der Mitarbeiter als auch auf die Konfiguration von IT-Komponenten beziehen. Konfigurationsvorgaben sollten dabei möglichst zentral umgesetzt werden, um Fehler zu vermeiden und bei Änderungen schnell überall den neuen Stand zu erreichen. Ein wesentlicher Baustein ist hier das Updatemanagement, das dafür sorgt, dass Softwareupdates (und in diesem Zusammenhang notwendige Konfigurationsdaten) zeitnah und koordiniert an alle relevanten Geräte verteilt und dort auch in Betrieb genommen werden. Während die Updates selbst durch automatisierte Prozesse installiert werden können (siehe Abschnitt 3.2.3), ist besonders in größeren Institutionen eine sorgfältige Ablaufplanung erforderlich.

Bei der Auswahl von Hard- und Softwarekomponenten und Online-IT-Dienstleistungen muss man neben Funktionalität, Sicherheit und aktuellen Kosten auch die digitale Souveränität berücksichtigen. Dazu gehört beispielsweise das Risiko, dass aufeinander angewiesene Komponenten zukünftig nicht mehr

[42] CERT-Bund: Computer Emergency Response Team für Bundesbehörden, zentrale Anlaufstelle für präventive und reaktive Maßnahmen bei sicherheitsrelevanten Vorfällen in Computer-Systemen.

oder nur noch mit deutlich höheren Kosten in der erforderlichen Kombination unterstützt werden (Vendor Lock-in). Ein anderes Beispiel sind gebührenfrei angebotene Online-IT-Dienstleistungen, bei denen sich viele Anbieter vorbehalten, ihre Geschäftsbedingungen beliebig ändern und Änderungen auf z. B. bereits dort gespeicherte Daten anwenden zu können.

Im organisatorischen Bereich, also der IT- und der digitalen Governance, kommt es weniger darauf an, bislang andersartig gelöste Prozessschritte eins zu eins durch digitale Pendants zu ersetzen, als logisch zusammenhängende Prozesse bzw. Prozessteile zu erkennen und im Zuge der Digitalisierung als Ganzes zu optimieren. Bei institutionsübergreifenden Prozessen kann dies durchaus auch zu einer (Rück-)Verlagerung von Zuständigkeiten führen, beispielsweise wenn Institutionen bei elektronischem Zugang ihrer Kunden, Klienten oder Dienstleister nicht mehr auf die Vor-Ort-Unterstützung durch eine andere Institution angewiesen sind.

3.2.9 Informations- und Beteiligungsmöglichkeiten im Zusammenhang mit der gesamtgesellschaftlichen Digitalisierung

Besonders Institutionen, die sich in einer gravierenden Digitalisierungsphase (Digitalisierung der Produktion, Einführung von E-Government …) befinden oder bei denen eine solche bevorsteht, haben einen weit über die technische Umsetzung hinausgehenden Informationsbedarf, z. B. zu Arbeitnehmerrechten und Mitarbeitermotivation. Typischerweise sind hier Verbände die ersten Ansprechpartner, aber auch staatliche Institutionen sollten durch eine themenorientierte Zusammenstellung und Aufbereitung insbesondere von Gesetzen und Verordnungen Orientierungshilfen bieten.

Vor allem Verbände und große Unternehmen wünschen sich Einflussmöglichkeiten, beispielsweise auf die arbeitsrechtliche Bewertung kurzzeitiger spontaner dienstlicher Inanspruchnahme außerhalb der regulären Arbeitszeit, die durch die inzwischen weit verbreitete ständige Erreichbarkeit über Mobilfunk und Internet in großem Maßstab möglich geworden ist. Prinzipiell besteht durch deren mittelbare Beteiligung am Prozess der Rechtsetzung die Möglichkeit, zu praxisgerechten Lösungen zu gelangen. Dazu ist allerdings auch eine angemessene Beteiligung der Arbeitnehmerseite erforderlich.

3.3. DIGITALE SOUVERÄNITÄT VON IT-PRODUZENTEN UND -DIENSTLEISTERN

Die digitale Souveränität von IT-Produzenten und -Dienstleistern steht und fällt mit der Verfügbarkeit von Mitarbeitern und ihrer Qualifikation. Aber auch in anderen Maßnahmenkategorien gibt es einige Spezifika.

3.3.1 Fachbildung

Wegen der oft sehr speziellen Ausrichtung insbesondere kleiner IT-Produzenten oder von Mitarbeitergruppen in größeren Unternehmen können Fortbildungen nicht immer über Verbände oder unabhängige kommerzielle Anbieter organisiert werden. In einigen Bereichen, z. B. zur IT-Sicherheit oder Qualitätssicherung, sind Seminarangebote von Hochschulen und Forschungseinrichtungen vorstellbar, um solche Lücken zu schließen.

3.3.2 Technische, organisatorische und rechtliche Unterstützung der Datensouveränität

Für Softwareproduzenten stellt die eigene Software den wesentlichen wirtschaftlichen Wert dar, für den, z. B. über das Urheberrechtsgesetz[43], umfassender Verfügungsschutz gilt.

[43] Urheberrechtsgesetz vom 9. September 1965 (BGBl. I S. 1273), das zuletzt durch Artikel 1 des Gesetzes vom 20. Dezember 2016 (BGBl. I S. 3037) geändert worden ist, https://www.gesetze-im-internet.de/urhg/UrhG.pdf.

INTERESSENAUSGLEICH ZWISCHEN SOFTWAREPRODUZENTEN UND BETRIEBSSYSTEMANBIETERN ERZIELEN.

Allerdings steht dieser Schutz in einem Spannungsverhältnis zum ebenfalls berechtigten Interesse von (potenziellen) Nutzern und gesellschaftlichen Institutionen, die Korrektheit, Seiteneffektfreiheit und Sicherheit von Software anhand offen gelegten Quellcodes und vollständig beschriebener Schnittstellen überprüfen zu können. Hier müssen gegebenenfalls Einzelfallentscheidungen getroffen werden.

Kopier- und Dekompilierungsschutzfunktionen sowie Funktionen gegen unlizenzierte Nutzung sind in diesem Zusammenhang ebenfalls häufiger Diskussionsgegenstand, insbesondere, wenn sie in entgegenstehende Rechte von Nutzern bzw. anderen Softwareproduzenten eingreifen. Auch hier können Einzelfallentscheidungen notwendig sein.

Softwareproduzenten können in verschiedenen großen Marktsegmenten ihre Komponenten nicht mehr direkt bzw. über selbst gewählte Distributoren vertreiben, sondern sind auf eine Freigabe oder gar die Distribution durch den Betriebssystem- oder Geräteanbieter angewiesen, wobei die Freigabe in der Regel nur nach Inspektion des Quellcodes erfolgt. Eine Freigabe, die rein auf der objektiven Bewertung von Betriebs- und Angriffssicherheitsaspekten beruht, ist dabei prinzipiell im Sinne von Nutzern und Netzbetreibern, sie muss allerdings zu fairen Bedingungen (z. B. Kosten) erfolgen. Eine (womöglich nicht einmal ausreichend qualifizierte) Bewertung, ob die Software rechtlich unzulässige Aktionen ermöglicht, oder gar eine Freigabeverweigerung, die sich lediglich auf unerwünschten Funktionen der Software abstützt, kann hingegen einen fragwürdigen Eingriff in die Datensouveränität von Softwareherstellern darstellen[44], insbesondere wenn rechtlichen oder kulturellen Unterschieden dabei nicht ausreichend Rechnung getragen wird.

Ein spezieller Interessenkonflikt tritt auf, wenn als geheimhaltungsbedürftig angesehene Software mit einem verpflichtenden Freigabeprozess eines Betriebssystem- oder Geräteanbieters zusammentrifft.[45] In einem solchen Fall muss typischerweise eine individuelle Regelung zwischen dem Softwareproduzenten, dem Betriebssystem- bzw. Geräteanbieter und gegebenenfalls den Softwarekunden gefunden werden.

3.3.3 Interoperabilität und Standardisierung

Während große IT-Produzenten sich ihr eigenes IT-Ökosystem schaffen können, sind kleine und mittlere Produzenten in hohem Maß auf Interoperabilität, Kompatibilität und Koexistenzfähigkeit mit den Produkten anderer Hersteller angewiesen und haben nur dann eine Vermarktungschance, wenn ihre Produkte über herstellerübergreifend standardisierte Schnittstellen mit Fremdprodukten kombiniert werden können.

Gerade kleine und mittlere Unternehmen haben jedoch oft nicht die Mittel, um sich aktiv an der Standardisierung, insbesondere an der Normung[46], zu beteiligen. Hier sollten Möglichkeiten geschaffen werden, die dem Ungleichgewicht zwischen wenigen großen Anbietern von Universalsystemen (z. B: Betriebssystemen, Browsern …) und vielen kleinen Spezialanbietern, die aber einheitliche Schnittstellen benutzen könnten, entgegenwirken.

3.3.4 Neutrale IT-Bewertung und -Zertifizierung

Während Bürger und Institutionen IT-Bewertungen und -Zertifikate für Beschaffungsentscheidungen nutzen, sind solche Bewertungen und Zertifikate im Gegenzug »Türöffner« für IT-

[44] Im Juli 2017 hat bspw. ein großer Distributor VPN-Software (Virtual Private Network: kann zur verschlüsselten Kommunikation mit von außen nicht erkennbaren Dritten genutzt werden) aus seinem chinesischen Angebot entfernt.

[45] Ein großer Betriebssystemanbieter hatte vor einigen Jahren ursprünglich geplant, auf neueren Versionen nur noch den Einsatz geprüfter Software zu ermöglichen, dies aber nach Protesten von Wirtschaft und öffentlicher Verwaltung nicht umgesetzt.

[46] Normung: Standardisierung durch offizielle Normungsgremien.

Produzenten und -Dienstleister. Hinderlich ist, dass in Europa jeder Staat eigene Bewertungs- und Zertifizierungsregeln hat und eine gegenseitige Anerkennung nicht immer vorgesehen ist. Hinzu kommen Zertifikate, die Entwickler- und Interessenvereinigungen erteilen, die sich aber in der Regel nur auf spezielle Aspekte der IT-Produkte beziehen. Strebt man also eine inhaltlich und geografisch umfassende Zertifizierung an, ist dies mit hohem personellem und oft auch monetärem Aufwand verbunden.

3.3.5 Eigenverantwortliches Handeln

IT-Produzenten und -Dienstleister sind in vielen Bereichen in hohem Maße vom Vertrauen ihrer Kunden abhängig. Dies gilt sowohl für den Privatkunden- als auch für den Wirtschafts- und Verwaltungsmarkt. Schutzmaßnahmen wie bei anderen Institutionen sind daher unerlässlich. Ein offener Umgang mit erkannten Schwachstellen der eigenen Produktions- bzw. IT-Umgebung oder der Produkte selbst – gepaart mit angemessenen Abhilfemaßnahmen – kann auf längere Sicht mehr Vertrauen schaffen als ein Vertuschen solcher Mängel (insbesondere wenn diese später doch offenbar werden).

3.3.6 Beteiligungsmöglichkeiten im Zusammenhang mit der gesamtgesellschaftlichen Digitalisierung

IT-Produzenten und -Dienstleister sind diejenigen, die typischerweise am besten wissen, ob bzw. wie sich eine gesellschaftlich, politisch oder wirtschaftlich erwünschte IT-Funktion realisieren lässt. Es ist daher unerlässlich, auch kleine und mittlere IT-Produzenten und -Dienstleister eng in Digitalisierungsentscheidungen und -prozesse sowie in die entsprechende Regulierung einzubeziehen. Bei Entscheidungen muss aus gesellschaftlicher Sicht jedoch stets auch berücksichtigt werden, welchen wirtschaftlichen Nutzen für die IT-Produzenten bzw. -Dienstleister eine von ihnen favorisierte Lösung hat und ob sie aus gesellschaftlichen Gesichtspunkten ebenfalls zu präferieren ist.

3.4 GESAMTGESELLSCHAFTLICHE DIGITALE SOUVERÄNITÄT

Da die gesamtgesellschaftliche digitale Souveränität zu wesentlichen Teilen von der digitalen Souveränität ihrer einzelnen Bürger, ihrer IT-nutzenden Institutionen und ihrer IT-Produzenten und -Dienstleister bestimmt wird, sind die dazu jeweils genannten Voraussetzungen auch für die gesamtgesellschaftliche digitale Souveränität prägend. Hinzu kommen jedoch einige spezifische Aspekte, die nur in der übergreifenden Betrachtung bewertet werden können.

3.4.1 Digitale Souveränität im technischen Bereich

Seit Jahren wird in Deutschland und Europa ein deutlicher und wachsender Verlust an technischer digitaler Souveränität beklagt, da wesentliche Fortschritte der IT-Technik fast ausschließlich in den USA, China, Japan und Südkorea erzielt werden. Daran haben auch die umfangreichen Förderprogramme der EU, beginnend mit dem 1. Forschungsrahmenprogramm 1984, und die massive nationale und regionale Förderung von IT-Forschung und -Entwicklung in vielen EU-Staaten einschließlich Deutschlands (z. B. das aktuelle Forschungsrahmenprogramm der Bundesregierung zur IT-Sicherheit[47]) bisher wenig geändert.

Bei der Standardisierung und speziell der Normung gilt es, nationale Alleingänge zu vermeiden und stattdessen frühzeitig nach in möglichst großem geografischem Rahmen kompromissfähigen, umfassenden Lösungen zu suchen, ohne dabei jedoch zeitgemäße Leistungs-, Qualitäts- und Sicherheitsanforderungen zurückzustellen. Eine sehr kleinteilige, anwendungs- und situationsspezifische Standardisierung, die konkurrierende Interessengruppen durch alternative Standards befriedigt, läuft

[47] BMBF: »Selbstbestimmt und sicher in der digitalen Welt 2015-2020«, 06.03.2015, https://www.bmbf.de/pub/Forschungsrahmenprogramm_IT_Sicherheit.pdf.

nicht nur dem Grundgedanken der Standardisierung, nämlich der Vereinheitlichung, entgegen. Sie begünstigt auch neue Abhängigkeiten, wenn in zunehmend komplexen Einsatzumgebungen mehrere, weil jeweils sehr spezielle Lösungen miteinander kombiniert werden müssen. Ein Beispiel einer solchen Entwicklung ist die für das Internet der Dinge und Industrie 4.0 wichtige Feldbustechnik mit rund 20 verschiedenen genormten Lösungen.

Eine weitere Möglichkeit, sich unabhängiger von Drittanbietern zu machen, ist die transnationale Entwicklung von IT-Komponenten (analog zum Aufbau des Airbus-Konzerns). In einer solchen Zusammenarbeit können von vornherein nationale Besonderheiten berücksichtigt oder durch das gemeinsame Auftreten der Partner ausgeräumt werden. Die Partner können auch unterschiedliche Schwerpunkte einbringen und von gemeinsamen technischen Ergebnissen profitieren, auf die sie sonst keinen Zugriff hätten.

Eine wesentliche Grundlage gesamtgesellschaftlicher digitaler Souveränität im technischen Bereich ist das ausreichende Vorhandensein entsprechend qualifizierter Hard- und Softwareentwickler. Gerade angesichts des demografischen Wandels erfordert dies optimale, aktuelle Bildungsangebote sowohl unmittelbar für Schulabgänger als auch für Quereinsteiger. Ebenso sind verstärkte Anstrengungen erforderlich, insgesamt mehr Menschen und insbesondere bisher unterrepräsentierte Gruppen – Frauen, Menschen mit Migrationshintergrund … – für die betroffenen Berufsbilder zu gewinnen und ausreichend Ausbildungs- und Studienplätze zur Verfügung zu stellen.

3.4.2 Digitale Souveränität im Bereich der plattformbasierten Dienstleistungen und des Handels

Auch bei IT-Dienstleistungen, die über das Internet erbracht werden und stark auf Netzwerkeffekten basieren – wie Suchmaschinen, Wissensplattformen und soziale Medien, aber auch Online-Versandhandel und Download- oder Streamingplattformen – herrscht kein ausgewogenes Verhältnis zwischen den Orten der Firmensitze und der geografischen Reichweite der Dienstleister.

Hier kommt zur Größe der jeweiligen Heimatmärkte häufig noch eine Sprachbarriere hinzu: Kleine Anbieter bieten häufig vorrangig oder sogar ausschließlich in ihrer Landessprache an, was eine Ausweitung der Geschäftsbeziehungen gerade auf das englischsprachige Ausland stark erschwert. Im Versandhandel spielen außerdem Aspekte wie Personalkosten, Zollvorschriften und sogar Versandkosten eine wesentliche Rolle.

Um im Bereich der kleinen und mittleren Anbieter international mehr Ausgewogenheit zu erreichen, sind gezielte Fördermaßnahmen zur Internationalisierung, z. B. Unterstützung beim Aufbau englischsprachiger Websites, denkbar. Ebenso können regional ausgerichtete Angebote dabei unterstützt werden, sich unabhängig von großen, internationalen Plattformen zu etablieren, beispielsweise durch die Förderung von regionalen oder themenbezogenen Portalen. Von solchen Maßnahmen könnten nicht nur kleine Unternehmen profitieren, die sich keine prominente Platzierung in internationalen Suchmaschinen leisten können, sondern vor allem auch ehrenamtliche und auf Nachbarschaftshilfe ausgerichtete Organisationen.

Ein Hilfsmittel bei plattformbasierten Dienstleistungen ist wiederum die Standardisierung. Sind beispielsweise Datenformate und Kommunikationsschnittstellen zwischen lokalem Klienten und Plattformserver standardisiert, erleichtert dies einen Anbieterwechsel oder die parallele Nutzung verschiedener Anbieter, was für neue Anbieter von Vorteil sein kann.

Erfolgreiche kleine bis mittlere deutsche und europäische Anbieter geraten häufig in den Übernahmefokus größerer außereuropäischer Anbieter, wodurch die deutsche bzw. europäische digitale Souveränität geschwächt wird.

Neben diesen wirtschaftlichen Gesichtspunkten spielen bei Plattformen, die ihren Schwerpunkt außerhalb Deutschlands bzw. der EU haben, auch kulturelle und gesetzliche Aspekte eine Rolle. Bekannte Beispiele sind unterschiedliche Bewertungen bzgl. der Darstellung menschlicher Nacktheit oder der Verherrlichung des Nationalsozialismus. Für Plattformen, die sich an deutsche Nutzer richten, müssen funktionstüchtige Lösungen gefunden werden, die sowohl mit hier liberaleren als auch mit hier engeren Regeln angemessen umgehen, um einerseits der Informationsfreiheit, andererseits aber auch rechtlichen Grenzen Geltung zu verschaffen. Auch wenn in jedem Einzelfall »schnelle Abhilfe« wünschenswert ist, sollte die Bewertungsverantwortung bei der Justiz verbleiben (die ja das Instrument der einstweiligen Verfügung besitzt).

3.4.3 Digitale Souveränität im organisatorischen Bereich

Das sogenannte Schengen-Routing – d. h. Routing zwischen europäischen Kommunikationspartnern ausschließlich über Router, die in Europa stehen und von europäischen Anbietern betrieben – und die Euro-Cloud – Clouddienste, deren Server in Europa stehen und von europäischen Anbietern betrieben werden – wurden als organisatorische Lösungsansätze ins Spiel gebracht, um internationaler Ausspähung entgegenzutreten.

Das Internet, als eine zwecks wissenschaftlichen Informationsaustauschs entstandene Infrastruktur, orientiert sich nicht an Staatsgrenzen. Funktionen, die entsprechende Parameter berücksichtigen, müssten zusätzlich integriert werden und könnten in ungünstig angebundenen geografischen Regionen negative Auswirkungen auf die Verfügbarkeit und Stabilität der Kommunikation haben.

Datenkommunikation und -speicherung mit Hilfe von Infrastrukturen, die ausschließlich europäischem Recht unterliegen, ermöglichen zwar prinzipiell ein Vorgehen gegen entsprechende Rechtsverstöße. Wenn solche Verstöße aber von Organen externer Staaten begangen werden, sind die praktischen Sanktionsmöglichkeiten eher gering (wie beispielsweise die NSA-Affäre gezeigt hat). Die vollständige Herausgabe bzw. Vernichtung unrechtmäßig erworbener Daten ist zudem kaum überprüfbar.

Der unberechtigte Zugriff auf Daten von entfernten Orten (also z. B. aus dem nichteuropäischen Ausland auf europäische Server) kann zwar eine erhöhte Hürde darstellen, ist aber angesichts der grundsätzlichen internationalen Vernetzung der hier betrachteten Komponenten kein unüberwindbares Hindernis. Zudem ist auch in Europa eine Einflussnahme auf die Mitarbeiter von Netz- bzw. Cloudbetreibern zur Erlangung des Zugriffs vorstellbar.

Um sensible Daten gegen Ausspähung zu schützen, führt kein Weg an einer starken Verschlüsselung – beim Transport und während der Aufbewahrung – vorbei. Dafür sind nicht nur geeignete Algorithmen, sondern auch vertrauenswürdige, zertifizierte Implementierungen und Einsatzumgebungen erforderlich. Für asymmetrische Verschlüsselung beispielsweise können Schlüsselvergabe und -verwaltung sowie Zertifikatsverzeichnisse zwar privatwirtschaftlich organisiert werden, die Vertrauenswürdigkeit der Anbieter muss jedoch sichergestellt sein.

Müssen sensible Daten von Dritten verarbeitet werden, kann dies bisher nur in sehr eingeschränktem Maß auf verschlüsselten Daten erfolgen (homomorphe Verschlüsselung). Die Verarbeitung durch Dritte ist daher nahezu immer mit einer Preisgabe von Datensouveränität verbunden und erfordert ein entsprechendes Vertrauen in den Verarbeiter und seinen Kontext (z. B. rechtliche Regelungen, denen er unterliegt). Mit zwischenstaatlichen Vereinbarungen (wie dem EU-US-Datenschutzschild[48]) kann man zwar versuchen, solches Vertrauen herzustellen, Fakt

[48] EU-U.S. Privacy Shield, http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm bzw. . http://ec.europa.eu/justice/data-protection/files/eu-us_privacy_shield_guide_de.pdf.

bleibt jedoch, dass man bei genügend großem Anreiz im Verhältnis zur Gefahr, zur Rechenschaft gezogen zu werden, fast immer jemanden findet, der bereit ist, einen Rechtsbruch gegen Besitz bzw. Eigentum zu begehen. Gegen staatliche Institutionen wie Geheimdienste sind derartige Vereinbarungen zudem meist völlig wirkungslos.

Vielfach basiert die eingesetzte Verschlüsselung, sowohl was die Verfahren an sich als auch was deren Implementierung betrifft, auf US-amerikanischen Entwicklungen, bei denen es immer wieder Hinweise auf gezielt eingebaute Schwachstellen gibt.[49] Derartigen Problemen kann man nur mit einer verstärkten eigenständigen deutschen bzw. europäischen Forschung und Entwicklung entgegenwirken. Zu berücksichtigen ist auch, dass selbst rechtskonforme staatliche Eingriffe (z. B. zur Verbrechensbekämpfung) in eine verschlüsselte Kommunikation oder verschlüsselt gespeicherte Daten die Sicherheit generell schwächen, da dazu die Unabhängigkeit der Schlüsselverwaltung eingeschränkt oder Schwachstellen geheim gehalten werden müssen.

3.4.4 Wirtschaftlich bestimmte digitale Souveränität

Ein wesentlicher Faktor ist – wie in vielen Wirtschaftsbereichen – der Entwicklungsstand des europäischen Binnenmarktes. Neben uneinheitlichen wirtschaftlichen Regeln hindern nach wie vor unterschiedliche technische Standards und Randbedingungen, aber auch immer noch national orientierte Entscheidungen bei Beschaffungen und Dienstleistungsaufträgen die europäische IT-Wirtschaft daran, optimalen Nutzen aus dem Binnenmarkt zu ziehen. Die auf den kleinen Teilmärkten erzielbaren, vergleichsweise geringen Umsätze machen hohe eigene Forschungs- und Entwicklungsaufwände der Unternehmen, beispielsweise für besonders leistungsfähige Geräte, unrentabel. Hingegen können sich Produzenten mit großen Heimatmärkten (wie den USA, China oder Japan) derartige Aufwände leisten, die ansonsten unversorgten europäischen Märkte mitbedienen und so auch mit Hilfe Europas ihren Vorsprung weiter ausbauen.

Die zunehmende Entwicklung und Bereitstellung wiederverwendbarer sektorbezogener Software, z. B. für öffentliche Einrichtungen über das JoinUp-Portal[50] auf europäischer Ebene, kann die Abhängigkeit von großen kommerziellen Anbietern verringern und wirtschaftlich schwächeren Einrichtungen eine beschleunigte Digitalisierung ermöglichen.

Themen im Zusammenhang mit der Wirtschaftlichkeit der Digitalisierung sind immer wieder der Breitbandausbau und aktuell auch der Aufbau von DVB-T2, des digitalen Fernsehens der 2. Generation. Während beim Breitbandausbau ein politisch gestecktes Ziel – zu dessen Angemessenheit unterschiedliche Ansichten existieren – durch finanzielle Förderung des Bundes[51] unterstützt wird, ist bei DVB-T2 mittelfristig keine flächendeckende Versorgung absehbar.

3.4.5 Gestaltung der Digitalisierung

Die umfängliche Digitalisierung der Gesellschaft ist ein lang andauernder Prozess, bei dem auch zukünftig großer Anpassungsbedarf infolge technischer Entwicklungen auftreten wird.

Um diesen Prozess erfolgreich und zukunftssicher gestalten und umsetzen zu können, ist zunächst ein Grobkonsens zu vielen Einzelaspekten erforderlich, was dort jeweils erreicht werden und wie die Digitalisierung dazu beitragen soll. Im Zuge dieser Konsensbildung muss man unter anderem auch die Querbezüge zwischen den Einzelaspekten ermitteln. Danach ist je nach Rolle ein breites Grundverständnis bis zu vertieftem Wissen

[49] Siehe z. B. die Berichterstattung zum »Dual_EC_DRBG«-Verfahren.

[50] https://joinup.ec.europa.eu/.

[51] http://www.bmvi.de/DE/Themen/Digitales/Breitbandausbau/Breitbandfoerderung/breitbandfoerderung.html.

erforderlich, um zu bestimmen, was die Digitalisierung leisten kann, in welchen Zeiträumen man dies erreichen kann, welche technischen Mittel dafür erforderlich sind, welche Kosten dies verursacht und welcher wirtschaftliche oder gesellschaftliche Nutzen dadurch erreicht werden kann.

Die digitale Souveränität einer Gesellschaft zeigt sich unter anderem darin, dass realistische Digitalisierungsziele gesetzt und dafür geeignete Maßnahmen ergriffen werden. Den vielfältigen Einzelaspekten ist aufgrund des umfangreichen Netzes von Querbezügen in der Regel wenig damit gedient, wenn Zuständigkeiten stark verteilt und gegeneinander abgegrenzt, womöglich sogar als »Besitz« verteidigt werden. So verpufft beispielsweise eine Maßnahme, die Bildungseinrichtungen mit moderner IT ausrüstet, aber keine entsprechende Schulung des Personals ermöglicht.

Die Digitalisierung erfordert auch weiterhin das Infragestellen und gegebenenfalls Aufbrechen von Regeln, Strukturen und Abläufen, die aus einer vordigitalen Realität stammen. Dies reicht vom privaten zwischenmenschlichen Umgang angesichts allgegenwärtiger und ständig verfügbarer Kommunikationsmöglichkeiten bis zu komplexen Fragen der regulativen Vergleichbarkeit klassischer Post-, Telekommunikations- und Rundfunkdienste mit E-Mail, Videotelefonie über einen Anwendungsanbieter und Streaming- bzw. Downloaddiensten.

3.5 NOTWENDIGE KOOPERATION DER AKTEURE

Alle Perspektiven und Facetten digitaler Souveränität erfordern die Kooperation der betroffenen Individuen und Institutionen, der Hersteller und Anbieter und der öffentlichen Hand, um die digitale Souveränität steigern zu können, wie folgende Beispiele exemplarisch zeigen:

- So kann man ein uneingeschränkt veröffentlichtes eigenes Foto oder Firmenprofil nicht selbst wieder »verschwinden« lassen, wenn man es irgendwann peinlich findet. Dazu bedarf es der Unterstützung der speichernden bzw. verarbeitenden Plattformen, der entsprechend ausgestatteten Software anderer Nutzer und der flankierenden Regulierung.
- Andererseits hätte der einzelne Bürger ohne entsprechende gesetzliche Regelungen kaum Chancen, die Speicherung seiner personenbezogenen Daten in Staaten mit schwachem Datenschutz zu verbieten.
- Sicherheitsbewusstsein und Gesetze nützen wiederum nichts ohne geeignete Produkte und Dienstleitungen der IT-Wirtschaft.

4. HANDLUNGSEMPFEHLUNGEN

Im Bereich der digitalen Souveränität besteht umfänglicher Handlungsbedarf. Während im vorangehenden Abschnitt viele Detailbedarfe herausgearbeitet wurden, sind hier die wesentlichen Handlungsfelder – mit besonderem Fokus auf den Zuständigkeiten von Regierung, Legislative und öffentlicher Verwaltung – zusammenfassend beleuchtet.

Die digitale Bildung umfänglich verbessern.
Die digitale Bildung muss in allen Bereichen – Techniknutzung, Mediennutzung, Sicherheit, Auswirkungen der Digitalisierung auf die Lebens- und Arbeitswelt … - und für alle Altersstufen grundlegend reformiert werden. Dazu gehören sowohl die Aktualisierung der Curricula als auch die Modernisierung der technischen Ausstattung, besonderes Augenmerk bedarf aber vor allem die Qualifikation der Lehrenden.

Wirkungsvollen Schutz der Privatsphäre in der digitalen Welt vorschreiben.
Solange Webseiten, Anwendungen und Betriebssysteme nicht so gestaltet sein müssen, dass sie ohne weiteres Zutun der Nutzer deren Privatsphäre standardmäßig bestmöglich respektieren, dass zwischen der funktionsbedingten und der darüber hinausgehenden Erfassung personenbezogener Daten klar unterschieden werden kann und dass die Nutzer gezielt die Erfassung der über das notwendige Maß hinausgehenden personenbezogenen Daten verhindern können, bleibt der Schutz der Privatsphäre in der digitalen Welt ein Lippenbekenntnis.

Gleiches gilt, solange eine tatsächlich informierte Einwilligung das Lesen und Verstehen der gesamten für eine IT-Komponente geltenden Geschäfts- und Nutzungsbedingungen erfordert.

Basiert die informierte Entscheidung eines Nutzers auf bestimmten Nutzungszwecken und einem bestimmten Erfassungs- und Verarbeitungsumfang, dann verliert diese Entscheidung durch eine Änderung der Zwecke oder des Umfangs ihre Grundlage. Deshalb dürfen derartige Änderungen nur wirksam werden, nachdem der Nutzer darauf in jedem konkreten Fall aufmerksam gemacht wurde und die Gelegenheit hatte, seine Entscheidung entsprechend anzupassen.

Das (EU-)Datenschutzrecht aktuell halten.
Der wirtschaftliche Wert personenbezogener und personenbeziehbarer Daten steigt nach wie vor, die Auswertungsmöglichkeiten solcher Daten werden immer komplexer und ausgefeilter. Deshalb ist es notwendig, regelmäßig den Umfang und die Wirksamkeit des Datenschutzrechts zu überprüfen und dieses gegebenenfalls anzupassen.

Die zunehmende externe Speicherung und Verarbeitung von Unternehmens- und Institutionsdaten legt nahe zu prüfen, ob auch hierfür grundlegende Schutzrechte rechtlich verankert werden sollten.

Die Vermeidung von Echokammern unterstützen.
Informationsanbieter und -makler sollten einen Modus bereitstellen, bei dem die Auswahl und die Priorisierung der angebotenen Informationen unabhängig von Kenntnissen über den individuellen Nutzer erfolgen.

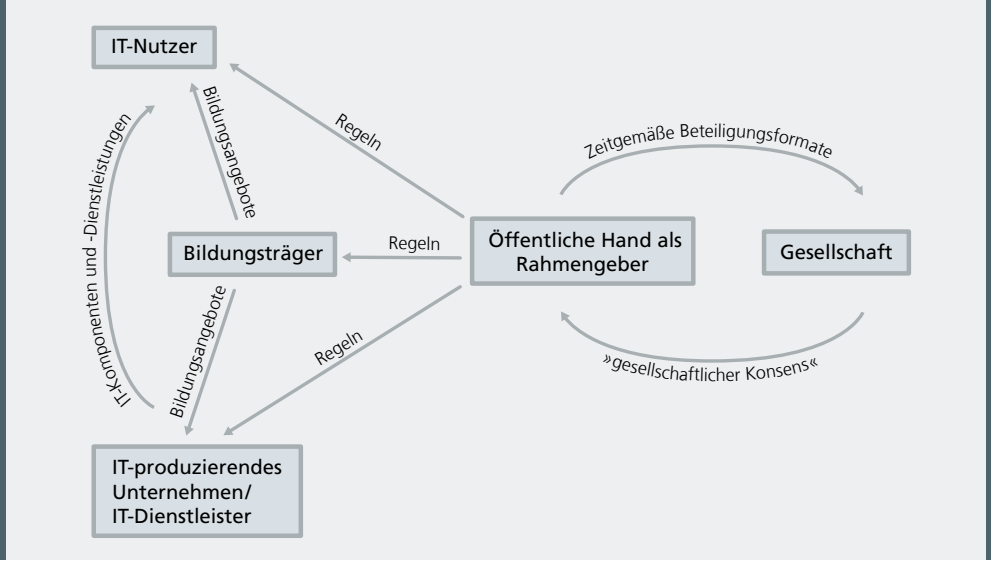
Zur Bereitstellung von Sicherheitsupdates verpflichten.
Analog beispielsweise zum Produkthaftungsgesetz[52] sollten die Hersteller bzw. die Anbieter kommerziell vertriebener Software[53] verpflichtet werden, für innerhalb eines (längeren) Haftungszeitraumes bekannt werdende Sicherheitsmängel Updates bereitzustellen. Der Haftungszeitraum sollte sich angesichts des evolutionären Charakters von Software dabei nicht am Zeitpunkt des erstmaligen Inverkehrbringens der Software (bzw. Softwareversion) orientieren, sondern an dem Zeitpunkt, an dem die allgemeine Weiterentwicklung der Software eingestellt wird. Anbieter sollten Kunden zudem darauf hinweisen müssen, wie lang der verbleibende Haftungszeitraum ist.

Digital souverän beschaffen.
Vordergründig günstige und »bequeme« Paket- und Rahmenvertragslösungen, die eine Bindung an unstandardisierte Schnittstellen, nicht quelloffene Software oder proprietäre Hardware bedeuten, können sich im Nachhinein als teurer Vendor Lock-in oder sogar als Sicherheitsrisiko entpuppen. Ebenso sind die Geschäftsbedingungen insbesondere gebührenfreier Online-Dienstleistungen häufig nicht mit dem Schutz sensibler Daten (Personendaten, Know-how) vereinbar.

---

[52] Produkthaftungsgesetz vom 15. Dezember 1989 (BGBl. I S. 2198), das zuletzt durch Artikel 180 der Verordnung vom 31. August 2015 (BGBl. I S. 1474) geändert worden ist http://www.gesetze-im-internet.de/prodhaftg/ProdHaftG.pdf.

[53] Dazu gehört nach unserem Verständnis auch der gemeinsame Vertrieb vorgeblich kostenlos mitgelieferter Software mit kostenpflichtiger Hardware, auf der die Software eingesetzt wird.



Die IT-Standardisierung Erfolg versprechend fördern.
Nationale und selbst große europäische IT-Standardisierungsaktivitäten gelangen meist nicht zum Durchbruch, wenn es in anderen Regionen (USA, Asien …) konkurrierende Aktivitäten gibt. Man muss also sorgfältig abwägen, ob ein weiteres nationales bzw. europäisches Gremium oder die Beteiligung an einem internationalen Gremium der Sache mehr dient. Zumindest dann, wenn keine starke gemeinsame europäische Position aufgebaut werden kann, ist eine ergebnisorientierte direkte Zuarbeit zu internationalen Gremien oft Erfolg versprechender.

Für die Mitarbeit in internationalen Gremien sollten insbesondere für kleine und mittlere Unternehmen Fördermöglichkeiten geschaffen werden, die nicht an ein Forschungs- und Entwicklungsprojekt im üblichen Sinn gebunden sind.

Die Offenlegung von Informationen zu IT-Sicherheit und -Funktionalität ausbauen.
Die vom BSI veröffentlichten Informationen zu IT-Sicherheit sind eine nützliche Quelle für Institutionen und interessierte Bürger. Hier sollte man prüfen, ob weiteres Material, z. B. Erkenntnisse über tatsächlich erfolgte konkrete Angriffe, publik gemacht werden kann, um die Sensibilität für kritische Sicherheitslücken und entsprechende Gefahren zu erhöhen.

Die angewandte Forschung (auch) entsprechend dem wirtschaftlichen Erfolg der Ergebnisse fördern.
IT-Forschungsförderung ist heutzutage überwiegend anwendungsnah und zielt final auf die Platzierung von Produkten auf dem Markt ab. Deshalb sollten die Ergebnisse auch hinsichtlich ihrer Marktwirkung bewertet werden und die Bewertung stärker in die Förderprogramme einfließen, sowohl bezüglich der geförderten Inhalte als auch hinsichtlich der geförderten Strukturen.

Informationsangebote zur Digitalisierung aufbereiten und thematisch bündeln.
Im Zuge der Digitalisierung bekommen viele Rechtsgebiete eine verstärkte Bedeutung für IT-nutzende Bürger und Institutionen oder die IT-Wirtschaft: Datenschutzrecht, Arbeitsrecht, Urheberrecht … Zum gegenwärtigen Zeitpunkt, zu dem einerseits das relevante Rechtswissen nicht ausreichend verbreitet ist und andererseits die Regulierung selbst laufend an die Digitalisierung angepasst werden muss, sind leicht auffindbare und gut verständliche Informationen für die unterschiedlichen Betroffenen- bzw. Interessentengruppen erforderlich.

Durch die Digitalisierung induzierte Rechtsänderungen auf eine breite gesellschaftliche Basis stellen.
Die Digitalisierung verändert die Arbeitswelt radikal. Die dadurch notwendigen Änderungen z. B. am Arbeits- und Sozialrecht müssen ausgewogen sein und möglichst für alle Beteiligten (Arbeitnehmer, Arbeitgeber, Staat …) positive Effekte bewirken. Deshalb sollten alle betroffenen Interessengruppen in den Rechtsetzungsprozess einbezogen werden, z. B. durch Online-Beteiligungsplattformen, bei denen jeder Vorschläge einbringen und die Vorschläge Anderer kommentieren kann.

W. ROBERT COLTON A.R.A.

GEFÖRDERT VOM

Bundesministerium
des Innern

Fraunhofer
FOKUS

KONTAKT

Gabriele Goldacker
Kompetenzzentrum Öffentliche IT (ÖFIT)
Tel.: +49 30 3463-7173
Fax: +49 30 3463-99-7173
info@oeffentliche-it.de

Fraunhofer-Institut für
Offene Kommunikationssysteme FOKUS
Kaiserin-Augusta-Allee 31
10589 Berlin

www.fokus.fraunhofer.de
www.oeffentliche-it.de
Twitter: @OeffentlicheIT

ISBN: 978-3-9818892-2-2

CC BY

kre | 1711 (Fotos: https://pixabay.com/; Infografiken: ÖFIT)