Wilfried Jäger, Michael Nentwich, Gerhard Embacher-Köhle, Jaro Krieger-Lamina

Digitale Souveränität und politische Prozesse

1. Zum Begriff der digitalen Souveränität eines Staates

Digitale Souveränität ist ein schillernder Begriff, der seit einiger Zeit Konjunktur hat. So war das Thema etwa ein Schwerpunkt der deutschen EU-Ratspräsidentschaft[1] und zuletzt hat in Österreich der Rat für Forschung und Technologieentwicklung mit einem Papier und einem Workshop zum Thema „Technologiesouveränität" aufhorchen lassen (RFTE 2021). Der Begriff geht über den engeren Terminus der digitalen Souveränität hinaus und fokussiert prinzipiell auf alle Technologien und Produkte, bei denen ein Nationalstaat wie Österreich von internationalen Märkten abhängig sein könnte. Jüngst wurde etwa im Zusammenhang mit der Covid-19-Pandemie deutlich spürbar, dass Österreich (und viele andere europäische Länder) im Bereich der Pharmaindustrie kaum souverän und auf Importe aus dem Ausland angewiesen ist (vgl. ARGE ITA-AIT Parlament, 2020a). Die digitale Souveränität der Staaten wurde in jüngerer Vergangenheit beispielsweise anhand des von chinesischen Firmen dominierten Marktes für bestimmte Komponenten beim Aufbau des 5G-Mobilfunknetzes äußerst kontrovers diskutiert. Die seit Anfang 2021 deutlich zunehmenden Cyberattacken, nicht nur auf Firmen, sondern auch auf staatliche Infrastrukturen wie etwa das irische Gesundheitssystem[2] oder die deutsche Kommunalverwaltung[3], zeigen eine weitere Seite der heute deutlich herausgeforderten digitalen Souveränität. In unserem Überblicksbeitrag 2019 definieren wir digitale Souveränität wie folgt:

> „Ein Staat ist im Idealfall dann digital souverän, wenn er in seinem Zuständigkeitsbereich selbstbestimmt handeln und das Monopol der Staatsgewalt auch ausschließlich ausüben kann, d.h. auch gegen den Widerstand anderer Staaten und insbesondere nichtstaatlicher Akteure. Das inkludiert neben dem Handeln im eigenen Bereich, insbesondere in der Verwaltung, aber auch in Hinblick auf die notwendigen Voraussetzungen für funktionierende demokratische Prozesse,

1 eu2020.de/eu2020-de/programm/staerkung-der-digitalen-souveraenitaet-europas/2365342; diese und alle weiteren Internetquellen wurden zuletzt am 23.07.21 gecheckt.

2 en.wikipedia.org/wiki/Health_Service_Executive_ransomware_attack.

3 tagesschau.de/investigativ/br-recherche/ransomware-103.html.

> auch die Herstellung jener rechtlichen und infrastrukturellen Rahmenbedingungen, die es seinen Staatsbürger*innen selbst ermöglicht, digital souverän zu handeln." (Nentwich et al. 2019, S. 7)

Im vorliegenden Beitrag werden wir nicht auf den zweiten Aspekt eingehen, also was der Staat tun kann, um seine Bürger*innen souverän zu machen, sondern auf den im Beitragstitel angesprochenen politischen Prozess fokussieren.

Wie in der oben angeführten Definition bereits anklingt, sollte der Staat seine Regeln auf seinem Territorium, und damit auch im digitalen Raum, durchsetzen können, d.h. Macht ausüben können. Dies ist gerade im Cyberspace keineswegs einfach, weil es zwar einen Teil des Cyberspace gibt, der einem bestimmten Staat zuordenbar ist (etwa alle Server und Kommunikationsverbindungen auf seinem Territorium), dieser jedoch nicht ohne Weiteres abgrenzbar ist (siehe auch den Begriff der Cloud-Services). So können etwa problemlos Dienstleistungen von Servern außerhalb des physischen Territoriums in Anspruch genommen werden, sogar ohne dass dies den Nutzer*innen bewusst sein muss. Aus demselben Grund ist die Unversehrtheit und Ungestörtheit des nationalen Teils des weltumspannenden Cyberspace nicht einfach sicherzustellen. Die digitale Sicherheit muss sowohl gegen äußere wie gegen innere Aggressoren gewährleistet werden.

Auf unser aktuelles Thema der politischen Prozesse heruntergebrochen heißt das konkret, dass unbefugte Akteure beispielsweise daran gehindert werden müssen, die politische Kommunikation zu beeinflussen, demokratische Wahlvorgänge sowie die öffentliche Meinungsbildung zu manipulieren, die staatlichen Organe und die Verwaltung lahm zu legen oder die Grundrechte (z.B. das Recht auf Privatsphäre als eine der Voraussetzungen eines funktionierenden demokratischen Systems) zu kompromittieren.

Daraus ergeben sich verschiedene fundamentale, dennoch selten in der gebotenen Tiefe diskutierte Fragen, beispielsweise: Wie können (elektronische) Wahlen oder Beteiligungsprozesse unter Wahrung der staatlichen Souveränität ablaufen? Wie kann die elektronisch vermittelte Manipulation der öffentlichen Meinung verhindert werden, während die Vorteile elektronisch vermittelten Meinungsaustauschs gewahrt werden? Die Antworten auf diese und ähnliche Fragen sind alles andere als trivial und können auch in diesem Beitrag nur ansatzweise diskutiert werden. Im Hauptteil werden wir zunächst die Ursache der Bedrohung der digitalen Souveränität des Staates näher erörtern und uns dabei auf die sogenannten Plattformen, also die von wenigen großen Internetfirmen bereitgestellten, internetbasierten Kommunikationsinfrastrukturen konzentrieren (2.). Anschließend beschreiben wir etwas ausführlicher, wie digitale Souveränität konkret gefährdet wird (3.)

und welche Rolle schon jetzt, in Zukunft aber noch viel mehr Künstliche Intelligenz dabei spielt (4.). Abschließend stellen wir ansatzweise Optionen dar, wie digitale Souveränität besser sichergestellt werden könnte (5.).

2. Plattformen stehen in politischer Konkurrenz zum Staat

Plattformen stehen im Zentrum der Diskussion der Digitalisierung – schon in seiner Keynote hat Phil Howard diese Super-Star-Companies mit ihrem Potential für Desinformation und Targeting in den kritischen Fokus gestellt (Howard 2021). Welches sind neben diesen Effekten die strukturellen Gefahren dieser Plattformen für die staatliche Souveränität?

Es gibt eine „*funktionale Souveränität*" von privatwirtschaftlichen Plattformen, die sich auch auf den politischen, öffentlichen Raum ausdehnt, indem sie staatliche Funktionen übernehmen und die Souveränitätsfunktion des Staates teils substituieren, teils unterlaufen. Diese Funktionen übernahmen Plattformen um ihr Geschäftsmodell zu fördern. Das digitale, globale Agieren stößt in ein institutionelles Vakuum, für das die Staatengemeinde bislang keine abgestimmten, allgemein anerkannten Strukturen bietet. Weder sind die unten besprochenen Standards auf nationaler Ebene immer komplett digital eingeführt, noch sind sie alle global abgestimmt und gültig. Vor diesem Hintergrund haben sich staatliche Funktionalitäten auf digitalen, globalen Plattformen verselbständigt.

Digitale Identitäten: Für die Zugangskontrolle zu digitalen Services sind globale digitale Identitäten nötig. Diese Identitäten sichern nicht nur den Ausschluss von nicht-zahlenden Individuen, sondern sind integraler Bestandteil der Werbeeinkünfte einer digitalen Plattform. Wenn die Menschen das „Produkt" sind, müssen sie identifizierbar und ihre Schritte nachverfolgbar sein. Durch diese Identitätsvergabe entsteht die Fähigkeit zur digitalen Verfolgung und Überwachung von Individuen im digitalen Raum, welche nach den nicht verhandelten (und nicht verhandelbaren) sowie intransparenten Kriterien der jeweiligen Plattformbetreiber erfolgt. Durch private Identitäten wie Google-ID oder Facebook-Login wird die klassische Aufgabe der Identitätsstiftung durch Staaten ausgehebelt. Die Ausgestaltung der privatwirtschaftlichen digitalen Identität – wie zum Beispiel die Strenge der Identifikation, der Transaktionsspeicherung der Identifizierten und die Zugriffsrechte auf diese Daten – kann innerhalb der Plattformen nicht diskutiert und einem politischen Legitimationsprozess zugeführt werden. Staatliche digitale Identitäten – wie zum Beispiel das Aadhaar-System in

Indien seit 2009[4] oder die eIDAS-Verordnung der EU[5] – unterliegen hingegen diesem politischen Prozess. Die notwendige technische Komplexität, datenschutzrechtliche Einschränkungen sowie gesellschaftliche und rechtliche Folgen werden öffentlich diskutiert, kritisiert, begründet und nötigenfalls adaptiert. Diese Korrektur fällt bei privatwirtschaftlich organisierten Plattformen völlig weg, wie die Diskussionen um den Verkauf von Identitäten und die Anreicherung derselben mit Metadaten (politische Gesinnung, Vermögensstärke etc.) gezeigt hat.

Rechtsetzung: Mangels eines allgemeinen internationalen Rechtsrahmens für digitale Konsumentengeschäfte und der mangelnden globalen Durchsetzbarkeit nationaler Rechte bei internationalen Konsumentengeschäften übernahmen die Plattformen mittels ihrer Allgemeinen Geschäftsbedingungen (AGB) diese Rolle. Diese sind – mangels gesetzlicher Regulierung – asymmetrisch einseitig zum Vorteil der Plattformen ausgelegt. Sie bieten aber eine einfache, realistische Option, globale Geschäfte im Consumer-Bereich abwickeln zu können. Dadurch werden jedoch mühsam erkämpfte Rechtsinstrumente des Konsument*innenschutzes und des Datenschutzes, welche auf nationalstaatlicher Basis erfolgen, stark eingeschränkt. Es werden fremde Rechtsvorschriften des Firmensitzes der Plattform weltweit verbreitet und durchgesetzt. Diese eigene Rechtssetzung der Plattformen wird erst ansatzweise politisch reguliert oder gefordert (etwa via Datenschutz- und Kartellrecht). Mit der Zunahme des lokalen Onlineversands gefährdet diese Entwicklung somit auch im nationalen Umfeld gültige Rechtsnormen zum Schutz der Bürger*innen und Konsument*innen.

Rechtsdurchsetzung: Die internationale Durchsetzbarkeit von Verträgen ist Gegenstand zahlreicher bilateraler Vereinbarungen und aufwändiger Schiedsgerichtsverfahren. Sind diese Instrumente schon bei großen Geschäftsvolumina sehr aufwändig, so sind sie für Konsument*innengeschäfte oder Social-Media-Transaktionen von Individuen nicht praktikabel. Die Entscheidung über Regelübertretungen wird innerhalb der Plattformen nun nach den selbst gegebenen AGB oder nach den Richtlinien der jeweiligen Konzernführung ohne jegliche Eingriffsmöglichkeit oder Transparenz durchgeführt. Die Sanktionen sind meist Zugangsverweigerung zu Services.[6] Der Ausschluss von privaten monopolistischen Netzwerken kann

4 de.wikipedia.org/wiki/Aadhaar.

5 Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt, eur-lex.europa.eu/legal-content/de/ALL/?uri=CELEX:32014R0910.

6 Siehe jüngst das Beispiel der Sperrung des Twitter-Accounts des Ex-Präsidenten der USA, blog.twitter.com/en_us/topics/company/2020/suspension.

eine massive Gefährdung der Interessen von Individuen oder Gruppen sowie eine illegitime Einschränkung von allgemeinen Rechten (wie freier Meinungsäußerung etc.) bedeuten. Kritisch ist an dieser Entwicklung, dass es sich de facto um ökonomische Monopole handelt, die ein einfaches Ausweichen auf andere Netzwerke verunmöglichen, sowie die Intransparenz und die Nicht-Anfechtbarkeit der Verdikte.

Intransparenz: Neben den oben besprochenen Legitimations- und Transparenzdefiziten der AGB sind auch die Geschäftsmodelle und die Operationskriterien der Plattformen ein Geschäftsgeheimnis. Dies steht im krassen Widerspruch zu staatlichem Handeln, bei dem öffentliche Parlamente, Gerichtshöfe sowie die Öffentlichkeit der Entscheidungskriterien (meist auf gesetzlicher Grundlage) Transparenz und Legitimation bieten. Besonders, wenn algorithmische Bewertungen von Plattformen die öffentliche Meinung und so die politische Öffentlichkeit beeinflussen, sind die ökonomischen Interessen dieser privaten Bewertungsmechanismen politisch relevant. Weiters stellt die Bewertung von Personen nach in der Öffentlichkeit unbekannten Kriterien und der Weiterverkauf dieser Bewertungen ohne Wissen der Betroffenen einen massiven Eingriff in das Leben der Einzelnen ohne Transparenz und Korrekturmöglichkeiten dar.[7] Diese Algorithmen-Intransparenz tritt aber nicht nur bei klassischen Plattformen, sondern bei allen Dienstleistern auf, welche derartige Algorithmen einsetzen. Besonders deutlich wird dies in den Bewertungsalgorithmen von Arbeitssuchenden, welche von „geheimen" Algorithmen privater Human-Ressource-Dienstleister oder sogar öffentlichen Arbeitsämtern vorselektiert und so potentieller Chancen beraubt werden können. Auch können Verhaltensweisen, typische Lebensläufe etc. zur Norm erklärt werden, obwohl sie aufgrund der Auswertungskriterien einem Bias unterliegen (Allhutter et al. 2020).

Währung: Das Prägen von Münzen und die Währungshoheit waren bis dato staatliche Aufgaben, um die Sicherheit und Werthaltigkeit des Geldes für die Bürger*innen zu garantieren. Das Aufkommen von Kryptowährungen hat dieses Monopol gebrochen. So hatte Facebook ein Projekt, eine eigene Währung für die Bezahlinteraktionen zu schaffen, welches derzeit wieder auf Eis liegt.[8] Da Währungen und deren Regulierung wesentliche Merkmale der Wirtschaftssteuerung per se sind, würden anerkannte „private Währungen" eine Beschneidung dieser politischen Kompetenz darstellen.

7 Beispielsweise verkaufte die Österreichische Post Daten zur errechneten Parteipräferenz ihrer Kund*innen, futurezone.at/netzpolitik/oesterreichische-post-verkauft-daten-ueber-politische-vorlieben/400370723.

8 pay.facebook.com.

Politische Kommunikationsinfrastrukturen: Die Versammlungsfreiheit stellt die Basis für die eigenständige politische Selbstorganisation der Bürger*innen dar. Wird sie reduziert oder manipuliert, ist der politische Prozess eines demokratischen Gemeinwesens gefährdet. Ab einer gewissen Größe und de facto Monopolstellung – die auch auf Inhalte und Formate fokussiert sein kann – übernehmen somit private Firmen öffentliche Funktionen. Praktisch zeigt sich dies durch die massive Nutzung dieser Kommunikationskanäle durch politische Parteien und Interessensgruppen. Während der Werbemitteleinsatz im politischen Umfeld kein plattformspezifisches Phänomen ist, wird es durch die Erweiterung um digitale, KI-unterstützte Datenanalyse-Methoden aus einem nie dagewesenen Datenpool (z.B. Targeting-Optionen auf Einzelpersonenbasis) als auch durch die Globalisierung der Einflussnahme (Lobbygruppen, ausländische Staaten etc.) durch Plattformen auf ein neues Niveau gehoben. Der Zugang und der Ausschluss von der politischen Öffentlichkeit werden durch Entscheidungen von Einzelpersonen, von Plattformeignern und Managern bestimmt. Willkürlicher, nicht demokratisch legitimierter Ausschluss von Kommunikations-Infrastrukturen (Beispiel Twitter Donald Trump, s.o.) oder Ausschluss von Content (Beispiel Facebook in Australien[9]) beeinflussen den politischen Prozess ebenso wie der Datenhandel und die Blockierung von Aussagen nach privaten Regeln (AGB). Im öffentlichen Umfeld ist die Verweigerung des Zugangs zu Infrastrukturen an gesetzlich legitimierte Kriterien gebunden. Weiters gibt es in vielen Fällen eine gesetzliche Betriebspflicht für digitale öffentliche Services. Die Erkenntnis, dass private, digitale Kommunikationsnetze aufgrund ihrer Größe eine politische Dimension bekommen können, motiviert zahlreiche politische Regulierungsversuche und wissenschaftliche Untersuchungen über Einflussnahmen auf politische Wahlen (Howard 2020).

Diese *neue politische Qualität* von Plattformen wurde in jüngster Zeit wegen deren massiver Nutzung, den beobachtbaren Verzerrungen des politischen Diskurses und des Aufdeckens von gezielten politischen Interventionen vermehrt wahrgenommen. Große, nicht demokratisch verfasste Staaten wie Russland und China haben als Reaktion eigene soziale Netze aufgebaut und teilweise globale Plattformen verboten. Zulassungen im eigenen Herrschaftsbereich wurden an die Kooperation bei der Durchsetzung von Zensurmaßnahmen und der Kontrolle über die Daten gekoppelt. Zwar können auch diese Staaten keine 100-prozentige Kontrolle ausüben, haben die Verbote jedoch mit strengen Strafen bei Nichteinhaltung gekoppelt. In der EU entstanden zivilgesellschaftliche Initiativen, die den Kampf um

9 about.fb.com/news/2021/02/changes-to-sharing-and-viewing-news-on-facebook-in-australia/.

die Implementierung politischer Werte und Gesetze, wie die Datenschutzgrundverordnung (DSGVO), führen.

3. Demokratische digitale Souveränität als Balance: Implizite Verschiebungen durch Technologie und Strukturen

Demokratische digitale Souveränität zu bieten, ist ein heikler Balanceakt. Einerseits soll sie die Interessen der Gemeinschaft, des Staates und des politischen Systems als Gesamtes schützen, um so den politischen Prozess sicher ablaufen zu lassen, andererseits die einzelnen Bürger*innen nicht an der Ausübung ihrer politischen Freiheiten hindern. Diese Balance wird wesentlich durch die „Waffengleichheit" zwischen Bürger*innen und dem Staat definiert und war auch in der Vergangenheit ein Schauplatz institutioneller Kämpfe und Vorkehrungen. Heute wird diese digitale Waffengleichheit implizit durch technologische, scheinbar „unpolitische" Entscheidungen beeinflusst.

Die Wahrnehmung der legitimen Staatsaufgaben, wie des Schutzes seiner Bürger*innen gegen äußere und innere Aggressoren, wird im digitalen Zeitalter oft durch eine tiefe, permanente Überwachung digitaler Aktivitäten verfolgt. Weiters verwischen sich die Grenzen zwischen staatlichen und nichtstaatlichen Akteuren im digitalen Raum zusehends. So kann das erpresserische Lahmlegen von kritischen Wirtschaftsbetrieben und öffentlichen Einrichtungen sowohl dem Erbeuten von Lösegeld[10] als auch der Destabilisierung von Organisationen und Staaten dienen. Rachefeldzüge aus politischen Motiven werden sowohl von privaten als auch staatsnahen Akteuren unternommen. Da die Angreifenden meist nicht klar erkennbar sind und sich über unverdächtige Kanäle nähern, lässt sich der Kreis der Aggressoren für eine Überwachung nicht klar eingrenzen. Da Angriffe im digitalen Raum durch mehrschichtige, komplexe Angriffssoftware erfolgen, ist eine permanente Überwachung der gefährdeten Systeme notwendig, was de facto zu einem weltweiten permanenten kalten Krieg im digitalen Raum führt. In der Wahrung der äußeren digitalen Souveränität erwarten die Bürger*innen, dass Staaten und Staatenverbünde wie die EU diese Sicherheit gewährleisten. Der politische Druck auf das Funktionieren der digitalen Verteidigung steigt bei jedem erfolgreichen bekannten Überfall an. Es schafft in der Politik die Bereitschaft, Einschränkungen bei Bürgerrechten hinzunehmen. Bürger*innen sind jedoch in der Regel nicht bereit, diesen angeblichen „Trade-Off" zwischen Sicherheit und Privatsphäre unwidersprochen einzugehen (vgl. Pavone et al. 2015 und die Proteste gegen Bundes-Tro-

10 de.wikipedia.org/wiki/Ransomware.

janer, Upload-Filter usw., vgl. Strauß 2017). Diese Einschränkungen wirken aber auf den politischen Prozess, den zu verteidigen der Staat angetreten ist, selbst zurück. Die digitale Souveränität des Individuums hängt sehr stark vom Schutz der Privatsphäre als Voraussetzung des demokratischen Prozesses, somit von seiner individuellen Datensouveränität ab.

Dazu kommen Aggressoren von innen, welche die Ablöse der Regierungsform, die Unterwanderung des Staates oder simple kriminelle Aktivitäten verfolgen. Auch sie können über ausländische Server und globale Plattformen verdeckt operieren. Dadurch wird das Feld potentieller Aggressoren zusätzlich erweitert. In konsequenter Logik sind die Geheimdienste großer Länder angetreten den gesamten Internetverkehr – ohne jegliche Einschränkung der Überwachungsziele – zu überwachen.

Die Freiheit der Bürger*innen bedingt die Option zu abweichenden Meinungen und Lebensstilen ohne Benachteiligung. Diese Grenze zwischen Umsturzgefahr, berechtigtem Protest und harmlosem Klatsch ist gesellschaftlich volatil und schwer zu ziehen. Sie markiert aber den „freien digitalen Raum" vom „unerlaubten, sanktionierten digitalen Raum" und muss daher laufend offengehalten und politisch verhandelt werden.

4. Angriffe auf Wahlen und KI-Manipulation des politischen Prozesses

Im letzten US-Wahlkampf wurde allein der Anschein und Diskurs über die mögliche Manipulation der Wahlen dazu herangezogen, die Legitimation des demokratischen Wahlprozesses in Zweifel zu ziehen. Häufig öffentlich genannte Angriffsvektoren bei Wahlen waren der Angriff auf Wahlmaschinen und Auszählungen, die Manipulation der öffentlichen Meinung mittels KI-Technik sowie das Targeting von Bürger*innen.

Wahlmaschinen sind in den USA ein bevorzugtes Angriffsziel, da aufgrund der gewünschten Anonymität des Wahlvorganges die nachträgliche Verifikation des Wahlergebnisses schwerfällt und sie direkt in den Wahlvorgang eingreifen. Da diese Wahlmaschinen diesmal anscheinend gut geschützt waren, konnte keine Manipulation durch Cyberangriffe nachgewiesen werden. In Europa ist dieser Angriffsweg wegen der analogen Wahl mittels Stimmzettel oder Briefwahl heute kaum relevant.[11] Zukünftige digitale Wahloptionen müssen aber gegen diesen Angriff gerüstet sein.

Manipulation der öffentlichen Meinung war und ist ein inhärenter Teil der politischen Auseinandersetzung. Neu ist allerdings, dass Meinungen

11 Mit Wahlgeräten gibt es in Europa nur vereinzelt Erfahrungen, etwa in Deutschland und den Niederlanden, vgl. de.wikipedia.org/wiki/Wahlger%C3%A4t#Beispiele_f%C3%BCr_Probleme_mit_Wahlger%C3%A4ten_(Ausland).

anonym und in digitaler Serienproduktion unter Vorspiegelung falscher Identitäten erzeugt werden. Über Jahre hinweg angelegte Profile auf Plattformen werden mit KI-Antwort-Algorithmen oder einfachen Weiterleitungs- und Verteilungsfunktionen hinterlegt. Damit können Wellen von Fake-News durch soziale Netze gespült und damit gewünschte Stimmungen erzeugt werden. Eine andere Vorgehensweise besteht darin, die politische Polarisation per se in sozialen Netzwerken zu verstärken. Die KI-Multiplikation und automatisierte Orchestrierung machen diese Meinungsangriffe gegenüber den menschlichen Akteuren sehr mächtig. Durch die Werbeorientierung und das Profiling der Netzwerkteilnehmer*innen kann jeder beliebige Werbekunde Informationen über Individuen für seine Zwecke nutzen. Der Cambridge-Analytica-Skandal[12] zeigt, dass Lifestyle-Fragebögen auf Plattformen genutzt wurden, um gezielt psychologische Dispositionen für die Auftraggeber zu nutzen (siehe dazu ausführlich Howard 2020).

Deep-Fakes durch digitale Manipulation von „authentischen" Nachrichten durch Sprache und Video eröffnen neue Optionen der Erzeugung von Falschnachrichten, welche vermutlich auf absehbare Zeit schwer zu identifizieren sind. Doch erst die Verwendung von Sozialen-Medien-Plattformen, automatisierten Bots und Microtargeting erlaubt die Verbreitung und somit eine Manipulation der öffentlichen Meinung (ARGE ITA-AIT Parlament, 2020b).

Neben der inhaltlichen Falschmeldung erzeugen diese Ereignisse ein breites Misstrauen in den gesellschaftlichen Kommunikationsprozess und damit in den Prozess der politischen Meinungsbildung. Unter Nutzung netzwerkspezifischer Effekte wie den sog. Echokammern können notwendige Dispute durch Trollfabriken und Falschmeldungen in die Destruktivität geführt werden (Falkner 2021). So sind etwa Datenangriffe auf politische Entscheidungsträger und deren Bloßstellen durch vertrauliche Informationen (vgl. Hillary Clintons Mailverkehr und Jeff Bezos' Fotos) sowie deren Verbreitung in sozialen Medien ein wirksames Einschüchterungsmittel.

Microtargeting über Plattformen nimmt verschiedene Formen an. Durch die vielfältigen digitalen Spuren, die von Plattformen zur Erhöhung der Werbegenauigkeit intensiv gesammelt werden, werden mittels Data-Analytics auf politische Ausrichtung, psychologische Dispositionen, Interessen, Communities und Kaufverhalten geschlossen (ARGE ITA-AIT Parlament, 2020c). Sind bei genau platzierten Werbungen die gesellschaftlichen Folgen meist gering, ist dies bei der konkreten Ansprache im politischen Umfeld nicht der Fall.

12 de.wikipedia.org/wiki/Cambridge_Analytica#Einflussnahme_auf_US-Wahlk%C3%A4mpfe.

Verdeckt, für die Betroffenen nicht erkenntlich, ist die individuelle Anpassung von politischen Nachrichten an die errechnete persönliche politische Ausrichtung. Im „optimalen Fall" erhält jede*r Bürger*in, die auf ihn*sie zugeschnittene politische Aussage. Neben der bewussten Irreführung verhindert ein solches Vorgehen die Etablierung einer gemeinsamen, kollektiven Diskussionsbasis und entsprechend informierter Entscheidungsfindung. Microtargeting klassifiziert Menschen aufgrund intransparenter Kriterien, drängt sie in Informationsblasen und nutzt private, nichtöffentliche, individuelle Eigenschaften für die Erzielung von kommerziellen und zunehmend auch politischen Interessen aus. Das ist qualitativ unterschiedlich zum bisherigen „Straßenwahlkampf", der aufgrund Umstehender und oftmals anwesender Medienleute deutlich transparenter ist, zugleich aber den Wahlwerbenden nur einen Bruchteil der im Rahmen von Microtargeting zur Verfügung stehenden Informationen über das Gegenüber zur Verfügung stellt. Die Manipulation in sozialen Medien hat hingegen „kein Gesicht", d.h. niemand verliert an Glaubwürdigkeit, sollte der „Trick" nicht greifen.

Für viele dieser Bedrohungen lassen sich derzeit keine klaren Gegenmaßnahmen angeben. Dennoch kann das digitale Kommunikationsumfeld so gestaltet werden, dass destruktive Manipulation des politischen Meinungsbildungsprozesses erschwert wird: So kann und wird KI auch zur Identifikation und Eliminierung von Fake-Bots eingesetzt. Aktiver, KI-gestützter Kampf gegen Trollfabriken jeglicher Provenienz kann deren Effektivität eindämmen. Weiters kann die Förderung kuratierter, ausgewogener Berichterstattung in den Massenmedien (Zeitungen, Fernsehen) zu einem Gegengewicht zu Echokammern führen. Die Einschränkung von politischer Werbung kann die Attraktivität von exzessiver Nutzung von Microtargeting senken. Wesentlich für einen freien offenen Diskurs ist aber die Zurverfügungstellung von öffentlichen, digitalen Räumen und Kommunikationsplattformen, welche nicht dem Diktat der Nutzer-Analyse und Überwachung aus kommerziellen oder politischen Gründen unterworfen sind. Solche Räume könnte der Staat (bzw. die EU) als Infrastruktur bereitstellen oder es könnten vertrauenswürdige, unabhängige Institutionen dabei unterstützt werden.

5. Sicherung des politischen Prozesses: Was kann getan werden?

Digitalisierung wird von immer wieder neuen, der breiten politischen Öffentlichkeit zunächst unbekannten und in ihren Konsequenzen intransparenten Technologien getrieben. Nur auf funktionale Kriterien beschränkte lokale Entscheidungen können daher zu unbeabsichtigten, gesellschaft-

lich unerwünschten Summeneffekten für den politischen Prozess führen. Die technisch fokussierte Entscheidungsfrage „Welche Software erfüllt meine Anforderungen?" ist durch Rahmenbedingungen und politische Entscheidungskriterien zu ergänzen. Sind diese umfassenderen Kriterien implementiert, stützen die dezentralen Entscheidungen eine Absicherung des politischen Prozesses. Dabei haben sich unterschiedliche prinzipielle Ansätze zur Sicherung von Transparenz und Abschätzbarkeit der Konsequenzen herausgebildet.

Der *Open-Source-First*-Ansatz bevorzugt die Verwendung von Open-Source-Software bei öffentlichen Vergaben. Derartige Kriterien könnten in Beschaffungs- und Ausschreibungsrichtlinien leicht implementiert werden und würden so die prinzipielle Überprüfbarkeit des verwendeten Codes sichern. Dadurch könnten Bürger*innen, Parteien, Organisationen der Zivilgesellschaft und andere jederzeit allfällige Tendenzen, Sicherheitslücken oder nicht vereinbarte Zusatzfunktionen von eingesetzter Software entdecken, überprüfen und neu verhandeln. Die beanstandeten Punkte könnten genau eingegrenzt und einer Lösung zugeführt werden. So wäre zum Beispiel das verdeckte Übermitteln von Userverhalten, Bewegungsdaten und privater Informationen bei mobilen Handybetriebssystemen bei einem Open-Source-Ansatz sofort aufgefallen und hätte sofort durch Änderung des offenen Codes abgestellt werden können. Bei der Diskussion um Algorithmen sind die Verteilung von Gewichten und die eingesetzten Berechnungsmethoden Basis für Kritik, aber auch für Alternativvorschläge. Diese Transparenz würde die Legitimität der Entscheidungsvorbereitung durch KI-Anwendungen in allen öffentlichen Belangen erhöhen.

„*Public Code for Public Money*"[13] fordert, dass alle mit öffentlichen Mitteln erstellte Software der Öffentlichkeit zur Verfügung gestellt wird. So könnte das eingesetzte Steuergeld für eine Software mehrfach verwendet werden, um internationales oder lokales Wissen zur rascheren Bereitstellung von öffentlichen digitalen Assets zu nutzen und der steuerzahlenden Privatwirtschaft Standard-Software-Module zur Verfügung zu stellen. Die Chancen für eine „Community der öffentlichen digitalen Verwaltung" mit intensivem Knowhow- und Softwareaustausch würden durch ein solches Instrument beflügelt. Damit könnten internationale Verwaltungsstandards – der Verwaltungen selbst – entsprechend der Gesetzeslagen eingeführt und allen Interessierten zu Verfügung gestellt werden.

Die Zurverfügungstellung von Verwaltungs- und Auswertungssoftware würde den Bürger*innen und Institutionen die Nutzung von bereits verfügbaren Open-Data-Quellen erleichtern. Vielfach hängt die Nutzung von

13 Vgl. fsfe.org/activities/publiccode/publiccode.de.html.

Open Data vom Auswertungsknowhow ab. Daher haben große private, proprietäre Plattformen einen Vorsprung, diese Daten für ihre Zwecke zu nutzen (Keller/Tarkowski 2021). Durch Open-Source-Tools könnte dieser Vorsprung aus der Sicht von Bürger*innen und NGOs wesentlich verringert werden. Die Bereitstellung solcher freier Auswertungssoftware kann – neben Open-Government-Data – als Realisierung der staatlichen Verpflichtung zur Transparenz seines Handelns gesehen werden.

Offene Standards: Proprietäre Datenstandards erzeugen nicht nur Gemeingut-gefährdende, teure Lock-In-Situationen, sondern schließen auch kleinere, (lokale) innovative Firmen vom Wettbewerb aus. Sie verhindern die Langzeitnutzung von Daten und verursachen überproportionalen Datenwartungsaufwand. Wer kann nach zwanzig Jahren noch die Lesbarkeit eines Verwaltungsdokumentes, erstellt in einem proprietären Standard, vielleicht einer nicht mehr existenten Firma sicherstellen? Die meisten derzeit verwendeten Dokumentenstandards sind proprietär. Alleine die Verpflichtung, öffentliche Dokumente in einem offenen Standard zu speichern und zu übermitteln, würde dieses Problem lösen und Souveränität über die eigenen Dokumente und verschriftlichte Wissensbasis herstellen.

Sichere Standards: Kommunikation läuft über technologische Standards, auf deren Verschlüsselung und andere Sicherheitsfeatures die Bürger*innen vertrauen können müssen. Diskussionen über schwache Sicherheitsstandards im Telekommunikations- und Datentransferbereich verunsichern und erzeugen Missbrauchspotential. Mit der Entwicklung und dem Einfordern von offenen, jederzeit überprüfbaren und sicheren Standards könnte der Staat seine Souveränität und die seiner Bürger*innen gewährleisten.

Offene Schnittstellen: Die beliebige Austauschbarkeit von Softwarekomponenten hängt neben der Softwarearchitektur auch von der Standardisierung der Schnittstellen ab. Hier ist die Arbeit in Standardisierungsgremien und die Einforderung dieser Standards bei Entwicklungsrichtlinien und Einkaufsvorgaben wesentlich. Diese Modularisierung würde die rasche, flexible Anpassung von Prozessen und Algorithmen erlauben, wenn diese nicht mehr den Anforderungen entsprechen.

Erhalten der staatlichen Entscheidungsfähigkeit: Die Durchführung der obigen Vorgaben erfordert ein profundes technologisches Knowhow in den staatlichen Institutionen. Die Aushöhlung des Knowhows dieser Institutionen führt zu Fehlentscheidungen, Mängeln in strategischen Entscheidungen sowie Ziel- und Projektdefinitionen und damit letztlich zum Verlust der staatlichen digitalen Souveränität. Auch wenn bei der Ausführung auf privatwirtschaftliche Firmen zurückgegriffen wird, sollte die Ausschreibung, Überwachung und Implementierungsbegleitung ein nicht delegierbarer Anteil des Staates sein. Da digitale Entscheidungen, welche Konsequenzen

für das gesamte System haben, lokal getroffen werden müssen, ist breites Fachwissen nötig. Um den einzelnen Bürger*innen und Verwaltungsbeamt*innen in ihren situativen Entscheidungsfindungsprozessen Unterstützung geben zu können, sind nationale und letztlich international akkordierte Ausschreibungs- und Digitalisierungsrichtlinien zu verabschieden. Das Wissen über die umfassenden sozialen und politischen Konsequenzen der eigenen technischen Entscheidungen sollte entwickelt, politisch diskutiert, geschult und weiterverbreitet werden. Diese Investition in nur vermeintlich „verwaltungsfremdes" Knowhow innerhalb der Verwaltung verhindert das Aushöhlen demokratischer Institutionen und deren De-facto-Steuerung durch von Eigeninteressen geleitete Technologielieferanten. Auf der privatwirtschaftlichen Seite kann ein solches Vorgehen die Entwicklung einer dezentralen und lokalen digitalen Wertschöpfung fördern und die Resilienz der eigenen digitalen Souveränität erhöhen.

Förderung unabhängiger Fact-Checking-Initiativen: Während es bereits zahlreiche Websites gibt, die mit hohem redaktionellem Aufwand versuchen, Fake-News, Deep-Fakes und sonstige manipulative Informationen im Netz bloßzustellen und damit zu einem faktenbasierten demokratischen Diskurs beizutragen, dürfte es noch großes Potenzial für die Unterstützung dieser Prozesse durch (teil-)automatisierte Technologien (KI) geben. Es wäre im Interesse des Staates, in deren Entwicklung, aber auch Verbreitung und Nutzung massiv zu investieren.

6. Fazit

Digitale Souveränität ist ein aktuelles, international relevantes Thema für Forschung und Politik. Der in diesem Beitrag gegebene Überblick macht deutlich, dass die Gefährdung der Demokratie durch die Digitalisierung real ist. Disziplinen-übergreifende Beschäftigung mit den vielen offenen Fragen bei der Identifikation und Umsetzung von souveränitätsstärkenden Initiativen (technisch, rechtlich, politisch) erscheint daher sehr wichtig. Darüber hinaus erfordert die Herstellung der digitalen Souveränität eines einzelnen Staates nicht nur entschlossenes Handeln auf nationaler Ebene, sondern auch internationale Übereinkünfte. Die EU-Ebene kann dabei eine wichtige Rolle spielen, auch wenn Einigung unter den 27 Mitgliedstaaten und geschlossenes Auftreten auf der Weltbühne aufgrund zunehmend divergierender Interessenslagen immer schwieriger werden. Die Arbeiten zur DSGVO und der Regulierung von KI zeigen aber, dass bei allen damit verbundenen Defiziten eine Einigung auf einen europäischen Standpunkt möglich ist und dieser auch über den europäischen Raum hinaus ausstrahlt. Wenn Lösungen für Europa gefunden würden, wäre das jedenfalls ein erster

Schritt, auch wenn es sich letztlich angesichts der transnationalen Akteure um eine globale Herausforderdung handelt.

Die Rolle der Technikfolgenabschätzung liegt klar auf der Hand: Es geht darum, die politischen und gesellschaftlichen Konsequenzen von vermeintlich unpolitischen technologischen (und ökonomischen) Entscheidungen offenzulegen und zur Diskussion zu stellen.

Literatur

Allhutter, D.; Mager, A.; Cech, F.; Fischer, F.; Grill, G. (2020): Der AMS Algorithmus – Eine Soziotechnische Analyse des Arbeitsmarktchancen-Assistenz-Systems (AMAS). Wien; epub.oeaw.ac.at/ita/ita-projektberichte/2020–02.pdf

ARGE ITA-AIT Parlament (2020a): Europäische Resilienz in Krisenzeiten. FTA-Monitoring für das Österreichische Parlament; parlament.gv.at/ZUSD/FTA/091_europ_resilienz.pdf

ARGE ITA-AIT Parlament (2020b): Deepfakes – Perfekt gefälschte Bilder und Videos. FTA-Monitoring für das Österreichische Parlament; parlament.gv.at/ZUSD/FTA/005_deep_fakes.pdf

ARGE ITA-AIT Parlament (2020c): Microtargeting – Personalisierte Nachrichten zur Beeinflussung von Verhalten. FTA-Monitoring für das Österreichische Parlament; parlament.gv.at/ZUSD/FTA/008_microtargeting.pdf

Falkner, G. (2021): Digitale Demokratie oder Digitale Diktatur? Keynote bei der NTA9-TA21-Konferenz in Wien, 10.-12. Mai 2021; https://www.oeaw.ac.at/ita/veranstaltungen/aktuelle-veranstaltungen/nta9-ta21-konferenz/programm

Howard, PN. (2020): Lie Machines: How to Save Democracy from Troll Armies, Deceitful Robots, Junk News Operations, and Political Operatives. New Haven/London

Howard, P.N. (2021): Lie Machines. Keynote to the NTA9-TA21 conference in Vienna, May 10–12, 2021; https://www.oeaw.ac.at/ita/veranstaltungen/aktuelle-veranstaltungen/nta9-ta21-konferenz/programm

Keller, P.; Tarkowski. A. (2021): The Paradox of Open. https://paradox.openfuture.eu/

Nentwich, M.; Jäger, W.; Embacher-Köhle, G.; Krieger-Lamina, J. (2019): Kann es eine digitale Souveränität Österreichs geben? Herausforderungen für den Staat in Zeiten der Digitalen Transformation. ITA Manu:scripts Nr. ITA-19–01; epub.oeaw.ac.at/ita/ita-manuscript/ita_19_01.pdf

Pavone, V.; Degli-Esposti, S.; Santiago, E. (2015): Key factors affecting public acceptance and acceptability of SOSTs. Deliverable D 2.4, S. 152ff.; https://surprise-project.eu/wp-content/uploads/2015/02/SurPRISE-D24-Key-Factors-affecting-public-acceptance-and-acceptability-of-SOSTs-c.pdf

RFTE – Rat für Forschung und Technologieentwicklung (2021): Thesenpapier Technologiesouveränität. Rat für Forschung und Technologieentwicklung, 19.01.2021; rat-fte.at/files/rat-fte-pdf/publikationen/2021/RFTE_Neujahrsempfang_2021_Thesenpapier.pdf

Strauß, S. (2017): A game of hide and seek? Unscrambling the trade-off between privacy and security. In Friedewald, M.; Burgess, J.P.; Čas, J.; Bellanova, R.; Peissl, W. (Hg.): Surveillance, Privacy and Security. Citizens' Perspectives. Abingdon, Oxon/New York, NY, S. 255–272