Die Stärkung der digitalen Souveränität

Wege der Annäherung an ein Ideal im Wandel

Diskussionspapier von iRights.Lab

Autoren: Eike Gräf, Henning Lahmann und Philipp Otto

unter Mitwirkung von Wiebke Glässer, Ulrike Thalheim und Julia Schrader

Mai 2018

Inhaltsverzeichnis

1 Einleitung

Alle wollen, alle sollen digital souverän sein: Staaten wie Deutschland, ganze Staatenverbünde wie die Europäische Union, aber insbesondere auch die einzelnen Nutzerinnen und Nutzer. Dieser Eindruck entsteht, wenn man der aktuellen Debatte folgt. In den vergangenen Jahren hat sich unter dem Stichwort „digitale Souveränität" ein breiter gesellschaftlicher Diskurs über Potenziale, Risiken und Gestaltungsmöglichkeiten der Digitalisierung entfaltet. Unterschiedlichste Akteure nutzen diesen Begriff jeweils mit ganz eigenen Zielsetzungen und Verständnissen. Denn digital souverän zu sein bedeutet für Staaten etwas anderes als für Einzelpersonen. Gerade in Bezug auf letztere wird die Diskussion in jüngster Zeit mit verstärktem Fokus geführt.[1] Doch was genau wird unter „digitaler Souveränität" in den einzelnen Bedeutungskontexten jeweils verstanden? Die Auffächerung des Verständnisses dieses noch nicht eindeutig definierten Konzepts ist Voraussetzung für den weiteren Diskurs und damit insbesondere dafür, dass digitale Souveränität für alle Beteiligten letztlich auch erreicht werden kann. Darum geht es in dem vorliegenden Themenpapier: Es zeigt, wie in der bisherigen Debatte die verschiedenen Nuancen digitaler Souveränität genutzt werden können, um die Digitalisierungspolitik wertebasiert, besonnen und vor allem für Nutzerinnen und Nutzer ergebnisorientiert voranzutreiben. Die digitale Souveränität kann insoweit als wünschenswertes Ziel für ein digitales Miteinander auf den verschiedenen Ebenen festgesetzt werden.

Dieses Papier bietet zunächst einen Überblick über den Begriffsinhalt, über relevante Akteure und den Stand der Debatte (2). Es folgt eine Analyse der Dimensionen, Vorteile und derzeitigen Grenzen des Konzepts der „digitalen Souveränität" (3). Anschließend werden Vorschläge zur Stärkung der digitalen Souveränität aufbereitet und um Ausblicke ergänzt (4). Im Fazit wird zusammengefasst, welche Potenziale eine weiterführende Auseinandersetzung mit dem Konzept der digitalen Souveränität als Zielsetzung bietet (5).

2 Überblick: Die Bedeutung digitaler Souveränität

Wer kann wie und unter welchen Umständen digital souverän sein? Und was bedeutet das konkret? Im Folgenden werden die verschiedenen Interpretationen der digitalen Souveränität dargestellt und es wird erläutert, wer dieses Konzept mit welcher Zielsetzung verwendet. Anschließend wird zusammengefasst, wo heute die größten Herausforderungen bei der Erreichung einer digitalen Souveränität liegen.

[1] Vgl. Abschnitt 2 dieses Papiers

2.1 Begriffsinhalt

Wer „digitale Souveränität" beschreiben will, muss zunächst beim Begriff der Souveränität allgemein ansetzen. Aus der Staatslehre stammend, meint dieser „das unteilbare und unveräußerliche Recht [eines Staates] zur Letztentscheidung sowohl nach innen wie nach außen."[2] Ein souveräner Staat ist in seinen Machtbefugnissen grundsätzlich niemandem unterworfen, und kann eigenständig über seine Gesellschaftsordnung und sein Rechtssystem bestimmen. Er kann beispielsweise Gesetze erlassen und durchsetzen, und außenpolitisch handeln, verhandeln und militärisch aktiv werden. Seit der französischen Revolution liegt der Ursprung dieser Souveränität in jeder modernen Demokratie beim Volk, ganz gleich wie diese institutionell im Einzelnen ausgestaltet ist. Dieser Zustand wird als Volkssouveränität bezeichnet.[3] In einem solchen demokratischen Gesellschaftssystem gewährleistet der Staat so weit wie möglich die Selbstbestimmung der einzelnen Bürgerinnen und Bürger. Ist diese rechtliche Selbstbestimmung der einzelnen Person im staatlichen Gemeinwesen hergestellt und garantiert, so ist auch das Individuum in diesem Sinne als rechtlich souverän zu bezeichnen.

Vereinzelte Debatten über die Bedeutung von Technologie für die nationale Souveränität von Staaten gibt es unter dem Begriff der „technologischen Souveränität" seit den siebziger Jahren.[4] Eine flächendeckende Debatte über die digitale Souveränität Deutschlands und Europas kam allerdings vor allem durch Edward Snowdens Enthüllungen umfangreicher Überwachung durch staatliche Geheimdienste im Jahr 2013 zustande[5], etwa, weil die Abhängigkeit Europas von den USA laut Kritik einem resoluten politischen Vorgehen gegen die Überwachung deutscher Funktionsträger und der deutschen Bevölkerung im Wege stand.[6] Zusätzlich wurden die technologischen Fähigkeiten zum Schutz vor digitalen Eingriffen in Deutschland und Europa kritisch diskutiert.[7] Das Konzept der digitalen Souveränität wurde zu einem *Buzzword* der Digitalisierungspolitik[8] und schaffte es als „technologische Souveränität" 2013 in den Koalitionsvertrag[9] sowie 2014 in die digitale Agenda der Bundesregierung[10].

---

[2] Rüdiger Voigt (2016): *Staatliche Souveränität Zu einem Schlüsselbegriff der Staatsdiskussion*. S.1
[3] Vgl. Voigt (2016) S. 5f.
[4] Vgl. Fokko Misterek (2017): *Technikutopien und Gestaltungsansprüche demokratischer Politik*. MPIfG Discussion Paper 17/11, S.19.
[5] Vgl. Ebd. S.1f.
[6] Vgl. Anna Biselli (2014): *Generalbundesanwalt Range: Wohl keine Ermittlungen gegen Überwachung durch ausländische Geheimdienste* (Update: Antwort). https://netzpolitik.org/2014/generalbundesanwalt-range-wohl-keine-ermittlungen-gegen-ueberwachung-durch-auslaendische-geheimdienste/. Medienbeitrag, abgerufen am 12.02.2018.
[7] Vgl. Mike Friedrichsen und Peter Bisa (2016): *Einführung – Analyse der digitalen Souveränität auf fünf Ebenen.* In: Mike Friedrichsen; Peter Bisa (Hrsg.) (2016): "Digitale Souveränität. Vertrauen in der Netzwerkgesellschaft.*"* S.2ff.
[8] Vgl. Harald Lemke (2013): *Digitale Souveränität – Buzzword oder Aufbruch zu neuen Ufern? Wir brauchen eine schnelle und eindeutige politische Positionierung*. https://www.divsi.de/digitale-souveraenitaet-buzzword-oder-aufbruch-zu-neuen-ufern-wir-brauchen-eine-schnelle-und-eindeutige-politische-positionierung/ Blogbeitrag, abgerufen am 06.02.2018.
[9] Vgl. S.103f des Koalitionsvertrags. https://www.cdu.de/sites/default/files/media/dokumente/koalitionsvertrag.pdf. Abgerufen am 14.02.2018.
[10] Vgl. S.4 und S.32 der Digitalen Agenda 2014-2017. https://www.digitale-agenda.de/Content/DE/_Anlagen/2014/08/2014-08-20-digitale-agenda.pdf?__blob=publicationFile&v=6. Abgerufen am 14.02.2018.

„Digitale Souveränität" kann als Zustand oder Ideal sowohl für Nationalstaaten gelten als auch für ganze Staatenverbünde wie die EU.[11] Auch Einzelpersonen können prinzipiell in ihrer Qualität als Nutzer von Technologie oder als Bürger digital souverän sein. Verbrauchersouveränität in der digitalen Welt wird seit 2007 politisch diskutiert, etwa vom früheren Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz BMELV.[12] Zu den Zielvorgaben der digitalen Agenda 2014-2017 der Bundesregierung gehört explizit die Wiederherstellung der „Souveränität der Verbraucherinnen und Verbraucher auf den digitalen Märkten"[13] und der aktuelle Koalitionsvertrag für die 19. Legislaturperiode hebt digitale Souveränität als „besonders wichtig" hervor[14].

In groben Zügen ähnelt die individuelle digitale Souveränität dem Recht auf informationelle Selbstbestimmung,[15] also dem Recht von Einzelpersonen, grundsätzlich selbst über die Preisgabe und Verwendung ihrer personenbezogenen Daten zu bestimmen.[16] Digitale Souveränität umfasst neben dem Anspruch informationeller Selbstbestimmung aber noch weitere Aspekte, wie beispielsweise die Fähigkeit, digitale Technologien den eigenen Vorstellungen gemäß zu nutzen.

Der Aspekt der Selbstbestimmung ist den meisten Beschreibungen digitaler Souveränität gemein. Eine einheitliche Definition der digitalen Souveränität von Staaten oder Einzelpersonen gibt es jedoch nicht. Verschiedene Diskursteilnehmerinnen und -teilnehmer stellen jeweils unterschiedliche Aspekte in den Vordergrund, von denen die digitale Souveränität ihrer Ansicht nach abhängt. Um einen Überblick zu vermitteln, werden zunächst die wichtigsten inhaltlichen Ansätze zur Beschreibung digitaler Souveränität beispielhaft für verschiedene relevante Zugänge zur Debatte wiedergegeben. Es ist nicht Ziel dieses Themenpapiers, eine allgemeingültige Definition digitaler Souveränität vorzuschlagen, von der sich ableiten ließe, wann ein Staat, ein Unternehmen oder eine Person digital souverän ist. Vielmehr soll gezeigt werden, welche Forderungen und Bedarfe unter Verwendung des Begriffs diskutiert werden und wie sich, je nach Zuschnitt der gewählten Anforderungen an die digitale Souveränität, verschiedene Handlungsanforderungen ergeben. Ein besonderer Schwerpunkt liegt dabei auf der digitalen Souveränität von Nutzerinnen und Nutzern.

---

[11] Vgl. BITKOM (2015): *Digitale Souveränität Positionsbestimmung und erste Handlungsempfehlungen für Deutschland und Europa*. Positionspapier. S.6.
[12] Vgl. Sachverständigenrat für Verbraucherfragen (2017): *Digitale Souveränität. Gutachten des Sachverständigenrats für Verbraucherfragen*. S.2.
[13] Vgl. S.32 der Digitalen Agenda 2014-2017. https://www.digitale-agenda.de/Content/DE/_Anlagen/2014/08/2014-08-20-digitale-agenda.pdf?__blob=publicationFile&v=6. Abgerufen am 14.02.2018.
[14] Ein neuer Aufbruch für Europa. Eine neue Dynamik für Deutschland. Ein neuer Zusammenhalt für unser Land. Koalitionsvertrag zwischen CDU, CSU und SPD, Zeile 1775. Siehe auch Zeile 1618f: „Wir wollen Neugier auf digitale Technologien wecken und Souveränität im Umgang mit ihnen schaffen."
[15] Vgl. Friedrichsen; Bisa (2016) S.2.
[16] Das Recht zur informationellen Selbstbestimmung geht auf ein Urteil des Bundesverfassungsgerichts vom 15.12.1983 zurück (Aktenzeichen 1 BvR 209, 269, 362, 420, 440, 484/83).

Die digitale Souveränität von Nationalstaaten zeichnet sich zunächst durch die Gewährleistung der Integrität der digitalen Infrastruktur aus.[17] Einerseits hängt der Erfolg der Exportnation Deutschland von der hier ansässigen digitalen Expertise ab.[18] Gleichzeitig ist der Staat für die Sicherheit der digitalen Infrastruktur verantwortlich, die wiederum auch für die digitale Souveränität aller Anwenderinnen und Anwender entscheidend ist. Die Medienwissenschaftler Friedrichsen und Bisa zitieren dahingehend den ehemaligen Bundesinnenminister Hans-Peter Friedrich:

> *„Wir können die digitale Souveränität Europas nur dann erhalten, wenn es uns gelingt, in der Zukunft die technologische Souveränität über die Netzinfrastruktur und die Netztechnik zu erlangen und zu verstärken."*[19]

Hier besteht ein starker Zusammenhang sowohl zwischen den Bedarfen von Unternehmen als auch den Fähigkeiten, die zum Großteil von der Wirtschaft entwickelt werden. Die Bundesdruckerei erklärt in diesem Sinne auf ihrer Webseite:

> *„Technologische Souveränität heißt, dass nationale Unternehmen in entscheidenden Bereichen eine Marktposition besitzen, die es ihnen erlaubt, ihre Geschäftsmodelle weiterzuentwickeln und neue Dienstleistungen sicher anzubieten. Dazu gehört, dass bestimmte digitale Schlüsseltechnologien in Deutschland und Europa beherrscht oder zumindest verstanden werden sollten."*[20]

In einem Positionspapier von 2015 blickt auch der Branchenverband Bitkom insbesondere auf die Leistungsfähigkeit der Wirtschaft:

> *„Digital souveräne Systeme verfügen bei digitalen Schlüsseltechnologien und -kompetenzen, entsprechenden Diensten und Plattformen über eigene Fähigkeiten auf internationalem Spitzenniveau. Sie sind darüber hinaus in der Lage, selbstbestimmt und selbstbewusst zwischen Alternativen leistungsfähiger und vertrauenswürdiger Partner zu entscheiden, sie bewusst und verantwortungsvoll einzusetzen und sie im Bedarfsfall weiterzuentwickeln und zu veredeln. Nicht zuletzt sind souveräne Systeme in der Lage, ihr Funktionieren im Innern zu sichern und ihre Integrität nach außen zu schützen."*[21]

Die effektive Entscheidungsgewalt und -kompetenz als Hauptkriterium der digitalen Souveränität findet sich sowohl bei den Ansätzen, die sich auf Staat und Unternehmen beziehen,

---

[17] Vgl. Sachverständigenrat für Verbraucherfragen (2017) S.2.
[18] Vgl. Friedrichsen; Bisa (2016) S.2.
[19] Ebd. S.3.
[20] Der im Zitat verwendete Begriff der technologischen Souveränität bezieht sich auf die Komponente der technologischen Fähigkeiten, denen, wie im Zitat dargestellt, für die weiter gefasste digitale Souveränität eine entscheidende Bedeutung zukommt. Bundesdruckerei: *Digitale und technische Souveränität braucht Rahmenbedingungen.* https://www.bundesdruckerei.de/de/Themen-Trends/Magazin/Digitale-Souveraenitaet-braucht-Rahmenbedingungen Blogbeitrag, abgerufen am 06.02.2018.
[21] BITKOM (2015) S.7.

als auch bei den Konzeptionen, die Einzelpersonen in den Vordergrund stellen. Der Sachverständigenrat für Verbraucherfragen legt in einem Gutachten von 2017 vier Anforderungen fest, die zum Erreichen digitaler Souveränität von Bürgerinnen und Bürgern nötig seien: Wahlfreiheit bei der Nutzung von Diensten, Selbstbestimmung, Selbstkontrolle und Sicherheit.[22] Dabei geht die Definition digitaler Souveränität des Gremiums über die Dimension des reinen Konsumierens hinaus:

> *„Unter Digitaler Souveränität verstehen wir die Handlungsfähigkeit und Entscheidungsfreiheit der Verbraucher, in der Digitalen Welt in verschiedenen Rollen zu agieren, nämlich als Marktteilnehmer, als Konsumentenbürger einer Gesellschaft sowie als „Prosumer"[23] in Netzwerken."*[24]

Diese Entscheidungsfreiheit kann sich insbesondere auch auf Nutzerdaten erstrecken. Die Datensouveränität gilt häufig als Teil der digitalen Souveränität.[25] So schreibt der Politikwissenschaftler Baumann in einem Diskussionsbeitrag für das Deutsche Institut für Vertrauen und Sicherheit im Internet (DIVSI): „Souverän ist, wer entscheiden kann, und digitale Souveränität bedeutet dann, selbst über die Verwendung der eigenen Daten entscheiden zu können."[26]

Die Faktoren, die nötig sind, um die digitale Souveränität von Staat, Unternehmen, oder Einzelpersonen zu stärken, entfalten diverse Wechselwirkungen, weshalb es nötig ist, sie in ihrem Wechselspiel zu erfassen und nicht unabhängig voneinander zu betrachten. Um die Ausgestaltung dieser Faktoren geht es in der politischen Debatte. Nach der hier folgenden Übersicht der Diskursteilnehmerinnen und -teilnehmer werden der Stand der Debatte und eine Auswahl zentraler Herausforderungen diskutiert.

2.2 Akteure

Die Relevanz des Konzepts der digitalen Souveränität für den gegenwärtigen politischen Diskurs äußert sich insbesondere darin, dass diverse Akteure das Konzept als wichtigen Bestandteil der Digitalisierungspolitik definieren. Die folgende Auswahl vermittelt einen Eindruck davon, welche Personen und Strukturen sich in Deutschland schwerpunktmäßig mit der digitalen Souveränität auseinandersetzen.[27]

---

[22] Vgl. Sachverständigenrat für Verbraucherfragen (2017) S. 3.
[23] Der Begriff der „Prosumer" ist ein Kofferwort aus „Produzent" und „Konsumer". Es versinnbildlicht den Umstand, dass oft unklar ist, welche dieser Rollen wir im Internet einnehmen, und dass wir oft beide Rollen zugleich innehaben, etwa wenn wir ein soziales Netzwerk nutzen und dabei Inhalte erstellen und dort veröffentlichen.
[24] Ebd. S. iv..
[25] Stefan Werden (2016*): Digitale Souveränität, ein Orientierungsversuch*. In: Mike Friedrichsen; Peter Bisa (Hrsg.) (2016): "Digitale Souveränität. Vertrauen in der Netzwerkgesellschaft. "S.35.
[26] Max-Otto Baumann (2015): *Privatsphäre als neues digitales Menschenrecht? Ethische Prinzipien und aktuelle Diskussionen.* Diskussionsbeitrag für das Deutsche Institut für Vertrauen und Sicherheit im Internet (DIVSI), S. 32.
[27] Die Auswahl beruht im Wesentlichen auf der Sichtbarkeit im Diskurs und stellt keine qualitative Gewichtung dar.

2.2.1 Politik

Neben Sigmar Gabriel[28], Brigitte Zypries[29], Thomas de Maizière[30] und Alexander Dobrindt[31], den Ministern der vergangenen Legislaturperiode, die sich als politisch Verantwortliche mit netzpolitischen Themen befassten, hat sich eine Reihe weiterer Politiker zum Thema digitale Souveränität geäußert. In einer beispielhaften Aufzählung lassen sich unter anderem Netzpolitiker wie Lars Klingbeil (SPD), Jimmy Schulz (FDP) und Thomas Jarzombek (CDU), sowie der Europapolitiker Jan-Philipp Albrecht (Bündnis 90/Die Grünen) oder auch Peter Tauber (CDU) und Dorothee Bär (CSU) erwähnen.[32]

2.2.2 Ministerien

Im Bereich der Ministerien sind das Bundesministerium für Wirtschaft und Energie (BMWi), das Bundesministerium der Justiz und für Verbraucherschutz (BMJV) und das Bundesministerium für Verkehr und digitale Infrastruktur (BMVI) besonders um die digitale Souveränität bemüht. So hat sich das BMWi 2015 anlässlich des IT-Gipfels mit den Leitplanken digitaler Souveränität[33] befasst und 2017 eine Studie zu den „Kompetenzen für eine digitale Souveränität" beauftragt.[34] Das BMWi und das BMJV haben 2015 einen gemeinsamen Maßnahmenkatalog mit dem Titel „Mehr Sicherheit, Souveränität und Selbstbestimmung in der digitalen Wirtschaft" veröffentlicht, der auf die digitale Souveränität von Anwenderinnen und Anwendern abzielt.[35] Mit dieser Dimension befasst sich auch der Sachverständigenrat für Verbraucherfragen, der 2014 vom BMJV eingerichtet wurde.[36] Das BMVI positioniert sich seit 2017 auf seiner Webseite mit mehreren Strategiepapieren[37] zur digitalen Souveränität

---

[28] Vgl. DIVSI (2016): *Die Digitalisierung ist eine der wichtigsten Veränderungen unserer Zeit.* Interview mit Sigmar Gabirel. DIVSI-Magazin 2/2016, S.6.
[29] Vgl. Pressemitteilung des Forschungszentrums für Informatik am Karlsruher Institut für Technologie (2017): https://www.presseportal.de/pm/126556/3660042 Abgerufen am 06.02.2018.
[30] Vgl. Thomas de Maizière (2018): *Soft- und Hardware-Hersteller in die Verantwortung nehmen.* https://www.bmi.bund.de/SharedDocs/kurzmeldungen/DE/2018/01/statement-chipsicherheitsmaengel.html Meldung des BMI, abgerufen am 06.02.2018.
[31] Vgl. Alexander Dobrindt (2013): *Digitale Souveränität zurückgewinnen.* https://www.bundesregierung.de/Content/DE/Interview/2013/12/2013-12-23-dobrindt-bams.html Interview, abgerufen am 06.02.2018.
[32] Sie alle trugen Kapitel zu einem Sammelband bei. Vgl. Friedrichsen; Bisa (2016) S. 113, 119, 137, 143, 153 und 161.
[33] Vgl. BMWi (2015): *Leitplanken Digitaler Souveränität*. https://www.de.digital/DIGITAL/Redaktion/DE/Downloads/it-gipfel-2015-leitplanken-digitaler-souveraenitaet.pdf?__blob=publicationFile&v=1 Diskussionspapier, abgerufen am 06.02.2018.
[34] FZI Forschungszentrum Informatik, Accenture GmbH, Bitkom Research GmbH (2017): *Kompetenzen für eine digitale Souveränität.*
[35] Das Maßnahmenprogramm wird auf der Webseite des BMWi verfügbar gehalten. https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/massnahmenprogramm-sicherheit-souveraenitaet-selbstbestimmung-digitale-wirtschaft.html. Abgerufen am 14.02.2018.
[36] Vgl. Webseite des BMJV. https://www.bmjv.de/DE/Ministerium/ForschungUndWissenschaft/Sachverstaendigenrat/Sachverstaendigenrat_node.html, abgerufen am 14.02.2018.
[37] Die Strategiepapiere werden auf der Webseite des Ministeriums bereitgehalten. https://www.bmvi.de/SharedDocs/DE/Artikel/K/dobrindt-strategie-fuer-digitale-souveraenitaet.html, abgerufen am 06.02.2018.

und befürwortet unter anderem ein neues Datengesetz[38], das den Umgang mit Daten grundsätzlich neu regeln soll. Während sich das Bundesministerium für Bildung und Forschung (BMBF)[39], das BMVI und das BMWi mit Bestandsaufnahmen und Vorschlägen zur Stärkung der digitalen Souveränität einbringen, konzentrieren sich das Bundesministerium des Innern (BMI) und das Bundesamt für Sicherheit in der Informationstechnik (BSI) vor allem auf den Aspekt der digitalen Sicherheit[40]. Die große Bedeutung der digitalen Souveränität für die deutsche Digitalisierungspolitik ist zudem daran erkennbar, dass das BMWi ein eigenes Referat mit Fragen der digitalen Souveränität betraut hat.[41]

Auch die Länder befassen sich mit der Stärkung der digitalen Souveränität.[42] Von einer detaillierten Auflistung der einzelnen Landesministerien sowie weiteren Behörden wird hier jedoch abgesehen.

2.2.3 Vereine, Verbände und Zivilgesellschaft

Auch die Vereine und Verbände aus dem Gebiet der Digitalisierung befassten sich in den letzten Jahren mit dem Konzept der digitalen Souveränität und speisen fortlaufend ihre Positionen in den Diskurs ein.

So führt der Branchenverband Bitkom ein eigenes Onlinedossier[43] zu digitaler Souveränität und hat 2015 ein Positionspapier[44] veröffentlicht. Zudem ist der Verband gemeinsam mit anderen Akteuren an Ausarbeitungen zum Thema beteiligt, wie etwa dem auf bildungspolitische Aspekte fokussierten Papier „Digitale Souveränität leben! Herausforderungen an das deutsche Bildungssystem“ für den Nationalen Digitalgipfel 2017.[45]

---

[38] Vgl. BMVI: *Wir brauchen ein Datengesetz in Deutschland!* https://www.bmvi.de/SharedDocs/DE/Artikel/DG/datengesetz.html Beitrag auf der Webseite des BMVI, abgerufen am 06.02.2018.
[39] Das BMBF sieht vermehrte Forschung zur Stärkung der digitalen Souveränität vor. Vgl. BMBF (2016): *Selbstbestimmt und sicher in der digitalen Welt 2015-2020. Forschungsrahmenprogramm der Bundesregierung zur IT-Sicherheit.* S.24.
[40] Vgl. BSI (2017): *Die Lage der IT-Sicherheit in Deutschland 2017* sowie Bernd Kowalski (2016): *Schriftliche Stellungnahme zur öffentlichen Anhörung „Entwurf eines Gesetzes zur Digitalisierung der Energiewende“ im Ausschuss für Wirtschaft und Energie am Mittwoch, den 13. April 2016.*
[41] Vgl. Organisationsplan auf der Webseite des BMWi, abgerufen am 06.02.2018. https://www.bmwi.de/Redaktion/DE/Downloads/M-O/organisationsplan-bmwi.pdf?__blob=publicationFile&v=136
[42] Vgl. beispielsweise die *Digitale Agenda für das Land Sachsen Anhalt* vom 19.12.2017, S.4.
[43] https://www.bitkom.org/Themen/Politik-Recht/Digitale-Souveraenitaet/index.jsp, abgerufen am 06.02.2018.
[44] Vgl. BITKOM (2015).
[45] Arbeitsgruppe 1 „Digitale Bildungsplattformen: Innovationen im Bildungsbereich“ Plattform „Digitalisierung in Bildung und Wissenschaft“ des Nationalen Digitalgipfels (2017): *Digitale Souveränität leben! Herausforderungen an das deutsche Bildungssystem.*

Der Bundesverband der Deutschen Industrie (BDI) befasst sich in einem Grundsatzpapier von 2016 insbesondere unter den Gesichtspunkten der Anwenderkompetenz, des Standortwettbewerbs und der Cybersicherheit mit dem Thema.[46]

Der Zentralverband Elektrotechnik- und Elektronikindustrie legt in einem Diskussionspapier zur digitalen Souveränität von 2015 den Schwerpunkt auf die Stärkung der digitalen Infrastruktur.[47]

Der Sachverständigenrat für Verbraucherfragen gab 2016 mehrere Studien zur digitalen Souveränität aus Verbraucherperspektive in Auftrag, etwa bei der Open Knowledge Foundation Deutschland, die sich dem ökonomischen Wert von Daten widmete.[48] Eine weitere Studie für den Rat zu technologischen Aspekten der digitalen Souveränität, erstellt von Rüdiger Weis, Stefan Lucks und Volker Grassmuck, wurde beim Jahreskongress 2016 des Chaos Computer Clubs (CCC) vorgestellt und diskutiert.[49] Auf diese Studien nimmt der Rat auch in seinem eigenen Gutachten von 2017 mit Vorschlägen zur Stärkung der digitalen Souveränität Bezug.[50]

Neben der Open Knowledge Foundation und dem Chaos Computer Club befassen sich weitere Akteure aus der Zivilgesellschaft mit der Debatte zur digitalen Souveränität. So hat beispielsweise die Redaktion von netzpolitik.org, die sich als eine „Plattform für digitale Freiheitsrechte“[51] beschreibt, Debattenbeiträge des Bitkom kommentiert[52] und die Wahlprogramme zur Bundestagswahl 2017 unter dem Gesichtspunkt „Verbraucherschutz und digitale Souveränität“[53] untersucht.

2.2.4 Wissenschaft

In der Wissenschaft findet das Konzept der digitalen Souveränität interdisziplinär Beachtung. Der Sammelband „Digitale Souveränität. Vertrauen in der Netzwerkgesellschaft“ von Friedrichsen und Bisa von 2016 vereint zum Beispiel eine Reihe überwiegend politischer

---

[46] Bundesverband der Deutschen Industrie e. V. (2016): *Grundsatzpapier Cybersicherheit. Voraussetzungen für die digitale Souveränität in Deutschland und Europa.*
[47] Vgl. Zentralverband Elektrotechnik - und Elektronikindustrie e. V. (2015): *Stärkung vertrauenswürdiger IT - Infrastrukturen in Deutschland und Europa*.
[48] Sachverständigenrat für Verbraucherfragen (2017a): *Der Wert persönlicher Daten. Ist Datenhandel der bessere Datenschutz?*
[49] Der Vortrag ist auf der Webseite des CCC als Video verfügbar: https://media.ccc.de/v/33c3-8097-technologien_fur_und_wider_digitale_souveranitat. Abgerufen am 14.02.2018.
[50] Vgl. Sachverständigenrat für Verbraucherfragen (2017).
[51] So steht es auf der Webseite von netzpolitik.org: https://netzpolitik.org/ueber-uns/, abgerufen am 14.02.2018.
[52] Vgl. Anna Biselli (2015): Realitätscheck: *BITKOM-Position zu Digitaler Souveränität – An Open Source denkt leider keiner.* https://netzpolitik.org/2015/realitaetscheck-bitkom-position-zu-digitaler-souveraenitaet-an-open-source-denkt-leider-keiner/. Bogbeitrag, abgerufen am 14.02.2018.
[53] Vgl. Ingo Dachwitz (2017): *Der netzpolitische Wahlprogramm-Vergleich, Teil 9: Verbraucherschutz und digitale Souveränität.* https://netzpolitik.org/2017/der-netzpolitische-wahlprogramm-vergleich-teil-9-verbraucherschutz-und-digitale-souveraenitaet/. Blogbeitrag, abgerufen am 14.02.2018.

Beiträge. Der Sammelband „Digitale Souveränität. Bürger, Unternehmen, Staat“ von Wittpahl von 2017 geht insbesondere auch auf wirtschaftliche und soziologische Aspekte ein. Zudem beteiligen sich Forschungseinrichtungen wie das Max-Planck-Institut für Gesellschaftsforschung oder die Fraunhofer-Gesellschaft mit Diskussionspapieren an der Debatte zu den normativen Implikationen[54] digitaler Souveränität sowie zu Fragen der technischen Architektur[55], die solch eine Souveränität begünstigen könnte. Die Forschung zum Gegenstand der digitalen Souveränität, hat ihren Weg in den deutschen Wissenschaftsbetrieb gefunden. Das neue Deutsche Internet-Institut, das Weizenbaum-Institut für die vernetzte Gesellschaft, nennt im Zuge seiner Eigendarstellung die digitale Souveränität, neben Aspekten wie Demokratie oder Partizipation, als einen der Gesichtspunkte, unter denen die geplante Forschung am neuen Institut durchgeführt werden soll.[56]

2.3 Stand der Debatte und aktuelle Herausforderungen

Der Stand der Debatte lässt sich gut mittels der Fähigkeiten, Bedingungen, Anforderungen und Herausforderungen verdeutlichen, die die verschiedenen Diskursteilnehmer derzeit als Notwendigkeiten zur Erreichung eines Zustands digitaler Souveränität anführen. Ein weiterer wichtiger Teil der Debatte sind zudem Vorschläge und Ansätze, wie der Status Quo in Richtung eines Zustands digitaler Souveränität verändert werden kann. Dies wird nach der folgenden Darstellung der Bedarfe und Herausforderungen in Abschnitt 4 gesondert thematisiert. Die prominentesten Punkte werden hier in Kurzform dargestellt, um einen schnellen Überblick zu ermöglichen. Die Auswahl beruht im Wesentlichen auf der Sichtbarkeit im Diskurs und stellt keine qualitative Gewichtung dar.

- Spionage mittels digitaler Kanäle, sowohl zwischen Staaten als auch in der Wirtschaft, stellt nach wie vor eine unbewältigte Herausforderung für die digitale Souveränität Deutschlands dar.[57]
- Die Sicherheit vor digitaler Kriminalität (etwa in Form von Computerviren wie Ransomware, Identitätsdiebstahl, Botnetzen usw.) ist strukturell noch nicht gewährleistet.[58]

[54] Vgl. Misterek (2017).
[55] Vgl. Boris Otto (2016): *Digitale Souveränität. Beitrag des Industrial Data Space.* https://www.isst.fraunhofer.de/content/dam/isst/de/documents/Publikationen/StudienundWhitePaper/Fraunhofer-Digitale-Souver%C3%A4nit%C3%A4t-IDS_102016.pdf, abgerufen am 07.02.2018
[56] Vgl. die Webseite des Instituts, https://vernetzung-und-gesellschaft.de/, abgerufen am 14.02.2018.
[57] Vgl. Dirk Graudenz (2014): *Bedroht und bereits verletzt. Der Blick auf den Status quo. Zehn Punkte, die uns alle zum Nachdenken anregen sollten. Das Fazit: Es wird höchste Zeit, Lösungen zu finden.* Medienbeitrag im DIVSI Magazin 01/2014, S.14.
[58] Vgl. Sachverständigenrat für Verbraucherfragen (2017) S.1.

- Wirtschaftliche Abhängigkeiten bei der Verfügbarkeit und Entwicklung von Schlüsseltechnologien stellen ein Hindernis für die Selbstbestimmung dar.[59]

- Die Marktmacht von (ausländischen und außereuropäischen) Monopolen schränkt die Wahlmöglichkeiten der Unternehmen und Anwenderinnen und Anwender ein.[60]

- Die Privatisierung der Öffentlichkeit in Form einer Konzentration auf wenige stark frequentierte Onlineplattformen ist problematisch. Da Onlineplattformen private Anbieter sind, können sie die Inhalte, die sie bereithalten, kontrollieren, gewichten und gegebenenfalls zensieren.[61]

- Die Medienkompetenz vieler Internetnutzerinnen und Internetnutzer ist in vielen Bereichen noch verbesserungsbedürftig.[62] Dies gilt gleichermaßen für die private wie für die berufliche Medienkompetenz.

- Selbst im Fall von Menschen mit hoher Medienkompetenz bestehen signifikante Informations- und Machtasymmetrien zwischen Onlineplattformen und Nutzerinnen und Nutzern.[63] So sind die Geschäftsbedingungen und Datenschutzerklärungen der meisten Anbieter enorm umfangreich und schwer verständlich. Häufig herrscht zudem Intransparenz bezüglich der Verarbeitung personenbezogener Daten. Kontrollmöglichkeiten für Anwenderinnen und Anwender gibt es diesbezüglich ebenso nur äußerst selten.

- Es herrscht ein hoher Gruppenzwang, der dazu drängt, trotz weithin bekannter Machtungleichgewichte und dem Mangel an Kontrolle über die Datenverarbeitung, Soziale Netzwerke und andere Plattformen weiterhin zu nutzen. Eine Entscheidung dagegen ist angesichts der Lebensumstände vieler Anwenderinnen und Anwender unrealistisch.[64]

---

[59] Vgl. Graudenz (2014) S.14.
[60] Vgl. Baumann (2015) S.37; Harald Schumann, Elisa Simantke (2017): *Europas fatale Abhängigkeit von Microsoft Die Cyber-Attacke mit "Wanna Cry" erfolgte über eine Sicherheitslücke bei Microsoft. Alle EU-Staaten nutzen Software des US-Konzerns. Das ist auch politisch höchst riskant. Eine Analyse.* http://www.tagesspiegel.de/weltspiegel/sonntag/cyber-attacken-auf-staatliche-it-europas-fatale-abhaengigkeit-von-microsoft/19628246.html Medienbeitrag, abgerufen am 16.02.2018
[61] Zur Bedeutung der Gewichtung bei der Verbreitung vom Inhalten vgl. Konrad Lischka und Christian Stöcker (2018): *Digital public: looking at what algorithms actually do.* https://theconversation.com/digital-public-looking-at-what-algorithms-actually-do-91119 . Artikel in einem Onlinemagazin, abgerufen am 07.02.2018.
[62] Vgl. Initiative D21 e.V. (2018): *D21 Digital Index 2017/2018. Jährliches Lagebild zur Digitalen Gesellschaft.* S.21ff.
[63] Vgl. Sachverständigenrat für Verbraucherfragen (2017) S.1.
[64] Vgl. Baumann (2015) S.34f sowie Sachverständigenrat für Verbraucherfragen (2017) S.1.

3 Einordnung: Ein fließendes Konzept

Unabhängig von einer präzisen Definition des Konzepts, die es noch zu finden gilt, besteht im Diskurs dahingehend Einigkeit, dass digitale Souveränität einen erstrebenswerten Zustand darstellt. Zugleich handelt es sich aber um einen Begriff, der auf vielfältige Arten als politisches Programm eingesetzt werden kann. Es ist daher sinnvoll, sich die Vielschichtigkeit dieses Begriffs zu verdeutlichen, bevor man sich mit Ansätzen zur Stärkung der digitalen Souveränität befasst.

3.1 Der Daseinszweck der digitalen Souveränität

Die gemeinsame Betrachtung der oben zusammengetragenen Aspekte legt nahe, dass eine strikte Unterscheidung zwischen nationalstaatlicher digitaler Souveränität und jener, die sich auf Unternehmen oder Einzelpersonen bezieht, nicht zweckdienlich ist, da sich die Herausforderungen auf mehreren Ebenen stellen und vielfältige Zusammenhänge bestehen. Dass sich das Konzept der digitalen Souveränität auf verschiedene Entitäten beziehen kann, ist konzeptuell nicht problematisch, sondern trägt unter anderem dem Umstand Rechnung, dass die Souveränität des Einzelnen im Sinne von Freiheit, Selbstbestimmung, Status als Rechtssubjekt, und dem Erwerb der für souveränes Handeln nötigen Kompetenzen und Möglichkeiten nur von einem souveränen Staat ermöglicht werden kann, wobei es zur tatsächlichen Erfüllung dieser verschiedenen Potenziale zusätzlich der Mitwirkung weiterer gesellschaftlicher Akteure, wie etwa einer freien Presse, bedarf.[65]

Ein Beispiel hierfür ist die angestrebte Stärkung der digitalen Souveränität des Einzelnen durch das sogenannte „Recht auf Vergessenwerden". Nach einem Urteil des Europäischen Gerichtshofs[66] haben Einzelpersonen unter bestimmten Umständen die Möglichkeit, Suchergebnisse, die in Bezug auf den eigenen Namen angezeigt werden, vom Suchmaschinenbetreiber unterbinden zu lassen. Diese Stärkung der Selbstbestimmung der Nutzerinnen und Nutzer hängt von der digitalen Souveränität der europäischen Nationalstaaten und der EU ab. Das Urteil aus Europa stößt seitens der USA auf massive Widerstände, etwa weil die Suchmaschinenbetreiber sich ihrerseits in ihrer Selbstbestimmung beschränkt sehen und zudem laut US-Gesetz den Grundsatz der Ausdrucksfreiheit gewährleisten müssen, der mit der neuen Regelung nicht ohne weiteres vereinbar ist.[67] Dass das sogenannte Recht auf Vergessenwerden auf dem Gebiet der EU umgesetzt wird, lässt sich als direkte Folge der Souveränität der EU und ihrer Mitgliedsstaaten auffassen.

[65] Vgl. Ebd.
[66] Vgl. Urteil des Europäischen Gerichtshofs 2014 in der Rechtssache C - 131/12.
[67] Vgl. Rory Cellan-Jones (2014): *US v Europe - a cultural gap on the right to be forgotten. http://www.bbc.co.uk/news/technology-27421969.* Medienbeitrag, abgerufen am 12.02.2018.

Die digitale Souveränität ist kein Selbstzweck, sondern dient in der digitalen Zeit dem breiteren demokratischen Ideal vom selbstbestimmten Leben und einem Staat, der eben dies prinzipiell gewährleisten soll. Für Misterek schließt dieses Souveränitätskonzept mit ein, dass...

> *„... der Einfluss des jeweiligen Demos auf die Ausgestaltung der Digitalisierung gewährleistet ist. Digitale Souveränität als politisches Programm bedeutet also grundsätzlich die Unterordnung der Dynamik der Digitalisierung unter das Primat der Politik."*[68]

Will man sich dieser Auffassung anschließen, heißt das, dass die digitale Souveränität eine weitere Bedeutungsebene aufweist: neben die selbstbestimmte Entscheidungsgewalt innerhalb der eigenen digitalen Umwelt tritt der Anspruch auf demokratische Mitgestaltung dieser digitalen Umwelt. Je nachdem, wie breit man den Begriff der digitalen Souveränität konzipiert, ergeben sich also unterschiedliche Zielsetzungen. Und von diesen Zielsetzungen hängt wiederum ab, welche Vorschläge zur Stärkung der digitalen Souveränität am ehesten Erfolg versprechen.

3.2 Stärken und Grenzen des Konzepts

Obwohl für ein bewusstes und zielgerichtetes Ansteuern eines Zustands der digitalen Souveränität ausschlaggebend ist, wie umfassend man dieses Konzept begreift, eignet sich das Konzept gerade wegen seiner Vielschichtigkeit als Identifikationsanker für eine große Bandbreite von Akteuren, die ihrerseits ganz verschiedene Schwerpunkte setzen mögen. Hinter dem Begriff können sich vielfältige Akteure vereinen, um über Detailfragen der Auslegung und Ausgestaltung zu streiten. Das hat den Vorteil, dass viele wertvolle Perspektiven und Aspekte in die Debatte aufgenommen werden können, von der Positionierung Europas in der Welt bis hin zu Fragen der Medienkompetenz.[69] Diese vielen Bedeutungsebenen können dabei durchaus ein großes Ganzes ergeben. Um Ordnung in diese Vielfalt zu bringen, und etwa Synergien zwischen verschiedenen Bemühungen zu ermöglichen, muss man sich mit der Debatte in ihrer gesamten Breite auseinandersetzen.

Neben diesem Vorteil, der letztendlich in der leichten Unschärfe des Konzepts der digitalen Souveränität begründet ist, gibt es allerdings ebenso Unklarheiten, die eher hinderlich sind. Hier stößt das Konzept bezüglich seiner Eignung als Zielvorgabe an seine Grenzen, weil unklar ist, welcher Zustand im Einzelnen als „digital souverän" gelten kann. Ein Beispiel ist der Teilbereich der Datensouveränität, also die Bestimmungsgewalt darüber, was mit den „eigenen" Daten geschieht.[70] Zum einen wird aktuell debattiert, ob Daten etwa eine

[68] Misterek (2017) S.25.
[69] Vgl. Friedrichsen; Bisa (2016).
[70] Der Sachverständigenrat für Verbraucherfragen beschreibt Datensouveränität wie folgt: "Den Begriff der Datensouveränität, der ein weiteres zentrales Konzept in der verbraucherpolitischen Debatte beschreibt, integrieren wir als eine

Eigentumsfähigkeit aufweisen.[71] Während das BMVI sich für die Festschreibung einer solchen Eigentumsfähigkeit in einem neuen Datengesetz ausgesprochen hat,[72] sehen Datenschützer eine Unvereinbarkeit einer Eigentumsfähigkeit personenbezogener Daten mit dem geltenden Recht und den Prinzipien des Datenschutzes.[73] Zudem ist ebenso unklar, was einzelne Daten wert sind, da ihr Wert vom Kontext, der Art der Aggregation und Nutzungsweise und weiteren Faktoren abhängt.[74] Darüber hinaus ist auch noch nicht geklärt, wer genau Zugriff auf welche Daten haben sollte, und unter welchen Umständen.[75] So hätten beispielsweise im Bereich der Logistik diverse Akteure ein berechtigtes Interesse am Eigentum oder zumindest dem Zugriffsrecht an Mobilitätsdaten: Fahrzeugnutzer, Fahrzeughalter, Fahrzeughersteller, Zulieferer, Infrastrukturbetreiber, Versicherer usw. Bei allen Daten zu Kommunikation zwischen Personen kann es zudem prinzipiell mehrere interessierte Parteien geben. Während das Konzept der Datensouveränität also eine Selbstbestimmungsfähigkeit über die „eigenen Daten" postuliert, ist oft unklar, wem diese Daten letztendlich eigen sind. Das gilt unabhängig davon, ob dies Eigentumsrechte mit einschließt oder nicht. Es hat sich noch keine akzeptierte Norm herausgebildet. Diese Frage stellt vorläufig noch eine Lücke im Konzept der Datensouveränität und somit der digitalen Souveränität dar. Dies und eventuelle weitere Lücken sollten bei der Entwicklung von Ansätzen zur Stärkung der digitalen Souveränität unbedingt berücksichtigt werden.

4 Ausblick: Möglichkeiten zur Stärkung der digitalen Souveränität

Wenn Bemühungen, die digitale Souveränität zu stärken, Synergien aufweisen und eine kohärente Strategie ergeben sollen, ist es wichtig, das zugrundeliegende Verständnis digitaler Souveränität und ihrer Zielsetzungen genau abzustecken und den Kontext, in dem die jeweiligen Bemühungen angestrengt werden sollen, zuvor genau zu betrachten. Im Folgenden werden daher Ansätze zur Stärkung der digitalen Souveränität dargestellt und in einem weiteren Abschnitt um eine Übersicht aktueller Entwicklungen ergänzt, die für die jeweilige Sinnhaftigkeit und Ausgestaltungsmöglichkeiten der präsentierten Ansätze eine hohe Bedeutung aufweisen.

---

wichtige Ausprägung von Digitaler Souveränität in unser Konzept, nämlich als die Wahlfreiheit von Verbrauchern über Erhebung, Verarbeitung und Nutzung ihrer persönlichen Daten." Sachverständigenrat für Verbraucherfragen (2017) S.2.

[71] Vgl. Nicola Jentzsch (2018): *Dateneigentum – Eine gute Idee für die Datenökonomie?* https://www.stiftung-nv.de/sites/default/files/nicola_jentzsch_dateneigentum.pdf. Impulspapier, abgerufen am 07.02.2018.

[72] Vgl. BMVI: *Wir brauchen ein Datengesetz in Deutschland!* https://www.bmvi.de/SharedDocs/DE/Artikel/DG/datengesetz.html Beitrag auf der Webseite des BMVI, abgerufen am 06.02.2018.

[73] European Data Protection Supervisor (2017): *Opinion 4 /2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content.*

[74] Vgl. Jentzsch (2018) sowie Sachverständigenrat für Verbraucherfragen (2017) S.8f.

[75] Vgl. Valerie Peugeot (2014): *Données personnelles : sortir des injonctions contradictoires. https://vecam.org/archives/article1289.html* Blogbeitrag, abgerufen am 12.02.2018.

4.1 Ansätze zur Stärkung der digitalen Souveränität

So wie oben bei der Auswahl der wichtigsten Herausforderungen auf dem Weg zur digitalen Souveränität, werden auch die Lösungsansätze hier in Kurzform dargestellt, um einen schnellen Überblick zu ermöglichen. Die verschiedenen Ansätze können sich jeweils schwerpunktmäßig auf Einzelpersonen, Unternehmen oder ganze Systeme beziehen. Vielfach ergeben sich Synergien zwischen einzelnen Faktoren. So profitieren beispielsweise auch Unternehmen und Staaten von einer weit verbreiteten hohen individuellen Medienkompetenz. Denn diese erlaubt es, sowohl Mitarbeiterinnen und Mitarbeiter als auch Anwenderinnen und Anwender in ihr Streben nach struktureller digitaler Souveränität einzubinden.

4.1.1 Technologie

Die Entwicklung und Ausgestaltung von Technologie ist entscheidend für die digitale Souveränität. Entsprechend gibt es diverse Ansätze, um mit Hilfe von Technologie die digitale Souveränität zu stärken. Dazu gehören:

- Der Aufbau eigener deutscher und europäischer „Fähigkeiten zur Entwicklung, Herstellung und Veredelung digitaler Schlüsseltechnologien, Dienste und Plattformen".[76] Dies benötigt kollektive Bemühungen, die durch eine intelligente Zusammenarbeit, Koordination und Förderung erleichtert werden können. Gemeinsame Forschungsprojekte und Investitionen der Wirtschaft sind geeignet, diesen Ansatz voranzutreiben.

- Der Aufbau und Erhalt von „Fähigkeiten zur Prüfung und Bewertung digitaler Technologien, Dienste und Plattformen unter Leistungs- und Sicherheitsaspekten."[77] Dies schließt eine gründliche und fortlaufende Aufklärung über bereits bekanntgewordene Schwachstellen und Verwundbarkeiten mit ein und ist somit ein ebenso kultureller wie technologischer Aspekt.

- Die Umsetzung der Datenschutzprinzipien „Privacy by Design" und „Privacy by Default" bei der Entwicklung neuer Produkte und Angebote für Einzelpersonen. Der Sachverständigenrat für Verbraucherfragen spricht sich dafür aus, dass staatlich geförderte Projekte sich an diesen Prinzipien orientieren sollen.[78]

[76] Vgl. BITKOM (2015) S.3.
[77] Ebd.
[78] Vgl. Sachverständigenrat für Verbraucherfragen (2017) S.iv.

- Eine besondere Berücksichtigung der Sicherheit von Produkten und Angeboten. Gerade im aufkommenden „Internet der Dinge" belegen regelmäßig auftretende Schäden durch Sicherheitsdefizite den erhöhten Verbesserungsbedarf.[79] Die aktuelle Debatte über eine Herstellerhaftung für vernetzte Objekte ist diesbezüglich hoch relevant.[80]

- Die Entwicklung von digitalen Anwendungen, deren Hauptzweck die digitale Souveränität ihrer Anwenderinnen und Anwender ist. Dazu gehören etwa „Personal Data Stores", mit denen man im Umgang mit Dienstleistern selbst die Verbreitung der eigenen Daten verwalten und kontrollieren kann.[81]

4.1.2 Kompetenzen und Kenntnisse

Die digitale Souveränität einer Person oder einer Struktur hängt maßgeblich von deren digitalen Kompetenzen ab. Um diese zu stärken, gibt es ebenfalls eine Reihe konstruktiver Ansätze:

- Die Debatte um die Medienkompetenz von Anwenderinnen und Anwendern ist sehr vielschichtig und enthält diverse wertvolle Vorschläge, wie etwa die Vermittlung von Grundsätzen der Informatik ab der Grundschulbildung[82] oder der verstärkten (Fort-)Bildung von Lehrkräften im Bereich digitaler Kompetenzen.[83] Hier hat der Staat weitgehende Handlungsspielräume. Der Sachverständigenrat für Verbraucherfragen empfiehlt zudem, auch außerschulische Angebote zur Förderung digitaler Kompetenz stärker als bisher finanziell zu fördern.

- Über die Medienkompetenz (als Kompetenz vorwiegend in der Nutzung von und im Umgang mit Medien) hinaus, gibt es den Ansatz, auch die Befähigung zur Technologiekritik als Kompetenz zu stärken.[84] Diese bezieht sich auf die Gestaltung von

[79] Die Süddeutsche Zeitung hat zu diesem Aspekt ein Dossier mit mehreren Artikeln erstellt, die von der Privatsphäre bis zu Sicherheit von Industrieanlagen verschiedene Teileaspekte beleuchten: http://gfx.sueddeutsche.de/apps/58343704f38f33fb247b637d/www/ Onlinedossier, abgerufen am 12.02.2018.
[80] Vgl. Stefan Krempl (2017): *Internet der Dinge: Forscher fordern verschärftes Haftungsrecht für vernetzte Produkte.* https://www.heise.de/newsticker/meldung/Internet-der-Dinge-Forscher-fordern-verschaerftes-Haftungsrecht-fuer-vernetzte-Produkte-3761982.html Medienbeitrag, angerufen am 12.02.2018.
[81] Vgl. Nikolai Horn, Anne Riechert, Christian Müller: *Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen.* Studie für die Stiftung Datenschutz. S.9.
[82] Vgl. Gerhard Seiler und Jutta Schneider (2016): *Programmieren lernen heißt fürs Leben lernen.* http://dasnetz.online/programmieren-lernen-heisst-fuers-leben-lernen/ Medienbeitrag, abgerufen am 12.02.2018.
[83] Vgl. Sachverständigenrat für Verbraucherfragen (2017) S.iv.
[84] Vgl. John Naughton (2017): *Why we need a 21st-century Martin Luther to challenge the church of tech.* https://www.theguardian.com/technology/2017/oct/29/why-we-need-a-21st-century-martin-luther-to-challenge-church-of-technology-95-theses, Medienbeitrag abgerufen am 07.02.2018.

Technologie und ist insbesondere relevant für die demokratische partizipationsbezogene Dimension der digitalen Souveränität.

- Zivilgesellschaftliche Ansätze, wie etwa die internationale und dezentral organisierte CryptoParty-Bewegung[85], NGOs und Aktivisten leisten neben der Vermittlung von oft sicherheitsbezogenen Kompetenzen auch Aufklärungsarbeit über systemische Missstände, wie etwa Diskriminierung als Folge der Trackingindustrie. Solche Bewegungen könnten stärker in Strategien zum Aufbau digitaler Souveränität einbezogen werden.

4.1.3 Gesellschaftliche Strukturen

Auch Menschen mit ausgeprägten Kompetenzen stoßen auf Grenzen, wenn es keine Möglichkeiten gibt, von diesen Gebrauch zu machen, oder sie einzig dazu dienen, sich der eigenen eingeschränkten digitalen Souveränität Gewahr zu werden. Die Gestaltung des digitalen Ökosystems auf gesellschaftlicher Ebene ist daher ein wichtiges Gebiet, welches sehr wirkmächtige Ansätze zur Stärkung der digitalen Souveränität bereithält:

- Die personelle und finanzielle Stärkung von Kontroll- und Schutzstrukturen, wie beispielsweise Verbraucherzentralen und Datenschutzbehörden ist geeignet, die digitale Souveränität der Bevölkerung mittelbar deutlich zu stärken.

- Konventionen, wie die Verwendung von Open-Source-Software in privaten und öffentlichen Strukturen, begünstigen den Aufbau vertrauenswürdiger Systeme und stärken somit die digitale Souveränität aller Anwenderinnen, Anwender und Stakeholder der jeweiligen Struktur.[86]

- Eine gezielte Förderung von Open-Data-Initiativen könnte zudem „ein Gegengewicht zu den dominierenden Marktdynamiken der Digitalisierung bilden“[87] und somit die digitale Souveränität der Gesellschaft stärken. Ein Beispiel hierfür ist etwa das zivilgesellschaftliche Projekt und Angebot OpenStreetMap, das eine Alternative zu den Kartendiensten großer privatwirtschaftlicher Plattformen darstellen kann. Open-Data bezeichnet verschiedene Ansätze, Datensammlungen, die mit öffentlichen Mitteln finanziert wurden, zugänglich zu machen um eine Weiterverwertung durch Forschung, Unternehmen und Zivilgesellschaft zu ermöglichen.[88]

[85] Eine Eigendarstellung findet sich auf der Webseite https://www.cryptoparty.in/, abgerufen am 07.02.2018.
[86] Vgl. Boris Hofferbert (2018): *Ist Open Source Software wirklich sicherer?* https://www.heise.de/tipps-tricks/Ist-Open-Source-Software-wirklich-sicherer-3929357.html Medienbeitrag, abgerufen am 12.02.2018.
[87] Misterek (2017) S.30.
[88] Vgl. Misterek (2017) S.23.

4.1.4 Regulierung

Regulierung kann angepasst und neu bzw. weiterentwickelt werden, um im digitalen Wandel die (digitale) Souveränität der Menschen und anderer Entitäten zu stärken. In diesem Zusammenhang sind die folgenden ausgewählten Herausforderungen und Regulierungsbereiche besonders relevant:

- Die Verbesserung der Transparenz von Datenverarbeitungsprozessen würde die digitale Souveränität aller Betroffenen stärken, da diese ihr Verhalten auf eine bessere Informationsgrundlage stützen könnten. Dies bedarf, vor allem im Bereich von automatisierten und datenbasierten Entscheidungsprozessen, regulatorischer Schritte. Ob die 2016 in Kraft getretene und ab dem 25. Mai 2018 umzusetzende EU-Datenschutzgrundverordnung (DSGVO) ein Recht auf die Erklärung solcher Entscheidungen enthält, wird derzeit debattiert.[89] Aber auch die Auflagen der DSGVO bezüglich der Länge und Lesbarkeit von und Datenschutzbedingungen oder eine Stärkung unentgeltlicher Auskunftsansprüche können die digitale Souveränität von Einzelpersonen stärken.[90] Ähnliche Auflagen zu Länge und Verständlichkeit von Allgemeinen Geschäftsbedingungen (AGB) wären in diesem Zusammenhang eine sinnvolle Ergänzung.

- Um Monopolbildungen und -festigungen entgegenzuwirken, könnten verpflichtende Standards für Interoperabilität bestimmter digitaler Angebote zweckdienlich sein. Ein niedrigschwellig wahrnehmbares Recht auf Datenportabilität könnte hier eine verstärkende Zusatzwirkung entfalten.[91] In diesem Zusammenhang bleibt abzuwarten, wie das Recht auf Datenportabilität aus der Datenschutzgrundverordnung in der Praxis umgesetzt werden wird.[92]

- Eine Art „Algorithmen-TÜV" könnte unter bestimmten Umständen sicherstellen, dass bestehende Normen, beispielsweise zur Bekämpfung von Diskriminierung, eingehalten werden, ohne Geschäftsgeheimnisse von digitalen Unternehmen zu lüften.[93] Die konkrete Ausgestaltung der Arbeitsweise und Zusammensetzung so eines Prüfgremiums ist allerdings noch offen.

---

[89] Einen guten Überblick zur Debatte liefert der Blogbeitrag von Merle Temme (2018): *The academic debate on transparency requirements in the GDPR: a brief overview.* http://technolawgeeks.eu/uncategorized/the-academic-debate-on-transparency-requirements-in-the-gdpr-a-brief-overview/, abgerufen am 07.02.2018.
[90] Vgl. DSGVO Art. 12 – 15.
[91] Vgl. Sachverständigenrat für Verbraucherfragen (2017) S.v.
[92] Vgl. DSGVO, Art. 20.
[93] Vgl. Klaus Müller (2017): *Algorithmen transparent gestalten - Forderungen an die Politik. https://www.vzbv.de/dokument/rede-algorithmen-transparent-gestalten-forderungen-die-politik.* Rede des Vorstands des Verbraucherzentrale Bundesverbands, abgerufen am 12.02.2018.

4.2 Aktuelle Entwicklungen

Die oben dargestellten Ansätze zur Stärkung der digitalen Souveränität hängen nicht in einem luftleeren Raum. Sie entfalten ihre Wirkung – im Falle einer (weiteren) Umsetzung – im Kontext einiger relevanter Entwicklungen. Eine Auswahl dieser Entwicklungen ist hier überblicksweise dargestellt.

4.2.1 Technologische Trends

Eine ganze Reihe gesellschaftlicher und technologischer Trends wirkt sich darauf aus, in welcher Realität dem Ideal digitaler Souveränität nachgeeifert wird. Zu diesen Trends gehören beispielsweise:

- Die Optimierung von Chatbots, beispielsweise im Kundendienst, die kaum von einem menschlichen Gegenüber zu unterscheiden sind.[94]
- Die Verbreitung sprachgesteuerter Geräte und Anwendungen, die zusammengenommen zu einer neuen Nutzungsweise digitaler Hilfsmittel verschmelzen. Die zunehmende Etablierung von Sprache als Interface zieht eigene Anforderungen an einen souveränen Umgang mit digitaler Technologie nach sich.
- Das immer alltagsrelevantere Internet der Dinge bringt mit seinen Kinderkrankheiten und Sicherheitsdefiziten neue Herausforderungen für die digitale Souveränität mit sich, insbesondere in Bezug auf Sicherheit.[95]
- Das Zusammenwirken der obigen Trends führt zu neuen Verhaltensweisen der Anwenderinnen und Anwender. Im Sinne der digitalen Souveränität wird darauf zu achten sein, dass die Menschen sich nicht unkritisch an ihre vernetzte Umgebung anpassen, sondern diese selbstbestimmt für sich nutzen.[96]

4.2.2 Politische Entwicklungen

Zusätzlich stehen auf rechtlicher und politischer Ebene einige Änderungen an:

- Das Inkrafttreten der EU-Datenschutzgrundverordnung im Mai 2018 bringt, wie oben teilweise bereits erwähnt, Neuerungen in Bezug auf verschiedene Schlüsselaspekte für die digitale Souveränität. So ermöglicht das Gesetz ein Verbandsklagerecht im Datenschutz, es könnte durch deutlich höhere Bußgelder als bisher der Durch-

[94] Vgl. Adam Milton-Barker (2016): *Mitsuku chatbot wins Loebner Prize for most humanlike A.I., yet again.*
[95] Die Süddeutsche Zeitung hat zu diesem Aspekt ein Dossier mit mehreren Artikeln erstellt, die von der Privatsphäre bis zu Sicherheit von Industrieanlagen verschiedene Teileaspekte beleuchten: http://gfx.sueddeutsche.de/apps/58343704f38f33fb247b637d/www/ Onlinedossier, abgerufen am 12.02.2018.
[96] Vgl. Luciano Floridi (2017): *Die Mangroven-Gesellschaft. Die Infosphäre mit künstlichen Akteuren teilen.* In: Philipp Otto; Eike Gräf (2017): "3TH1CS. Die Ethik der digitalen Zeit." S.18.

setzung des Datenschutzrechts auf die Sprünge helfen und es vereinfacht die Ansprache von Datenschutzbehörden für Einzelpersonen und Unternehmen.[97] Diese und zahlreiche weitere Auswirkungen der Datenschutzgrundverordnung sind von hoher Bedeutung für die digitale Souveränität der Europäerinnen und Europäer.

- Eine Neuauflage der bestehenden ePrivacy-Richtlinie befindet sich zurzeit[98] im EU-Gesetzgebungsverfahren. Während die endgültigen Änderungen noch nicht absehbar sind, ist angesichts der aktuellen Entwurfsfassung davon auszugehen, dass sie für die digitale Souveränität von hoher Bedeutung sein werden.

- Die Zusammenarbeit von Wettbewerbsbehörden mit Datenschutzbehörden, sowie die zunehmende Bezugnahme von Wettbewerbshütern auf Datensätze in Konzentrationsverfahren auf europäischer und nationaler Ebene ist ein Zeichen für einen Souveränitäts(rück)gewinn etablierter Strukturen über die digital geprägten Märkte.[99]

5 Fazit

Ob als Einzelperson, Unternehmen oder Staat – unsere digitale Souveränität hängt von Umständen ab, die wir als Gesellschaft vielfach beeinflussen können. Hierfür ist es erforderlich, nicht nur die Zielsetzungen einer digitalen Souveränität, sondern jeweils auch den Kontext und alle relevanten Zusammenhänge zu kennen und zu gestalten, innerhalb derer sich diese Zielsetzungen verorten. Die Nutzungsweisen digitaler Technologie ändern sich rasend schnell, bestehende Machtverhältnisse weniger schnell, und nationale wie europäische Regulierung im Vergleich eher langsam.

Auf der Grundlage einer genauen Kenntnis der Umstände können konkrete Bedarfe identifiziert, Ideen entwickelt, Maßnahmen durchgeführt, Verantwortungen zugewiesen und deren Erfüllung überprüft werden. Daraus ergibt sich ein deutlicher und permanenter Bedarf der Aktualisierung unserer Kenntnisse, was digitale Souveränität angesichts der raschen Weiterentwicklung der Digitalisierung und, mit ihr, unserer Lebensumstände bedeutet, um daraus eine Orientierung für eine demokratische, faire und besonnene Politik abzuleiten, die letztendlich uns allen ein selbstbestimmtes Leben in der digitalen Zeit gewährleisten soll. Dieser Bedarf der aktiven Beobachtung und Reflektion ist gleichermaßen eine Chance, die Ergebnisse und Erkenntnisse einer fortlaufenden Betrachtung der Anforderungen, die

[97] Einen guten Überblick zu den wesentlichen Neuerungen der europäischen Datenschutzgesetze liefert Natasha Lomas (2018): *WTF is GDPR?. https://techcrunch.com/2018/01/20/wtf-is-gdpr/.* Medienbeitrag, abgerufen am 12.02.2018.
[98] Februar 2018.
[99] Vgl. EDSB: *Big Data und Digital Clearing house*. https://edps.europa.eu/data-protection/our-work/subjects/big-data-digital-clearinghouse_de. Webseite des EDSB, abgerufen am 12.02.2018 sowie Bundeskartellamt (2017): V*orläufige Einschätzung im Facebook-Verfahren: Das Sammeln und Verwerten von Daten aus Drittquellen außerhalb der Facebook Website ist missbräuchlich. http://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2017/19_12_2017_Facebook.html*. Pressemitteilung, abgerufen am 12.02.2018.

wir an einen Zustand digitaler Souveränität knüpfen, auch in der Praxis voranzubringen. Denn die Grundlage hierfür wird mit einer wiederholten und gründlichen Bestandsaufnahme bereits gelegt. Aus dem Leitbild der digitalen Souveränität ergibt sich eine Vielzahl an politischen und gesellschaftlichen Handlungsbedarfen, die es zu durchdenken und zu gestalten gilt. Eine fortwährende Konkretisierung des Leitbilds der digitalen Souveränität ist somit ein geeignetes Mittel, um kontextbasierte und durchdachte Digitalisierungspolitik zu betreiben. Dieses Papier stellt hierfür einen Ausgangspunkt dar.