INSTITUT FÜR TECHNIKFOLGEN ABSCHÄTZUNG

Kann es eine digitale Souveränität Österreichs geben?

Herausforderungen für den Staat in Zeiten der digitalen Transformation

ÖAW ÖSTERREICHISCHE AKADEMIE DER WISSENSCHAFTEN

MANU:SCRIPTS

www.oeaw.ac.at/ita

Wien, Juni/2019
ITA-19-01
ISSN: 1681-9187

http://epub.oeaw.ac.at/ita/ita-manuscript/ita_19_01.pdf

Juni/2019
ITA-19-01

Kann es eine digitale Souveränität Österreichs geben?

Herausforderungen für den Staat in Zeiten der digitalen Transformation

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

Kurzfassung

Bislang wurden Dienste auf Basis moderner Informationstechnologie (IT) innerhalb der Verwaltung, wie Cloudcomputing, Automatisierung und Künstliche Intelligenz, hauptsächlich aus den Blickwinkeln der technischen Machbarkeit, der BenutzerInnenfreundlichkeit und der wirtschaftlichen Effizienz betrachtet. Die Perspektive der staatlichen Souveränität, also der digitalen Souveränität, steht noch aus. Dieser Artikel ist ein erster Versuch, die zahlreichen Folgen der IT für unser Verständnis der Rolle des Staates im Allgemeinen, der Plattform-Souveränität und der staatlichen Rolle als Regulator, Dienstleistungsanbieter und Käufer solcher Technologien zu überblicken. Darüber hinaus werden die gesellschaftlichen Folgen und Risiken der digitalen Technologien für politische und administrative Funktionen dargestellt und diskutiert. Die Autoren kommen zum Schluss, dass die Souveränität des Staates im digitalen Zeitalter unter großem Druck steht, sie stellen die entscheidenden Fragen, die in der Folge näher untersucht werden sollten und machen Vorschläge, wie die Gesellschaft mit dieser Herausforderung umgehen könnte.

Abstract

While so far modern IT services like cloud computing, automation, and artificial Intelligence within government have been mainly analysed from the perspectives of technical feasibility, user friendliness, and economic efficiency, their impact on the sovereignty of the state, i.e. digital sovereignty, is yet to be discussed. This article is a first attempt to give an overview on the manifold impacts of IT on understanding the role of government in general, platform sovereignty, and the role of government as a regulator, provider and buyer of such technology. Furthermore, the societal impacts and risks of digital technology for political and administrative functions are reviewed and discussed. The authors conclude that sovereignty of the state is under severe threat in the digital age; pose relevant questions for further investigation; and make proposals how to deal with this challenge.

Inhalt

IMPRESSUM

Medieninhaber:
Österreichische Akademie der Wissenschaften
Juristische Person öffentlichen Rechts (BGBl 569/1921 idF BGBl I 31/2018)
Dr. Ignaz Seipel-Platz 2, A-1010 Wien

Herausgeber:
Institut für Technikfolgen-Abschätzung (ITA)
Apostelgasse 23, A-1030 Wien
www.oeaw.ac.at/ita

Die ITA-manu:scripts erscheinen unregelmäßig und dienen der Veröffentlichung von Arbeitspapieren und Vorträgen von Institutsangehörigen und Gästen.
Die manu:scripts werden ausschließlich über das Internetportal „epub.oeaw“ der Öffentlichkeit zur Verfügung gestellt:
epub.oeaw.ac.at/ita/ita-manuscript

ITA-manu:script Nr.: ITA-19-01 (Juni/2019)
ISSN-online: 1818-6556
http://epub.oeaw.ac.at/ita/ita-manuscript/ita_19_01.pdf

Die Initialzündung zu diesem Artikel war ein Vortrag, den der Zweitautor am 28.02.2017 im ITA-Seminar gehalten hat, der eine lebhafte Diskussion ausgelöst und unmittelbar zum Wunsch nach Vertiefung der vielen aufgeworfenen Fragen geführt hat, die in unserer Einschätzung dringend umfassender Forschungsanstrengungen sowie einer intensiven öffentlichen Debatte bedürfen. Die informelle Kooperation zwischen den Autoren aus Wissenschaft und Praxis entwickelte sich über mehrere kleine Workshops; im Sommer 2018 wurde schließlich die Entscheidung getroffen, das Thema zunächst in einem Arbeitspapier überblickshaft darzustellen und die wichtigsten offenen Fragen herauszuarbeiten – in der Absicht, das Interesse des Parlaments, der verantwortlichen Ministerien und Verwaltungseinheiten sowie der Öffentlichkeit für diese wichtige Thematik zu wecken.

Alle Autoren vertreten in diesem Artikel ihre persönlichen Auffassungen und nicht notwendigerweise die Standpunkte ihrer Institutionen.

Die Autoren danken dem externen und dem internen Gutachter sehr herzlich für viele wertvolle Hinweise und Verbesserungsvorschläge.

1 Einleitung

Digitalisierung ist der größte Veränderungsprozess des ausgehenden 20. und beginnenden 21. Jahrhunderts. Kaum ein Bereich menschlicher Tätigkeit, von der Medizin und Landwirtschaft bis in die Fabriken, Büros und Schulen, von Kunst, Kultur und Wissenschaft bis zu Mobilität, Handel, Medien und vielen Facetten des Privatlebens (Unterhaltung, Kommunikation), kommt heute ohne elektronische Geräte und datengestützte Anwendungen aus. Immer höher entwickelte Informations-, Kommunikations- und Steuerungstechnologien, Datenverarbeitungen, miniaturisierte digitale Geräte aller Art, inklusive „Wearables", künstliche Intelligenz und Machine Learning, digitale Dienstleistungen und zunehmend autonome Systeme (z. B. Fahrzeuge, Roboter), teils auf Basis von Big-Data-Analytics oder Blockchain-Anwendungen prägen zunehmend das Bild einer auf fortgeschrittener und hochgradig vernetzter digitaler Technik aufsetzenden Gesellschaft.

Auch die Politik und die staatliche Verwaltung bilden bei dieser Entwicklung keine Ausnahme. Verwaltungshandeln ist längst nicht mehr Tätigkeit in Schreibstuben, schon vor rund zwei Jahrzehnten etablierte sich der Begriff E-Government. Der Staat erbringt mittlerweile mannigfache Dienstleistungen auch elektronisch über das Internet und auch im sogenannten Backoffice spielt Informationstechnologie (IT) eine zentrale Rolle. Das Verwaltungshandeln setzt immer mehr auf automationsunterstützte Kommunikation und Interaktion wie Chatbots, bündelt Dienstleistungen für die BürgerInnen in One-Stop-Shops, agiert zunehmend datengetrieben und exploriert das Potenzial von Künstlicher Intelligenz und Automatisierung, was zukünftig vermehrt zum „No-Stop-Government" führen soll, bei dem weder die BürgerInnen Anträge für Leistungen stellen, noch Verwaltungsbedienstete aktiv in Prozesse eingreifen.

Die Dynamik ist in allen angesprochenen Bereichen enorm, es ist nicht absehbar, ob sich die Entwicklung wieder abflachen und konsolidieren wird. In der Zwischenzeit sind wir Zeugen von Veränderungen, die Althergebrachtes radikal in Frage stellen oder bereits ersetzen und neuartige Möglichkeiten schaffen (Stichwort: Disruption), den Umgang miteinander, aber auch im Verhältnis zum Staat massiv beeinflussen, wirtschaftlich große Chancen bergen, aber auch die Gefahr, z. B. aufgrund von Netzwerkeffekten und Quasimonopolen ausländischer Unternehmen dauerhaft von diesen abhängig zu werden. All das wirkt sich auch auf die Individuen aus, auf deren Arbeitswelt und soziales Umfeld. Es entsteht das Bedürfnis nach Orientierungshilfen und Bildung in diesen neuen Bereichen. Überall gibt es bemerkenswerte Chancen und zugleich Herausforderungen. Zugleich muss die Gesellschaft mit den bei vielen dadurch entstehenden Ängsten umgehen, da vertraute Strukturen rasch verschwinden.

Der folgende Beitrag fokussiert auf einen Teilbereich dieser Dynamik, nämlich den öffentlichen Bereich bzw. die öffentliche Verwaltung und die Politik. Drei Bestandteile machen in der klassischen Definition einen Staat aus, nämlich Territorium, Staatsvolk und Gewaltmonopol. Durch die mit der Digitalisierung einhergehenden Veränderungsprozesse werden alle Elemente herausgefordert. Ist es erforderlich, Staat neu zu denken? Im Alltag manifestiert sich der Staat nicht zuletzt in seinem Verwaltungshandeln. Wenn sich dieses Handeln, die Grundlagen, auf denen es fußt, und die Mittel, mit denen es vollzogen wird, ändern, verändert das staatliche Handlungsweisen, das Verhältnis des Staates zu seinen BürgerInnen und internationale Abhängigkeiten. Es stellt sich letztendlich die entscheidende Frage, ob der Staat die laufenden Veränderungen unter Kontrolle hat und/oder sie ausreichend gestalten kann, um seine Souveränität zu erhalten. Unser Beitrag stellt diese Perspektive zur Diskussion, zeigt Wege zur Bewältigung einzelner aufgeworfener Probleme und Fragestellungen auf, gibt aber in erster Linie einen Überblick über die spezifischen Herausforderungen, vor die die Digitalisierung den Staat im 21. Jahrhundert stellt.

In diesem Artikel dreht sich alles um den Begriff der „Digitalen Souveränität". Dieser setzt sich aus zwei bestimmenden Teilen zusammen, nämlich Souveränität und Digitalisierung, die kurz einführend erläutert werden sollen, bevor der zusammengesetzte Begriff beschrieben wird.

„Souveränität" ist ein schillernder Begriff, der seit dem 16. Jahrhundert insbesondere in der Philosophie, im Völkerrecht, im Staatsrecht, jüngst auch in der Politikwissenschaft Verwendung findet. Im Kern geht es um ausschließliche Selbstbestimmung von Rechtssubjekten, insbesondere Staaten, aber auch von natürlichen Personen. Bei Staaten im politikwissenschaftlichen Sinne steht das Monopol der Ausübung der gesamten Staatsgewalt im Zentrum der Betrachtung. Souveränität ist ein normativer, kein deskriptiver Begriff: Ein Staat ist also Im Völker- und Staatsrecht per se souverän, egal ob er auch tatsächlich die Mittel hat, diese Souveränität auszuüben (Köchler 2016, S. 94).[1]

Absolute Souveränität kann es schon theoretisch nicht geben, da sowohl Individuen und Unternehmen als auch Staaten immer mit anderen solchen Rechtssubjekten zu tun haben, was automatisch die eigene Souveränität einschränkt, da alle Völkerrechtssubjekte formal gleich sind, also keines sich uneingeschränkt über alle anderen erheben kann; gleiches gilt selbstverständlich auch für die einzelnen Menschen aufgrund des Gleichheitsgrundsatzes (Köchler 2016, S. 96f.). Mit der Globalisierung, den damit einhergehenden mannigfachen Austauschbeziehungen und dem Aufkommen großer transnationaler Konzerne, die geschickt zwischen den einzelnen staatlichen Jurisdiktionen agieren, mit dem Aufbau transnationaler Infrastrukturen wie etwa dem Internet, aber auch mit den supranationalen Zusammenschlüssen von Staaten wie zum Beispiel der Europäischen Union, die zu geteilten Kompetenzen und damit einer Art geteilter Souveränität führen, ist der traditionelle Staatsbegriff und damit auch der Souveränitätsbegriff in einem fundamentalen Wandel begriffen.

An dieser Stelle seien kurz auch das Adjektiv „souverän" und das Substantiv „Souverän" angesprochen: Das Adjektiv kann einerseits auf Staaten angewendet werden, dann bezeichnet es deren Eigenschaft im Sinne der beschriebenen rechtlichen Selbstbestimmung. Auf Individuen bezogen wird damit hingegen die sichere oder überlegene Beherrschung einer Aufgabe bezeichnet. Diese Unterscheidung wird später, vor allem im Kapitel 5 eine Rolle spielen. Der Begriff des Souveräns meint schließlich den Inhaber der Staatsgewalt im staatsrechtlichen Sinne, somit in Österreich als Demokratie das Staatsvolk. Wenn wir von den Auswirkungen der Digitalisierung weiter Lebensbereiche, insbesondere auch des Staatshandelns, sprechen, betrifft dies also auch den autonomen staatlichen Wirkungsbereich, also den tatsächlichen Umfang der Staatsgewalt, dessen Inhaber der Souverän, also das Volk ist. In gewisser Weise geht es in diesem Artikel um die Frage, ob neben den verfassungsrechtlich verankerten Souverän schleichend ein oder mehrere (diffuse) weitere Souveräne bzw. Akteure mit Macht über ehemals exklusive Befugnisse des Souveräns Staatsvolk treten, die eben nicht das Staatsvolk sind; anders ausgedrückt, geht es um die Frage, ob der ursprüngliche, exklusive Wirkungsbereich des Souveräns eingeschränkt wird, wenn ja wie, und ob das alternativlos ist.

[1] Vgl. auch den in der Politikwissenschaft gebräuchlichen, von Michel Foucault geprägte Begriff „Gouvernementalität", wie etwa im Sammelband von Buhr, et al. (2018), der sich als Forschungsperspektive auf die verschiedenen Praktiken und Institutionen der Herausbildung von Staatlichkeit, auf die damit verbundenen Denkweisen und Wissensbestände und damit auf die Techniken des Regierens bezieht, also nicht unbedingt den Staat in den Mittelpunkt stellt. In dieser Perspektive wird, nicht unähnlich der Governanceperspektive, der Fokus auf neue Formen von Verflechtungen, Konstitutionsmomente von Macht und Staatlichkeit oder Fragen der Territorialisierung gelegt (ibid. 5f.). Ben Kamis (2018) beschreibt im selben Sammelband Gouvernementalität als diffuse Herrschaft in postnationalen digitalisierten Gesellschaften.

Unter „Digitalisierung“ wird im engeren Sinne das Umwandeln von analogen in digitale Daten verstanden, um sie in Computersystemen weiterverarbeiten zu können. Zumeist, so auch hier, wird damit aber der durch digitale Computertechnologien ausgelöste Umbruch in nahezu allen Lebensbereichen (siehe oben einleitend) verstanden.

Der Begriff der „Digitalen Souveränität“ bezeichnet in erster Annäherung also „Souveränität unter den Bedingungen der Digitalisierung“. Es liegt zwar nahe, diesen Begriff auf Staaten anzuwenden – was wir in der Folge auch tun werden – jedoch ist zu beobachten, dass die meisten Diskussionsbeiträge dazu in erster Linie die Souveränität Einzelner meinen, sei es von Individuen, sei es von Unternehmen. Hier kommt dann oft die zweite adjektivische Bedeutung von „souverän“ ins Spiel, geht es doch häufig um Medienkompetenz, also den „souveränen Umgang“ mit digitalen Medien. Studiert man etwa die Beiträge in dem umfangreichen Sammelband von Mike Friedrichsen und Peter-J. Bisa „Digitale Souveränität. Vertrauen in der Netzwerkgesellschaft“ (2016), wird rasch klar, dass die primäre Bezugsebene nicht der Staat ist, mit wenigen Ausnahmen (etwa Baums 2016 zur Standortpolitik; Tauber 2016 zu den öffentlichen Rechenzentren; Köchler 2016 allgemein zum Begriff).

Auf Staaten bezogen bekommt der Begriff der Digitalen Souveränität eine viel größere Breite und Tiefe, denn 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, auch die Herstellung jener rechtlichen und infrastrukturellen Rahmenbedingungen, die es seinen StaatsbürgerInnen selbst ermöglicht, digital souverän zu handeln. In der Folge werden wir uns der Digitalen Souveränität des Staates, konkret Österreichs, widmen. Auf die „digital souveränen BürgerInnen“ bzw. Unternehmen wird nur indirekt Bezug genommen, nämlich dann, wenn es darum geht, was der Staat für diese tun kann oder sollte (etwa bei der Bereitstellung sicherer Infrastruktur oder bei der Bildung).

Das Leitthema dieses Artikels ist die provokante Frage im Titel, nämlich ob es überhaupt eine digitale Souveränität Österreichs (stellvertretend für alle Nationalstaaten) geben kann. Um diese Frage ansatzweise zu beantworten, bedarf es zunächst eines Überblicks, in welcher Weise die staatliche Souveränität durch die laufende digitale Transformation aller Lebensbereiche herausgefordert wird und welche Gegenmaßnahmen technisch und organisatorisch umsetzbar wären. Wir analysieren diese Fragestellung in vier Bereichen: In Abschnitt 2 fokussieren wir auf das digitale Verwaltungshandeln des Staates, in Abschnitt 3 auf seine Funktion als Provider kritischer digitaler Infrastrukturen, in Abschnitt 4 auf den neuerdings auch digitalen Rahmen für den politischen Prozess und schließlich in Abschnitt 5 auf die staatliche Rolle in Hinblick auf die digitale Souveränität seiner BürgerInnen. Unser Überblick über diese teils massiven Herausforderungen für die (digitale) Souveränität lässt freilich noch viele Fragen offen, wie wir im Fazit einräumen werden.

2 Der Staat und die Digitalisierung der Verwaltung

In diesem Abschnitt analysieren wir, wie der Staat in seinem Hauptaufgabenbereich, der Verwaltung des Gemeinwesens, zunehmend mit Digitalisierung zu tun hat und daher aufgrund der konkreten technischen Eigenschaften der digitalen Technologien und deren globaler Vernetzung in seiner Souveränität massiv herausgefordert ist.

2.1 Verwaltungs-IT im Wandel des Verwaltungsverständnisses

Das Verwaltungsverständnis hat sich in den letzten Jahrzenten sowohl aufgrund des politischen Selbstverständnisses der BürgerInnen als auch der Regierenden stark gewandelt. So sind unterschiedliche Phasen des IT-Einsatzes in diesem sich wandelnden Selbstverständnis zu identifizieren.

Hoheitsverwaltung: Jahrtausende lang hatte die Verwaltung den Zweck, Ordnung im Staat zu erhalten und vor allem die notwendigen Geldquellen für Sicherheit, Rechtsprechung und staatliche Investitionen zu sichern. Der Fokus der Verwaltung lag in der professionellen, reibungsarmen Abwicklung der Umsetzung der Gesetze. Daher unterstützte die IT zunächst vor allem die effiziente Abwicklung von verwaltungsinternen Abläufen. Mächtige Back-End-Systeme erlaubten rasche Abwicklungen und Berechnungen, Abläufe wurden digital unterstützt – IT wurde als „mehr desselben" zur Steigerung der Verwaltungseffizienz eingesetzt. IT war anfangs eine neue Spitzentechnologie, die wenigen SpezialistInnen vorbehalten war. In dieser Pionierphase wurden innerhalb der Verwaltung kleine Technikabteilungen geschaffen, die mit den marktbeherrschenden internationalen Herstellern Back-End-Systeme aufbauten. Die Nutzung der Informationstechnik fokussierte auf mathematische Aufgaben (Steuerberechnungen), planerische Aufgaben (Budgetierung) und Textverarbeitung innerhalb geschlossener Applikationen.

Serviceverwaltung: Spätestens in den 1960er-Jahren kam der Obrigkeitsbegriff und die damit zusammenhängende Wahrnehmung der BürgerInnen als BittstellerInnen immer mehr unter gesellschaftliche Kritik. Eine politisch engagierte Öffentlichkeit verlangte Verantwortungsübernahme durch die Politik und einen Dialog mit BürgerInnen auf Augenhöhe. Gleichzeitig kam es mit der zunehmenden Sättigung von Konsumbedürfnissen in Österreich zu einem vermehrten Augenmerk auf die Servicequalität im Wirtschafts- und Konsumleben. Mit dieser neuen Sicht wurde Verwaltung zunehmend als eine den BürgerInnen verpflichtete Organisation zur Lieferung von staatlichen Dienstleistungen gesehen. Staatliche Dienstleistungen wurden und werden mit dem Servicegrad der Privatwirtschaft verglichen. Diese Neuorientierung wurde von der Politik ab der Jahrtausendwende in Form des Ziels einer an den BürgerInnen orientierten Verwaltung aufgegriffen. Der Servicecharakter rückte in den Vordergrund und die Vorgaben an die Verwaltung änderten sich zu: Schnelligkeit der Erledigung; zentrale BürgerInnen-Portale (Auskunft, Abwicklung etc.); Verfügbarkeit rund um die Uhr. Dieser neue Fokus führte zu neuen, bürgerzentrierten, innovativen Angeboten (wie zum Beispiel Finanz Online für die Steuererklärungen) aber auch zu Applikationssilos, mangelnder Interoperabilität und unterschiedlicher Qualität von Software. Kernaufgaben in dieser expansiven Phase der IT waren die Etablierung eines IT-Prozessmanagements (Information Technology Infrastructure Library/ITIL etc.) und von Software-Architektur-Frameworks zur Standardisierung.

Plattformverwaltung: Durch die Entwicklung intuitiver, nutzerorientierter Geräte und Anwendungen sowie automatisierter, virtueller Cloud-Computing-Techniken wurden in den letzten Jahren neue, globale privatwirtschaftliche Geschäftsmodelle (z. B. Software as a Service, Handelsplattformen wie eBay, Amazon, Social-Media-Plattformen) etabliert. Diese Plattformen stellten weltweit einfach zu bedienende Services für UserInnen und Firmen als Eco-Systempartner zur Verfügung. Sie revolutionierten unser Einkaufs-, Konsum- und, via Social-Media-Plattformen, unser Informationsgewinnungs- und Kommunikationsverhalten. Sie ermöglichten durch die Verbindung von NutzerInnen, Anbietern und Produkten das schnelle Auffinden einer riesigen Anzahl von Nischenprodukten und eine einfache Bezahl- und Transportlogistik. Die Daten, welche durch die digitale Abwicklung von Transaktionen anfallen, ermöglichen neue Mehrwerte in Form von größeren Warenangeboten, besseren Preisen, Produktbewertungen oder Vernetzungsoptionen, welche den Nutzen dieser Plattformen für alle TeilnehmerInnen (Betreiber und NutzerInnen) weiter erhöhen (Mayer-Schönberger/Ramge 2017). Zusätzliche Plattform-Angebote sind Empfehlungen von anderen NutzerInnen, treffsichere Vorschlagssysteme und die Möglichkeit, unterschiedliche Waren- und Kontakt-Optionen leicht überschaubar zu bündeln.

Diese neue Serviceart avancierte in den letzten Jahren auch zum Vorbild der Dienstleistungserbringung durch den Staat. Die Verwaltung soll – in Analogie zur Privatwirtschaft – neue digitale Verwaltungsservices anbieten, unter anderem nach den folgenden Prinzipien:

- *Mobility:* mobiler Zugriff auf alle Informationen und Transaktionen mit der Verwaltung via mobiler Endgeräte;
- *One stop government:* lebenslagenspezifische Bündelung von Verwaltungsaufgaben quer über ministerielle Zuständigkeiten;
- *Once only principle:* Unterstützung durch Ausfüllhilfen, automatische Nutzung von bereits vorhandenen Daten (z. B. Adresse, Sozialversicherungsnummer, Steuernummer etc.), und proaktive Vorschläge für Einreichungen;
- *No stop government:* Automatisierung von Verfahren ohne der Notwendigkeit, Anträge einzubringen oder manuell einzugreifen;
- *Location based services:* ortsspezifische Dienstleistungen und Auskünfte, wo sich staatliche Service-Stellen befinden; und
- *Open data:* Bereitstellung von Daten zur Nutzung für privatwirtschaftliche Services.[2]

In Analogie zu den privatwirtschaftlichen Plattformen wurde in den USA um 2010 die Idee des „Digitalen Plattform-Staates“ geboren (O’Reilly 2010). Diese Idee postuliert, dass die staatliche Hauptaufgabe darin besteht, für die BürgerInnen, Firmen und Verwaltungseinheiten eine Interaktionsplattform zur Verfügung zu stellen. Auf dieser Plattform würden nicht nur alle Interaktionen mit der Verwaltung stattfinden, sondern auf ihr könnten alle Stakeholder ihr Wissen und ihre Informationen bündeln und miteinander agieren.

Zu diesem Ansatz eines „Government-as-a-platform“ bestehen auch in Europa immer mehr konkrete Beispiele. So setzt insbesondere Estland auf diesen (Stichwort: „E-Society“) und geht dabei aktiv in die Innovatorenrolle und beschränkt sich nicht auf Regulierung von Technologien. (Plantera 2018). Die Idee der staatlichen BürgerInnen- und Unternehmerplattform zur zentralen Kommunikation mit der Verwaltung ist auch im Regierungsprogramm der aktuellen österreichischen Regierung bereits angesprochen und wurde im März 2019 mit oesterreich.gv.at präsentiert.[3]

---

[2] Beispiel Wien: wiengestalten.at/open-government-data-wien/. [Dieser und alle weiteren in diesem Artikel angegebenen URLs wurden zuletzt am 01.03.2019 aufgerufen.]

[3] Regierungsprogramm 2017-2022 der österreichischen Bundesregierung 2017, S. 81, bundeskanzleramt.gv.at/documents/131008/569203/Regierungsprogramm_2017%e2%80%932022.pdf/b2fe3f65-5a04-47b6-913d-2fe512ff4ce6.

Auch in dirigistischen Staaten werden analog staatliche Interaktions-Plattformen[4] (unter Einbindung privater Akteure) aufgebaut. In diesem zu Europa unterschiedlichen politischen Umfeld nutzt beispielsweise die politische Führung Chinas u. a. die private Marktplattform Alibaba, um die Datenkontrolle über alle BürgerInnen (Lee 2017) und Firmen – nicht nur chinesische – zu erhalten. Diese und viele weitere auf staatlichen und privaten Plattformen gesammelte Daten erlauben ein „Scoring" von BürgerInnen und Firmen entsprechend ihrem Wohlverhalten samt staatlichen Sanktionsmöglichkeiten.

2.2 Auf dem Weg zur teilautomatisierten digitalen Verwaltung

Während die Entwicklung zum Staat als Dienstleister in vielen Bereichen schnell voranschreitet und digitale staatliche Plattformen gerade etabliert werden, zeichnet sich in den letzten Jahren ein darüber hinausgehender Trend der zunehmenden Automatisierung der digitalen Verwaltung ab.

Regelbasierte Automatisierung: Regelbasierte Tätigkeiten wurden bereits am Anfang der Verwaltungs-IT mittels Verwaltungsapplikationen und Workflows teilautomatisiert verrichtet. Standardabfragen und die Aufbereitung von unterschiedlichen Informationsquellen können auch mit klassischen IT-Methoden einfach erledigt werden. Diese Automatisierungen sind strikt regelbasiert, in jedem Fall leicht nachzuvollziehen und enthalten keine Entscheidungspunkte. Falls Entscheidungen nötig sind, werden diese innerhalb der Workflows von Menschen getroffen. Durch die Fortschritte in der Softwaretechnik bieten klassische, repetitive Verwaltungstätigkeiten ein einfach zu hebendes Personal-Einsparungspotential (Maciag 2018). Aufgaben wie Anonymverfügungen aufgrund von Geschwindigkeitsüberschreitungen im Straßenverkehr erfolgen daher vom Erkennen der Zulassungsnummer, der Identifikation des/der Eigentümers/Eigentümerin mit gemeldeter Adresse bis zum Festsetzen des Strafmaßes bereits zu 100 % über IT-Systeme. Auch die Mehrzahl der Steuerbescheide wird vollautomatisch, regelbasiert erstellt und erlassen. Damit werden bereits autoritative Verwaltungstätigkeiten, die die BürgerInnen zu etwas verpflichten, von Maschinen erledigt.

Algorithmen-unterstützte Automatisierung: Bisher galten Arbeiten wie das Manipulieren, Klassifizieren von Schriftstücken, das Verknüpfen von Informationen und das Treffen von Entscheidungen als typisch menschliche Domäne. Die berühmt gewordene Digitalisierungsstudie aus Oxford (Frey/Osborne 2013), prognostizierte, dass in den USA ca. 47 % aller Tätigkeiten in Organisationen prinzipiell durch den Einsatz von Big Data und Künstlicher Intelligenz automatisierbar seien, mit einem Schwerpunkt auf jenen Verwaltungstätigkeiten, welche Informationen auf- und für Entscheidungen vorbereiten. Auch wenn diese Studie wissenschaftlich umstritten ist, so kommen doch alle Nachfolgestudien zu zwar geringeren Prozentsätzen, untermauern aber die festgestellte Grundtendenz (EPTA 2016).

In der Privatwirtschaft versuchten zunächst Finanzdienstleister die Abarbeitung von Einzelfällen durch IT zu unterstützen und zu automatisieren. Die Politik und mit ihr die Verwaltung sehen in diesen technologischen Entwicklungen die Möglichkeit, das Service für die BürgerInnen zu verbessern und zugleich (Personal-)Kosten zu sparen. Diese Entwicklungen bringen Verbes-

[4] Ministry of Finance Singapore eGov2015 Masterplan: „eGov2015 is about building an interactive environment where the Government, the private sector and the people work together seamlessly, through the enabling power of infocomm technologies." mof.gov.sg/Policies/e-Government.

serungen für die Verwaltungsleistung und die BürgerInnen, nämlich die Erhöhung der internen Effizienz der Verwaltung und rasche Durchlaufzeiten der Geschäftsfallerledigung für die BürgerInnen – im Idealfall sekundenschnelle.

Verwaltungsinterne intelligente Automatisierung wie Text erkennende, semantische Systeme, welche E-Mails und einlangende Schriftstücke automatisch nach Inhalt klassifizieren und verteilen, werden bereits vereinzelt eingesetzt. Intelligente Informationssysteme wie Chatbots nach dem Vorbild von Siri/Alexa etc. sollen in naher Zukunft den BürgerInnen mit KI-gestütztem Rat zur Seite stehen und Empfehlungen abgeben, jedoch keine Entscheidungen treffen.

Die prinzipielle politische Verpflichtung der rechtsstaatlichen Verwaltung, objektiv, ohne Ansehen der Person, nach gesetzlichen Regeln standardisiert (Gleichheitsgrundsatz) zu handeln, erleichtert die Automatisierung sowohl technisch als auch politisch. Als absolut regelkonformer, von der Willkür einzelner Verwaltungsbediensteter unabhängiger Gesetzesvollzug erscheint die digitale Automatisierung geeignet und attraktiv. Außer Acht gelassen werden dabei jedoch meist noch Überlegungen im Hinblick auf Algorithmen innewohnende Diskriminierungen (vgl. unten im nächsten Abschnitt).

KI-unterstützte Entscheidungen: Ein Einsatz von Künstlicher Intelligenz besteht darin, auch abwägende, beurteilende Verwaltungsschritte mittels Algorithmen zu unterstützen. So werden in den USA Systeme zur Beurteilung der Rückfallwahrscheinlichkeit von Straftätern auf Grundlage der Auswertungen beschlagnahmter Unterlagen, von Vernehmungen und anderen vorbereitenden Tätigkeiten eingesetzt (O'Neil 2017). Auch wenn in diesem Beispiel und vielen anderen Anwendungen derzeit Menschen die Letztbeurteilung vornehmen, so ist es schwierig, gegen den Vorschlag eines amtlichen Vorschlagssystems zu handeln. Einerseits ist es zeitintensiv, alle vorbereitenden Schritte manuell nachzuvollziehen, andererseits stellen derartige Vorschläge eine Verantwortungsentlastung dar. Es wird dem vermeintlich von Menschen nicht beeinflussten Vorschlag eine größere Objektivität zugeschrieben. Dadurch kommen dem Vorschlag widersprechende Personen in die Situation, ein Abweichen rechtfertigen zu müssen. Eine vorschlagskonforme Entscheidung ist dagegen nicht begründungspflichtig, weil dann davon ausgegangen wird, dass der Mensch die Entscheidungsgrundlagen in der gleichen Weise wie die Maschine bewertet hat. Oft lernen derartige Systeme aus den Bewertungen der einzelnen NutzerInnen oder anhand von Menschen bewerteter Trainingsbeispiele. Die laufende Forschung hat gezeigt, dass durch dieses Lernen bestehende gesellschaftliche Meinungen und Vorurteile „unsichtbar" in einen scheinbar objektiven Mechanismus übertragen werden. Dies kommt insbesondere beim sozialen Risiko-Scoring durch KI-Systeme zum Vorschein, wo implizite Vorurteile zu eklatanten Fehlbeurteilungen führten (Eubanks 2018; Kehl et al. 2017). Jüngst wurden auch in Österreich die Diskriminierungspotenziale von Algorithmen anhand des so genannten „AMS-Algorithmus" diskutiert, einem auf statistischen Daten beruhenden Tool, das 2019 testweise, ab 2020 im Vollbetrieb Arbeitssuchende in Gruppen mit unterschiedlichen Vermittlungschancen und daraus folgend unterschiedlicher Behandlung durch das Arbeitsmarktservice einteilen soll.[5]

Die Konsequenzen aus dieser (teilweisen) Abgabe von Verwaltungstätigkeiten werden erst in der Langzeitbeobachtung solcher Systeme sichtbar und schrittweise hinterfragt. Im operativen Tagesgeschäft mit limitierter Sicht und beschränkten Ressourcen unterbleibt oft eine generelle Abwägung und Neubewertung des Verwaltungshandelns und der neuen Abhängigkeit von Technologielieferanten und -bereitstellern. Auch wenn eine sachliche Evaluierung solcher Systementscheidungen und Maßnahmen wünschenswert erscheint, sind einerseits oft die Mittel

[5] Futurezone, 17.10.2018, futurezone.at/netzpolitik/der-ams-algorithmus-ist-ein-paradebeispiel-fuer-diskriminierung/400147421.

dafür nicht vorgesehen und organisationsintern schwerer zu beschaffen als zusätzliche Ressourcen zur Nachbesserung an bestehenden Systemen. Andererseits mag auch eine mangelnde positive Kultur im Umgang mit Fehlern dazu führen, dass einmal implementierte Systeme nicht mehr in Frage gestellt werden, selbst wenn sich ihr Nutzen nicht in der erwarteten Weise darstellt oder gar systematische Fehler als Einzelfälle (mit für diese Einzelfälle drastischen Auswirkungen) abgehandelt werden.

Offene Fragen zur Teilautomatisierung der Verwaltung:

- Wer übernimmt die Verantwortung für das Restrisiko automatisierter Entscheidungen, welche aufgrund statistischer, laufend optimierter Entscheidungsalgorithmen getroffen werden? BeamtInnen, welche als Domain-ExpertInnen die Anforderungen des Prozesses und Fragestellungen beherrschen, nicht aber die möglichen Fehler und Verzerrungen der mathematischen Algorithmen und deren Optimierungen (Bias)? Der Softwarehersteller, welcher vorgegebene mathematische Regeln codiert, aber nicht den Kontext und das Domain-Wissen kennt, in dem die Anwendung stattfindet? Der/die Implementierende, welche/r nur Parametereinstellungen vornimmt? Der Bereitsteller der Trainingsdaten für die laufende Weiterentwicklung des Algorithmus, der sich (durchaus gewollt) vom Ursprungszustand weiterentwickelt? Oder der Staat als Letztverantwortlicher für den Einsatz von teilautomatisierten Verwaltungssystemen?
- Wie kann sichergestellt werden, dass Algorithmen regelmäßig überprüft werden, um frühzeitig Individuen oder die ganze Gesellschaft betreffende Fehlentwicklungen zu erkennen?
- Inwieweit ist das im Regierungsprogramm 2017-2022[6] erwähnte „Einrichten eines ‚Ethikrates für gesellschaftliche Fragen in Zusammenhang mit der Digitalisierung'„ vorangeschritten und welche Erfahrungen gibt es hierzu?
- Wie kann sichergestellt und bewertet werden, dass ein automatischer oder autonomer Algorithmus geeignet ist und wie könnten allenfalls gesellschaftspolitisch unerwünschte Verzerrungen korrigiert werden?

2.3 Verwaltungsabhängigkeit von globalen digitalen Plattformen

Durch die Bündelung von Transaktionen vieler Individuen gewinnen privatwirtschaftliche Plattformen eine hohe, teils oligopolistische Wirtschaftsmacht und können Regeln zur Lösung von Transaktionskonflikten, zur Nutzung von Daten und zur Akzeptanz von Vertragsbedingungen unabhängig von nationalem Recht de facto erzwingen.

Plattform-Geschäftsmodell: Der Nutzen insbesondere privater digitaler Plattformen liegt unter anderem in den vielfach als brauchbar wahrgenommenen Empfehlungs- und Kaufvorschlagssystemen (Recommender-Engines) – sowohl für KundInnen als auch für Anbieter. Die Kundschaft erhält Angebote, welche sie selbst im unüberschaubaren Online-Angebot nicht hätte finden können, die Anbieter Kundenprofile, die sich für Werbung auf individueller Basis oder zur Optimierung des Angebots nutzen lassen. Das derzeitige Geschäftsmodell der großen Plattformen basiert auf der Verwertung der für eine andere Dienstleistung ohne Kosten gesammelten Daten zu „Verhaltens(vorhersage)-Produkten" für Produzenten, Werbeagenturen und Parteien (Zuboff 2016). Diese Produkte werden umso wertvoller, je präziser sie werden. Dies setzt eine Dynamik zu stärker personalisierter, digitaler Verhaltensanalyse in Gang. Der Platt-

[6] Siehe FN 3, Österreichisches Regierungsprogramm 2017, S.79.

formgigant Google hat sich konsequenterweise als Mission gegeben: „Wir versuchen, Bedürfnisse unserer Nutzer weltweit zu erkennen, bevor diese explizit ausgesprochen sind, und diesen Bedürfnissen dann mit Produkten und Diensten gerecht zu werden."[7]

Diese Plattformvision lässt sich nur mit einem „gläsernen Kunden" erreichen, wobei Algorithmen aus den umfassenden Daten Schlussfolgerungen ziehen, die dem Menschen selbst (noch) nicht bewusst sind. Dieser ultimative Servicegedanke führt zur Notwendigkeit des Sammelns von Daten über alle menschlichen Bereiche.

Wirtschaftssouveränität von Plattformen: Durch die Akkumulation von Daten, insbesondere Transaktionsdaten, sind auch präzise gesellschaftliche und wirtschaftliche Prognosen möglich. Die Inhaber dieser Daten und damit Prognosemöglichkeiten, große Plattformbetreiber wie zum Beispiel Amazon oder Facebook, verfügen über einen Informationsvorsprung und können diesen zur Beeinflussung von Wirtschaft und Staat nutzen. So können Prognosen über die Wirtschaftsleistung aus den Datenbeständen von Plattform-Giganten zu einem verminderten Bonitäts-Rating führen, das zu höheren Zinsen bei der Staatsverschuldung beiträgt, was dann tatsächlich zu vermindertem Wachstum führen kann. Die Möglichkeiten, die die großen Firmen auf Grund ihrer Marktmacht und Kapitalisierung haben – besonders wenn man den Hebel bedenkt, den sie über die potentielle Beeinflussung ihrer breiten Kundschaft hätten – werfen die Frage auf, ob Staaten hier wirklich unabhängig von diesen Plattformen agieren können. So hatte Googles Eric Schmid bereits 2010 angedeutet „*There are many, many things that Google could do, that we chose not to do ... One day we had a conversation where we figured we could just try to predict the stock market. And then we decided it was illegal. So we stopped doing that*." (zitiert nach Tate 2010).

Durch die immer größer werdende Bedeutung selbstlernender Systeme können die Machtasymmetrien am Markt oder zwischen dem privaten und dem staatlichen Bereich weiter zunehmen. Für den erfolgreichen Einsatz Künstlicher Intelligenz sind nämlich vor allem Trainingsdaten erforderlich. Wer also schon jetzt große Datenmengen sein Eigen nennen kann, hat auf dem umkämpften Markt bestimmt einen Vorteil zu erwarten (Mayer-Schönberger/Ramge 2017). Man kann davon ausgehen, dass das Datenschutzprinzip der Zweckbindung, also keine über den ursprünglichen Zweck der Datensammlung hinausgehende Nutzung, zukünftig eine vernachlässigbare Rolle spielen wird, sofern nicht regulierend eingegriffen wird.

Funktionale Souveränität von Plattformen: Die Fähigkeit von privaten digitalen Plattformen – zwischen vielen Marktteilnehmern

1. Transaktionsregeln unabhängig von nationalem Recht (durch Gestaltung der konkreten Transaktions- und Informationsoptionen) festzulegen,
2. TeilnehmerInnen effektiv einseitig von der Nutzung der Plattform, meist mit Nachteil für die Betroffenen, auszuschließen (durch Sperren, Nicht-Zulassen von potentiellen NutzerInnen) und
3. Dispute auf der Plattform (durch Moderation, Löschung oder Erzwingen von Geschäftsbedingungen) zu entscheiden und
4. öffentliche Diskussionen, Gruppenbildungen und soziale Aktivitäten zu verbieten (Sperren von Gruppen) sowie intransparenten, exklusiven Zugang zu Daten (an politische und privatwirtschaftliche Akteure) zu gewähren

gibt ihnen eine *funktionale Souveränität* (Pasquale 2018), welche bisher klassischerweise vom Staat ausgeübt wurde. So werden Ansprüche des Staates und der Legislative auf vertragsrechtliche Normierung (ad 1), auf Sicherstellen des gleichberechtigten Zugangs zu wesentlichen

[7] Google/Über Google/Unsere 10 Grundsätze, Grundsatz 10, google.com/about/philosophy.html.

Kommunikationsmitteln (ad 2), auf Rechtsprechung im Streitfall (ad 3) und Sicherstellung der Versammlungsfreiheit und Freiheit der Meinungsäußerung (ad 4) durch Plattformen nicht honoriert. Die intransparente Beeinflussung der öffentlichen Meinung stellt auf diesem technologischen Niveau eine neue politische Herausforderung für den Staat dar (siehe Kapitel 4).

Derzeit sind wir Zeuge eines Kampfes zwischen der staatlichen und der funktionalen Souveränität. Eine Reaktion von Staaten in Ausübung ihrer Souveränität auf die oben genannte Erosion der eigenen Souveränität durch die Plattformen besteht darin, über systematischen Zugriff auf die Daten privater Plattform-Giganten wie Amazon, Microsoft, Facebook oder Alibaba selbst die politische Diskussion zu beeinflussen und diese Daten zur Durchsetzung nationaler Gesetze zu nutzen. Der Zugriff der US-amerikanischen staatlichen NSA auf die Daten dieser Privatunternehmen zeigt, dass die Macht dieser Plattformen staatlicherseits anerkannt und benutzt wird (Greenwald 2014). Jüngst wird auch politisch diskutiert, staatliche Befugnisse auch an solche Plattformen abgetreten, zum Beispiel durch Zensurgebote in Form von Upload-Filtern.[8]

Offene Fragen[9] zu digitalen Plattformen:

- Wie kann sich staatliche Souveränität von funktionaler Souveränität abgrenzen und welche Konzepte gibt es dafür? Welche klassischen Politikfelder sind durch digitale Plattformen direkt betroffen?
- Welche Konzepte digitaler Souveränität werden in anderen Staaten verfolgt (Vergleichsstudie global, EU-weit) und welche Lehren sind für Österreich ableitbar?
- Wo haben sich nicht-staatliche Souveränitätsgebiete bereits etabliert und wie werden diese von der Bevölkerung aufgenommen?
- Wo besteht eine Abhängigkeit zur Erfüllung von staatlichen Aufgaben von digitalen Plattformen?

[8] Netzpolitik, 26.03.2019, #CopyFail: EU-Parlament beschließt Uploadfilter, netzpolitik.org/2019/copyfail-eu-parlament-beschliesst-uploadfilter/.

[9] All diese Fragen stellen sich unabhängig von illegalem Datendiebstahl, Hacking oder Datenschutzverletzungen bei Individuen.

3 Der Staat als Provider kritischer digitaler Komponenten

Der Staat tritt auch in Zeiten der Digitalisierung nicht nur mit seinen eigenen staatlichen Dienstleistungen (hier: Verwaltungshandeln inklusive Verteidigung) auf, sondern stellt auch kritische Infrastrukturen wie Verkehrs-, Energie- und Kommunikationsnetze, Rechenzentren, Gesundheits- und Sicherheitseinrichtungen für seine BürgerInnen zur Verfügung, auch wenn es mittlerweile zusätzlich viele private Dienstleister und Provider gibt. im neuen digitalen Bereich gelten jedoch z. T. andere Spielregeln und Risiken, wie in der Folge gezeigt werden kann.

3.1 Sicherheitsrisiken der digitalen Basisinfrastruktur

Staatliche Souveränität kann in den Kategorien der letztinstanzlichen juristischen Entscheidungs- und Rechtsgewalt im eigenen Territorium und der Fähigkeit, diese nach innen und außen durchzusetzen, beschrieben werden (Münkler/Straßenberger 2016). Die neuen, digitalen Verwaltungssysteme weisen mehrere neuartige Charakteristika auf, welche die bisherige Funktionsweise der Verwaltung gegenüber den BürgerInnen verändern. Wesentliche kritische Merkmale der neuen Instrumente in der Verwaltungs-IT sind Vernetzung, intransparente Funktionsweise und Delokalisierung möglicher Angriffshandlungen.

Vernetzung digitaler Infrastrukturen: Durch die weltweite Vernetzung und den potentiell weltweiten Zugriff auf digitale Assets wie IT-Infrastrukturen, alle IT-gesteuerten Geräte und Steuerungseinheiten (Stichworte: Internet of Things und Industrie 4.0) sind territoriale Absicherungsmaßnahmen (der Vergangenheit) gegen örtlichen Zugriff nicht wirksam. Beispiele wie Stuxnet (Zetter 2014), mit dem Urananreicherungsanlagen über fremde Malware zerstört wurden, um Waffenentwicklungen zu verhindern, bis zu umfangreicher, systematischer digitaler Industriespionage, um an militärtechnische Erkenntnisse zu kommen, sind heute wohlbekannt. Schon vor den Enthüllungen von Edward Snowden wurde vermutet, dass allgemein verkaufte Industrieprodukte Backdoors für Datenabfragen und verdeckte Steuerung über Fernzugriff fabrikmäßig eingebaut haben könnten. Kein digitales Verwaltungsasset ist von einer Vernetzung auszuschließen, ohne dass die Leistung als Verwaltungswerkzeug leidet. Verwaltungsorganisationen sind daher in dem gleichen Dilemma gefangen, das viele andere Bereiche der Digitalisierung ebenfalls bieten: Um die Sicherheit zu gewährleisten, dürften die Komponenten nicht vernetzt sein. Um die größtmögliche Funktionalität zu bieten, ist eine weitreichende Vernetzung erwünscht. Dadurch wird der Aspekt der Informationssicherheit oft als Hindernis (die vom Hersteller versprochenen Funktionen nutzen zu können) wahrgenommen. Für kritische Systeme ist jedoch der Sicherheit jedenfalls der Vorrang zu geben. Nicht nur weitere Einfallstore werden durch Vernetzung geöffnet, auch die Komplexität steigt, wodurch auch die Fehler- und Ausfallwahrscheinlichkeit steigt (Strauß/Krieger-Lamina 2017). Schließlich muss auch darauf hingewiesen werden, dass der Aufwand, vernetzte Systeme sicher zu betreiben, deutlich höher ist, da alle Schnittstellen zu anderen Systemen abgesichert und gewartet werden müssen.

Intransparente Funktionsweise von IT-Komponenten: Alte „Instrumente“ waren in ihren Wirkungen bisher klar beurteil- und abschätzbar. Was ein physisches Werkzeug kann oder nicht kann, ist in der Regel klar nachvollziehbar und bekannt. Ganz anders verhält es sich mit Universalwerkzeugen, deren Programmstruktur in industrieller proprietärer Hard- und Software nicht offenliegt. Der Verwendungsausschluss für chinesisches IT-Equipment[10] und russische Software durch US-amerikanische und britische Behörden[11] basiert auf diesen zwar plausiblen, aber bisher unbewiesenen Vorwürfen. Ebenso gibt es Diskussionen rund um die Netzwerkkomponenten des US-Konzerns CISCO und auch das European Telecommunications Standards Institute (ETSI) beschäftigt sich mit Abhörschnittstellen.[12] Es sind also weder die Integrität der verwendeten Verwaltungswerkzeuge noch deren Funktionieren gesichert – im Gegenteil ist die Verwaltung potentiell weltweit verdeckt und angreifbar, ohne dass der Staat es weiß.

Delokalisierung möglicher Angriffshandlungen auf digitale Infrastrukturen: Mit dem Einsatz von IKT-Verwaltungswerkzeugen gehen viele Veränderungen einher. Manche erschließen sich sofort, so wie veränderte Wartungsmaßnahmen, andere sind nicht gleich offensichtlich. Durch die Vernetzung mit dem Internet und anderen Datennetzen, die nicht unter der direkten Kontrolle der staatlichen Verwaltung betrieben werden, sind diese Komponenten jederzeit und von überall auf der Welt angreifbar. Musste in vergangenen Zeiten eventuell nur der Raum mit der EDV-Anlage versperrt werden, muss nun auch der Zugriff aus dem virtuellen Raum kontrolliert werden. Dort lauern allerdings ungleich mehr Angreifer, von denen die meisten nie sichtbar werden, auf ihre Chance. Das geht von meist glimpflich verlaufenden Störaktionen über Datendiebstähle bis hin zu gezielten Angriffen auf die staatliche Verwaltung mit dem Ziel, deren Handlungsfähigkeit einzuschränken oder ganz auszuschalten. Wenn man sich die Aufgaben und Dienstleistungen des Staates vergegenwärtigt, von einfachen Verwaltungsakten bis hin zur Landesverteidigung, wird die Brisanz dieser Entwicklung deutlich. Ein spezielles Angriffsmuster stellen dabei mit „Schläfern“ vergleichbare Programme dar, die schon sehr früh auf relevante Systeme eingebracht werden, um dort auf den zentralen Angriffsbefehl zu warten, der in der Regel erfolgt, wenn der größtmögliche Schaden zu erwarten ist, bspw. während Wahlen. Der Schutz der vernetzten Systeme wird durch die asymmetrische Bedrohung schwierig und ist mit hohem Ressourcenaufwand verbunden.

---

10 Reuters, 27.07.2018, „Pentagon report will reveal military’s dependence on Chinese components”, reuters.com/article/us-usa-china-pentagon/pentagon-report-will-reveal-militarys-dependence-on-chinese-components-idUSKBN1KH1TI.

11 Die Welt, Wirtschaft 02.12.2017, Behörden warnen vor Russischem Kaspersky Virenscanner, welt.de/wirtschaft/article171194420/Behoerden-warnen-vor-russischem-Kaspersky-Virenscanner.html.

12 Heise online, 14.11.2018, „Verschlüsselung: Europäischer Abhör-Standard veröffentlicht“, heise.de/security/meldung/Verschluesselung-Europaeischer-Abhoer-Standard-veroeffentlicht-4220967.html. Siehe dazu auch in Abschnitt 3.2 unten.

3.2 Anforderungen an kritische Infrastrukturen im digitalen Zeitalter

Das Deutsche Fraunhofer-Institut FOKUS definiert digitale Souveränität als „*die Summe aller Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rollen in der digitalen Welt selbständig, selbstbestimmt und sicher ausüben zu können*“ (Goldacker 2017). Für die Verwaltung bedeutet in diesem Sinne die effektive Souveränität sowohl das Funktionieren im Inneren als auch die Integrität nach außen schützen zu können. Dafür stellt der Staat kritische Infrastrukturen bereit, welche für seine Souveränitätsausübung und Sicherung der Handlungsfähigkeit nötig sind. Dazu gehören unmittelbar zum Beispiel Militärinfrastrukturen, Verwaltungssysteme, medizinische Versorgung und Kommunikationsnetze. Daneben ist er in seinem Funktionieren von zahlreichen Infrastrukturanbietern abhängig, über welche er mittelbare Kontrolle ausüben können muss. Dazu gehören zum Beispiel Verkehrs-, Kommunikations- und Energienetze.

Diese Bereiche waren bisher durch die territoriale Souveränität eines Staates mitgeschützt und konnten autonom innerhalb des Staatsgebietes gesichert werden. Dieser inklusive Schutz ist in einer digitalen Umwelt aufgrund der „Grenzenlosigkeit“ digitaler Technologie nicht mehr gegeben. Einerseits gibt es im virtuellen Raum praktisch keine Grenzen mehr, deren „Überschreitung“ außer mit massiven Eingriffen verunmöglicht werden könnte (wie etwa im Iran oder in China). Andererseits ermöglicht es der virtuelle Raum, ohne Überschreitung von Grenzen in der realen Welt einzudringen, also Handlungen aus der sicheren Ferne zu setzen.

Diese Diskussion um eine neugedachte digitale Souveränität beeinflusst derzeit die Diskussion über die Aufgabentrennung zwischen Wirtschaft und Staat. Die Palette der Reaktionen reicht vom Ignorieren potentieller Gefahren bis zur versuchten Herstellung von Autarkie im IT-Infrastrukturbereich – im Speziellen der ausschließlichen Nutzung von im Land erzeugten IT-Komponenten, unabhängig von deren Qualität und Kosten. In einer globalen Interaktion ist dieser Weg der Autarkie und Isolation kaum möglich. Um aber die Selbstbestimmtheit effektiv ausüben zu können, wurden unter anderem folgende Maßnahmen vorgeschlagen (Goldacker 2017; BITKOM 2015).

Transparenz der Instrumente/Open-Source-Software (Quell-Offenheit): Proprietäre Software (dies inkludiert auch Maschinensprache und Software auf einer tiefen Ebene) ist nicht einsichtig und nachvollziehbar. Open-Source-Umgebungen, sofern sie auf einer Vielzahl von unabhängigen KontributorInnen beruhen, zeigen Eigenschaften, die den meisten proprietären Entwicklungen abgehen, insbesondere: eine agile, rasche Integration von neuen Entwicklungen, transparente Algorithmen, intensives Review und Testing durch die Community, was zu einer sehr raschen Fehler- oder Malware-Entdeckung im Code führt, sowie agile Fehlerbehebung durch große Communities. Diese Eigenschaften erhöhen sowohl die Betriebssicherheit als auch die Vertrauenswürdigkeit des Softwarecodes. Ein allfälliger Spionage- oder Schadcode würde durch die hohe Anzahl unabhängiger, weltweit verteilter ReviewerInnen und EntwicklerInnen rasch aufgedeckt. Dieses Transparenzgebot führt neben handfesten wirtschaftlichen Argumenten (insb. Unabhängigkeit) zu einer zunehmenden Bevorzugung von Open-Source-Software in der Verwaltung (Köchler 2016).

*Standards und Schnittstellen: S*ichere und offene Standards regeln die Interaktion zwischen den unterschiedlichen Anwendungen und ermöglichen den Wechsel von Anbietern. Verschlüsselung und andere Sicherheitsfeatures, welche in Standards eingebettet sind, bestimmen den am Markt verfügbaren Schutzgrad, um das Gesamtrisiko und die Fortpflanzung der Risiken innerhalb des Systems zu managen. Aufgrund der Relevanz und Verbreitung dieser Standards

spielen in diesem Feld Lobbys und Geheimdienste eine große Rolle, was wiederum die Stärke der staatlichen Souveränität beeinflusst, sich gegen Ausspähung und Beeinflussung zu wehren. So eröffnete etwa die schwache Verschlüsselung des Europäischen Telekommunikationsstandards und die Definition einer Abhörschnittstelle (Zarzer 2001) ein Einfallstor für den massenhaften Abgriff und das Mitlesen von Geheimdiensten und Polizei (Greenwald 2014). Die qualifizierte Mitarbeit in Standardisierungsgremien und eine klar definierte Security-Agenda mit hohen, transparenten Verschlüsselungsstandards ist demnach wesentlich für die digitale Souveränität eines Staates.

Technologiebeherrschung: Aufgrund der raschen technologischen Entwicklung in den Bereichen Künstliche Intelligenz, Softwareentwicklung und moderner IT-Infrastrukturen sind für einen sicheren und risikobewussten Umgang neue Fähigkeiten notwendig. Um die Konsequenzen von komplexen digitalen Steuerungssystemen, Automatisierungen, Big Data- und Künstliche-Intelligenz-Anwendungen verstehen und beherrschen zu können, sind umfangreiche technische und mathematische Kenntnisse erforderlich. Diese missionskritischen Knowhow-TrägerInnen müssen in der Verwaltung integriert sein. Ihre Aufgaben sind die Auswahl und Risikobewertung der einzusetzenden Instrumente, die Anpassung und Wartung der Software und digitalen Assets der Verwaltung sowie die Steuerung und sachgemäße Anwendung. Wo diese Voraussetzungen nicht gegeben sind, herrscht eine hohe Abhängigkeit von privatwirtschaftlich gewinnorientierten und anderen Zielen verpflichteten Akteuren, die nicht kontrolliert werden können. Damit ist in einem Krisenfall die selbständige Handlungsfähigkeit nicht mehr gegeben und die Souveränität der Verwaltung gefährdet. Wegen Knowhow- und Ressourcen-Engpässen innerhalb der Verwaltung wird die Implementierung und Abwicklung von kritischen Infrastrukturen ohne ausreichendes Wissen oft ausgelagert. Mangels Sachwissen werden Technologieentscheidungen vielfach auf Basis von persönlicher Risikominimierung und nach Firmen-Status und Größe des Anbieters getroffen. Dies und die Tendenz zu operativer Dringlichkeit bewirken einen Entscheidungsbias in Richtung großer internationaler IT-Anbieter, eine Bevorzugung von Komplettservices (Outsourcing, Cloud-Services), welche intransparent für die Verwaltung sind und hohe Abhängigkeiten schaffen. Damit kommt es in vielen Fällen auch zum Einsatz neuer Technologien wie maschinelles Lernen und Künstliche Intelligenz ohne Verständnis der Konsequenzen für die kritischen Infrastrukturen. Obwohl diese Gefährdungen gesehen werden (BITKOM 2018), gibt es außer dem Aufbau von Cyber-Defence-Einheiten noch wenig Änderung.

Offene Fragen zu den Anforderungen an kritische Infrastrukturen im digitalen Zeitalter:

- Welche Vorgaben und Maßnahmen im Bereich Transparenz gibt es bei internationaler Open-Source-Software?
- Wie hoch ist der Anteil der Nutzung von EU-geförderten Technologien im Verwaltungsumfeld?
- Welche verwaltungseigenen Kompetenzzentren sind nötig, um Wissen auf nationalem/internationalem Niveau zu bündeln?
- Welche transnationalen Verwaltungskooperationen können geschaffen werden, um Verwaltungslösungen und Technologiewissen aufzubauen?
- Welche Governance-Maßnahmen sind nötig, um die systemischen Gesamtrisiken aus kritischen Infrastrukturen für eine Gesellschaft langfristig zu senken (dies beinhaltet neben den Standards auch technologiespezifische Qualitätsvorgaben und Transparenzgebote)?
- Welche Standardisierungen sind für Österreichs Souveränität relevant und wie beteiligt sich Österreich daran?
- Wie wirken Standards auf Neuproduktentwicklungen und auf den österreichischen Wirtschaftsstandort?

3.3 Der Staat als Beschaffer digitaler Services

Das Nachfragevolumen der Verwaltungen gestaltet massiv technologische Entwicklungen und in Wechselwirkung damit die staatliche Souveränität. Abgesehen von den großen transnationalen Unternehmen hat kein anderer Akteur auf dem Markt eine so geballte Wirtschaftsmacht wie Staaten. Die Verantwortung, welche mit dieser Macht einhergeht, muss auch bewusst und zielorientiert wahrgenommen werden, da sie sonst in opportunistischen Einzelentscheidungen verpufft. Im Folgenden werden einige der Optionen im Bereich der Beschaffung beschrieben, mit der demokratische Staaten die Innovationsstärke und die Flexibilität der Märkte nutzen können, um die Digitalisierung souveränitätsfördernd voranzutreiben.

Stimulierung digitaler Kompetenz: Die technischen Richtlinien für Verwaltungsdigitalisierung sind innerhalb der Verwaltung nach Zweckmäßigkeit und den rechtlichen Vorgaben frei festlegbar. Aufgrund der strikten Beschaffungsregeln wirken technische Standardisierungsbemühungen in der Verwaltung sofort weiter. Damit können die genannten souveränitätsrelevanten Vorgaben umgesetzt werden. Vorgaben wie Open Source First, Privacy-by-Design, die Bevorzugung dezentraler Technologien sowie Verschlüsselungstechnologien können die Handlungssicherheit des Staates besser gewährleisten. Dies gilt insbesondere für die Beschaffung von Elementen kritischer Infrastruktur. Auch andere Ziele, zu denen sich der Staat verpflichtet hat, wie Klimaschutz- oder Nachhaltigkeitsziele der UNO, können durch strategischen Einkauf unterstützt werden. Durch diese Nachfrage können auch neue Produkte und Innovationen induziert werden, sodass das Angebot der Nachfrage folgt. Da viele Parteien mit der Verwaltung kommunizieren und deren digitale Services nutzen, haben diese Technologievorschriften und Schnittstellen- und Verschlüsselungsvorgaben eine über den Verwaltungssektor weit hinausgehende Wirkung.

Durch die öffentliche Beschaffung werden bestimmte Wirtschaftszweige stimuliert und es kann über Förderungen und laufende Dienstleistungen regionales Knowhow indirekt aufgebaut werden. Dieses regionale Knowhow erhöht den Zugriff auf eigene Ressourcen und erhöht die digitale Handlungsfähigkeit der Staaten beträchtlich. Ebenso wie eine FinTech-Start-Up-Szene hat sich auch eine GovTech-Start-Up-Szene entwickelt, welche sehr agil und mit modernster Technik auf Anforderungen reagieren und ihrerseits Vorschläge unterbreiten kann. Große Firmen haben die Kraft dieser Communities erkannt und betreiben einen intensiven Austausch mit Aufträgen und Geschäftsoptionen. Viele Themen mit sehr schnellen Innovationszyklen wie Security-Anforderungen, Open-Source-Transparenz und Agilität können von diesem weltweit vernetzten Ökosystemen besser bedient werden als von großen Konzernanbietern. Hier würde eine dedizierte, zielgerichtete Kommunikation, Betreuung und Beauftragung dieser Communities durch die Verwaltungen in Richtung Erhöhung der Souveränität wirken.

Wahlmöglichkeiten und Vendor-Abhängigkeit: In einem sich rasch entwickelnden digitalen Umfeld, in dem hohes Innovationstempo herrscht und noch keine dominante technologische Richtung sichtbar ist, ist die prinzipielle Möglichkeit des Wechsels von Lieferanten wesentlich. Durch die Beschaffung von proprietärer Software und geschlossenen Schnittstellen wird dies nahezu verunmöglicht (sog. Vendor-Lock-In).

Beispiele wie das europäische Joint-Venture Airbus zeigen, dass politische „Befreiungsschläge“ auch gegen scheinbar übermächtige Quasi-Monopole möglich sind. Die EU hat ehrgeizige Förderprogramme für innovative Softwareentwicklung aufgelegt, um Schlüsseltechnologien bereit zu stellen, wie zum Beispiel innerhalb der EU-Programme Horizon 2020[13] oder Future

[13] ec.europa.eu/programmes/horizon2020/en.

Trust[14]. Auch der länderübergreifende Austausch von bereits entwickelten Verwaltungs-Softwaremodulen hilft ein eigenständiges Gegengewicht zu proprietären Entwicklungen zu schaffen.

Bisher wurde der Einkauf zentral ausgerichtet, um Mengen- und Preisvorteile zu erreichen. In der Privatwirtschaft ist man von einer derartigen nicht strategischen Betrachtungsweise abgerückt, da durch diesen engen Fokus die Interessen der Käuferseite nicht berücksichtigt werden: Insbesondere kann es zum beschriebenen Vendor-Lock-In kommen, man partizipiert nicht an der Innovation und es kommt zu keinen übergreifenden Kooperationen im relevanten Umfeld. Durch die Aufnahme dieser Ziele in die Vorgaben der Beschaffungsinstitutionen können diese einen raschen und wirksamen Beitrag zur digitalen Souveränität des Staates leisten.

Offene Fragen zur Beschaffung digitaler Services:

- Welche Auswirkungen haben demografische Entwicklungen und Ausbildungsprojektion auf das digitale Funktionieren des österreichischen Staates?
- Wie werden technologische Abhängigkeiten in (internationalen) Verhandlungen ausgenutzt?[15]
- Welche werden die zukünftigen Kerntechnologien in der Verwaltung sein?
- Was ist der Stand des Technologiewissens in der österreichischen Verwaltung?
- Welche Abhängigkeit besteht in der österreichischen Verwaltung von Hardware- und Software-Lieferanten und wie könnte dieser Abhängigkeit begegnet werden?

14 cordis.europa.eu/project/rcn/202698/factsheet/en.

15 Siehe aktuell den US-amerikanischen Druck gegen die Ausrüstung der eigenen Handelspartner mit chinesischer IT („Pompeo warnt vor Geschäften mit Huawei“ 11.02.2019, orf.at/stories/3111131/.

4 Digitale Souveränität und politischer Prozess

Der Staat ist nicht nur eine „Verwaltungsmaschine“, sondern zuvorderst auch ein Raum der politischen Aushandlung dessen, wie das Gemeinwesen nach innen und außen agieren soll, also eine politische und regulierende Infrastruktur. Nicht nur weil sich, wie eingangs erwähnt, der Staatsbegriff und damit auch das, was überhaupt innerhalb der Staatsgrenzen verhandelbar ist und verhandelt wird, in Zeiten der Globalisierung und Supranationalisierung entschieden verändert, sondern auch und gerade weil die allgegenwärtige und umfassende Digitalisierung neue Bedingungen schafft, ist selbst die politische Seite der Souveränität betroffen – also wie souverän im Sinne von selbstbestimmt und unbeeinflusst die politischen Prozesse ablaufen, mit anderen Worten: staatliche digitale Souveränität im Bereich der Politik. Da Politik in der Demokratie auf gesellschaftliche Kommunikation und Aushandlungsprozesse angewiesen ist, spielen die sich rapide verändernden Informations- und Kommunikationstechnologien eine entscheidende Rolle bei der aktuellen und zukünftigen Gestaltung dieser Kernfunktion eines souveränen Staates.

4.1 Staatspolitische digitale Souveränität

Während es ein ganz offensichtliches Interesse der BürgerInnen gibt, selbst nicht überwacht zu werden, ist die Position des Staates in dieser Hinsicht gespalten: Einerseits hat er das Interesse, selbst nicht von fremden Mächten (ausländischen Geheimdiensten, Unternehmen, organisierter Kriminalität/Terroristen usw.) überwacht zu werden, weil das seine eigene Souveränität einschränken würde. Andererseits hat der Staat ein Interesse an Überwachung, um bestimmte Staatsaufgaben zu erfüllen, insbesondere im Interesse der inneren und äußeren Sicherheit und Verbrechensbekämpfung. Während sich also der Staat bemüht, möglichst unverwundbar gegen Spionage zu sein, indem Cybersicherheit höchste Priorität hat, hat er zugleich ein Interesse, sich nicht jener Mittel zu begeben, die ihm generell oder im Anlassfall die Möglichkeit eröffnen, selbst überwachend tätig zu werden. Spätestens seit den Snowden-Enthüllungen ist offensichtlich, dass einige Staaten die digitale Souveränität von Individuen und Unternehmen zum Zwecke der Erhaltung der Souveränität des Staates sowie darüber hinaus der Durchsetzung ihrer nationalen und internationalen Interessen massiv verletzen.

Dies wird zum Teil mit einer sozusagen höherwertigen, übergeordneten Souveränität des Staates gegenüber jener der Individuen argumentiert. Ähnlich wie in vielen anderen Staaten, gibt es auch in Österreich etwa im Telekommunikationssektor, gesetzlich abgesichert, sogenannte Backdoors, also elektronische Hintertüren für eine „Lawful Interception“, um die Kommunikation abzuhören oder Bewegungsprofile festzustellen (Zarzer 2001; Moechel 2001). Auch über staatliche Trojaner, die legal auf private Computer übertragen werden, um die über diese Geräte laufende Internetkommunikation abzugreifen, wird öffentlich nachgedacht und diese seit 2018 sind jene auch in Österreich zulässig – (Al-Ani/Stenzel 2018). Ganz zu schweigen von nicht-demokratischen, autoritären Regimen, unter denen über staatliche Backdoors nicht einmal öffentlich diskutiert wird.

Technologische Vorkehrungen wie Staatstrojaner, das Verbot von starker Verschlüsselung sowie Gesetze und enorme Ressourcen, um die weltweite Kommunikation abzugreifen, machen deutlich, dass die digitale Souveränität des Einzelnen hinter der des Staates zurückgestellt wird Ob das legitim ist, ist seit Jahren Gegenstand intensiver Debatten. Ein zentrales Ergebnis

des europäischen Technikfolgenabschätzungsprojekts SurPrise[16], das auch auf breit angelegter BürgerInnenpartizipation fußte, ist, dass der Trade-off Sicherheit versus Überwachung nicht allgemein akzeptiert wird. Was sich BürgerInnen in dem Zusammenhang erwarten, sind Lösungen, die sowohl staatliche als auch individuelle Sicherheitsbedürfnisse befriedigen, während die Grundrechte gewahrt werden. BürgerInnen haben unter bestimmten Voraussetzungen Verständnis für den Einsatz von Überwachungstechnologien, aber nicht in der Art und Weise, wie es bisher oft geschehen ist. Aus deren Sicht sollten Überwachungstechnologien u. a. zielgerichtet und effektiv sein, von kompetenten und vertrauenswürdigen Personen eingesetzt werden und ganz klar gegen Kriminelle gerichtet sein. Was abgelehnt wird, sind Überwachungsmaßnahmen ohne Anfangsverdacht gegen die gesamte Bevölkerung sowie Maßnahmen, die Menschen neuen Risiken aussetzen oder zu intrusiv bzw. die Privatsphäre verletzend sind. Besonders in Österreich machen sich die BürgerInnen große Sorgen um die Missbrauchspotentiale, die aus mangelnder Zweckbindung und Kontrolle entstehen (Strauß 2017).

Die Wahrung der digitalen Sicherheitsinteressen des Staates, welches eine wesentliche Legitimation des Gewaltmonopols darstellt, umfasst zwei Ebenen, nämlich die Sicherheit gegen äußere Aggressoren und gegen innere Umsturzversuche. In der Cybersphäre sind diese beiden Ebenen freilich untrennbar miteinander verbunden und nicht zu trennen.

Digitale Sicherheit gegen äußere Aggressoren: Auf militärischer Ebene setzen auch die Streitkräfte auf die Vorteile von Plattformen wie z. B. die Netzwerkeffekte als Basis der Einbindung von externen Informationen, aber auch von Personen und Dienstleistungen (Al-Ani/Stenzel 2018). Alleine diese Öffnung der militärischen Infrastruktur zeigt, dass eine rigide Begrenzung der „Kombattanten" in einer Plattform-dominierten Welt nicht möglich ist. Es entsteht eine dauernde Wechselwirkung, Abhängigkeit und gegenseitige Durchdringung mit zivilen, globalen Plattformen. Diese Wechselwirkung wird nötig, um das Funktionieren einer gesamtheitlichen Verteidigung, inklusive physischer Assets zu gewährleisten. Gleichzeitig setzt das Militär, einschließlich des österreichischen Bundesheers, auch vermehrt auf Eigenentwicklungen in der IT, um sich eben nicht in die Abhängigkeit von Drittanbietern zu begeben.

Die Führung eines „Cyberwars", also sowohl aggressive, aber vor allem auch defensive Maßnahmen im Cyberspace als Kriegshandlungen, hat sich in den letzten Jahren zu einem in manchen Ländern den physischen Streitkräften ebenbürtigen Schauplatz entwickelt (Kurz/Rieger 2018). Auch in Österreich gibt es mittlerweile mehrere Stellen, die für Cyber-Defence zuständig sind. Neben den nachrichtendienstlichen Aufgaben, die Kompetenzen im Heeresabwehramt bündeln, gibt es im Kommando „Führungsunterstützung und Cyber-Defence" des Bundesheeres eine zuständige Organisation.[17] Da das Bundesheer für die Landesverteidigung zuständig ist, werden Zwischenfälle, die nicht als Angriff einzustufen sind, vom Bundesministerium für Inneres bearbeitet, wo ebenfalls Kompetenzen in dem Bereich vorhanden sind.[18]

Dadurch, dass digitale Kriegsführung die Infiltration der potentiellen gegnerischen Plattformen bereits in Friedenszeiten bedingt, gibt es praktisch keinen digitalen Frieden. Weiters werden durch asymmetrische Kriegsführung nicht-staatliche Kombattanten auf den Plan gerufen. Diese nutzen globale zivile Kommunikationsinfrastrukturen unabhängig von Staatszugehörigkeiten und bauen ihrerseits Netze im zivilen Umfeld auf.

16 Projektwebsite: surprise-project.eu.

17 bundesheer.at/sk/cyber/index.shtml.

18 onlinesicherheit.gv.at.

Sicherheit gegen innere Aggressoren: Zu den inneren Aggressoren zählen BürgerInnen, die die Regierung stürzen oder die Macht des Staates auf andere Weise gewaltsam untergraben wollen, das organisierte Verbrechen sowie Personen innerhalb der staatlichen Verwaltung, die auf Grund von Erpressung oder Bereicherungsabsichten Daten missbräuchlich verwenden, verändern oder weitergeben. Potenziell bedienen sich diese inneren Aggressoren derselben Mittel wie die äußeren. Diese Faktoren machen die Identifizierung von Sicherheitsbedrohungen schwierig und führen zur Forderung nach lückenloser Massenüberwachung. Die derzeitige Massenüberwachung bindet alle bestehenden Plattformen ein. So nutzt die Geheimdienst-Plattform der NSA Daten und Algorithmen von zivilen Plattformen wie Facebook, Google, Microsoft und anderen (Greenwald, 2014).[19] Die nationale Gesetzgebung gibt diesen Anforderungen im Regelfall nach und schafft so eine staatenübergreifende Überwachungsplattform.

Dieses gemeinsame digitale „Überwachungsinteresse" von globalen Privatfirmen und der nationalen Geheimdienste/Militärs in verschwimmenden Plattformen unterminiert die Position des Staates als Wahrer der Digitalen Rechte des Individuums. Im politischen Prozess muss daher eine informierte, problembewusste Gesellschaft eine Abwägung zwischen Freiheits- und Sicherheitsinteressen treffen, soweit dieser Widerspruch nicht nur scheinbar ist (Pavone et al. 2015), um nicht in eine totale Überwachungsgesellschaft abzudriften (Zuboff 2018).

Dieses Dilemma ist nicht einfach aufzulösen, zumal in demokratischen Staaten beide Souveränitätsansprüche gegeneinander abgewogen werden müssen. Selbst wenn diese Abwägung zu Gunsten der Staatssouveränität ausgehen sollte, ist es nach unserer Einschätzung dennoch die Aufgabe des Staates, die digitale Souveränität seiner BürgerInnen im verbleibenden Spielraum soweit wie möglich zu fördern. In einer Demokratie sind selbstbestimmt entscheidende BürgerInnen eine *conditio sine qua non*. Deshalb gibt es Grundrechte, die das sicherstellen sollen. Jede Aushöhlung der Grundrechte ist auch eine Unterminierung der demokratischen Grundfesten des Staates. Daher hat der Staat seine BürgerInnen gegenüber anderen Individuen, dem organisierten Verbrechertum und Terrorismus wie auch gegenüber anderen Staaten bestmöglich zu verteidigen. Genaugenommen zählt es auch zu den Aufgaben des Staates, dafür Sorge zu tragen, dass er selbst nur in dem zur Wahrung seiner eigenen Souveränität erforderlichen Ausmaß, das heißt nicht überschießend, die Souveränität seiner BürgerInnen beschränkt.

Offene Fragen zur staatlichen digitalen Souveränität:

- Wie könnten legistische Maßnahmen, etwa im Bereich Datenschutz, den Interessensausgleich zwischen staatlicher und individueller digitaler Souveränität herstellen? Welche Umgehungsmaßnahmen wurden bereits festgestellt?
- Welche Ressourcen der Datenschutzbehörden sind zur effektiven Durchsetzung notwendig?
- Können sogenannte Gegenplattformen unter den Rahmenbedingungen: mit den gleichen Daten ausgestattet (Open Data), Zugang zu offenen Algorithmen habend (Open Source) und auf sicherem rechtlichen Boden stehend, ein Gleichgewicht schaffen?
- Welche Rolle kann staatliche Regulierung bei der Gewährleistung der digitalen Souveränität spielen? In welcher Weise kann (regionale) internationale Kooperation, supranationale oder völkerrechtliche Rechtsetzung ein neues Modell (digitaler) staatlicher Souveränität schaffen, das unter den Bedingungen der weltweiten Digitalisierung ein neues, faires Gleichgewicht schafft?

[19] „Internetkonzerne als Kollaborateure von Militärs und Diktaturen", fm4.orf.at/stories/2928880/.

4.2 Elektronische Wahlen und Beteiligung

In Österreich spielen elektronische Wahlen, anders als in einigen anderen Ländern, allen voran Estland, bislang keine große Rolle.[20] Angesichts der Durchdringung von immer mehr Lebensbereichen mit digitalen Services, auch und gerade im Staatsbereich, steht jedoch zu erwarten, dass der Wunsch nach elektronischen Wahlen langfristig dazu führen wird, dass auch in Österreich (wieder) über dieses Thema debattiert werden wird.

Potenziell ist die (teil-)elektronische Abwicklung von Wahlen und Abstimmungen ein großes Thema unter dem Gesichtspunt der digitalen Souveränität. Die dafür notwendige Infrastruktur muss höchsten technischen Standards entsprechen. Es gibt freilich international einige Beispiele, insbesondere aus den USA, für die Manipulierbarkeit von elektronischen Wahlmaschinen (Schwartz 2018). Findet das E-Voting über das Internet statt, potenzieren sich die möglichen Angriffspunkte. Weiters stellen sich, mehr noch als bei der Briefwahl, Herausforderungen für die Sicherstellung der „freien und unbeeinflussten Stimmabgabe“, da diese nunmehr mobil über das Smartphone und damit in praktisch jeder Umgebung und von einem unsicheren Gerät aus erfolgen kann. Jedenfalls müsste der Staat eine manipulations- und ausfallsichere Infrastruktur für Wahlen zur Verfügung stellen, was keineswegs einfach ist.

Darüber hinaus stellen sich spezielle Fragen der staatlichen Souveränität bei der Beteiligung an elektronischen Wahlen nicht nur von StaatsbürgerInnen im Ausland, sondern sogar Fremden, wie das etwa in Estland der Fall ist. Staatsangehörigkeit gerät auch angesichts eines anderen Phänomens unter Druck: Die Beobachtung globaler Kommunikationen, etwa durch den US-Geheimdienst NSA, betrifft nicht nur die eigenen StaatsbürgerInnen, sondern basiert auf der algorithmischen Auswertung von Kommunikationsdaten, was Cheney-Lippolds als „ius algoritmi“ bezeichnet (Cheney-Lippolds 2018).

Angesichts der eingesetzten staatlichen Ressourcen wäre es denkbar, diese Wahlinfrastruktur nicht unbedingt nur für demokratische Wahlen auf den verschiedenen Ebenen des Staates, sondern auch für Abstimmungen in der Zivilgesellschaft, in Vereinen, Unternehmen usw. zur Verfügung zu stellen. Schließlich muss auch die Partizipationsinfrastruktur, die für elektronische Petitionen, Begutachtungsverfahren, Umfragen, Informations- und Kommentierungsprozesse auf allen staatlichen Ebenen aufgebaut wird, denselben Standards wie jener bei Wahlen genügen, um Manipulationen hintanzuhalten.

BürgerInnenbeteiligung hätte, so sie entsprechend gestaltet ist, das Potenzial, das Vertrauen in den Staat und damit eine Stärkung der (digitalen) Souveränität zu fördern.

Offene Fragen zu elektronischer Beteiligung:

- Wie müssten elektronische Wahlen gestaltet sein, um sie gleich sicher wie analoge Wahlen durchzuführen?
- Soll Österreich und, wenn ja, wie, auch eine Infrastruktur für elektronische Wahlen anbieten?
- Soll der Staat eine Infrastruktur für elektronische Wahlen und Beteiligungsprozesse auch für die Zivilgesellschaft zur Verfügung stellen?

[20] Unseres Wissens wurde in Österreich nur einmal bei einer gesetzlichen Wahl mit E-Voting experimentiert und zwar bei den Wahlen zur Hochschülerschaft im Jahre 2009, Der Standard 19.05.2017, derstandard.at/2000057975328/OeH-Wahl-Skepsis-bei-E-Voting.

4.3 Manipulation der öffentlichen Meinung

Beeinflussung der öffentlichen Meinung war schon immer zentral für den politischen Prozess. Im positiven Sinne kann dies durch Überzeugungsarbeit geschehen, in negativen durch unlautere Manipulation. Im 21. Jahrhundert kamen insbesondere mit dem Web 2.0. also den Sozialen Medien, neue Möglichkeiten der Manipulation hinzu, die wir plakativ unter „Manipulation 2.0" fassen. Im Anschluss erörtern wir Strategien gegen diese neuartigen Manipulationsmöglichkeiten.

4.3.1 Manipulation 2.0

Elektronisch oder analog, Wahlergebnisse können auch ohne Beeinflussung der technischen oder physischen Stimmabgabe manipuliert werden. Unter dem Begriff „Computational Propaganda" versteht man Programme und Algorithmen, die die Manipulation der öffentlichen Meinung zum Ziel haben. Auf Basis von Big Data erstellen, verbreiten und vervielfältigen autonome Agenten politische Botschaften über Social Media vielfach mit dem Ziel, Unzufriedenheit zu säen, Unsicherheit zu schüren und Opposition außer Gefecht zu setzen (Woolley/Howard 2017). Oft werden dafür Social Bots herangezogen, also automatisierte Social-Media-Accounts, die menschliches Verhalten imitieren und mit NutzerInnen in sozialen Netzwerken interagieren, gewöhnlich ohne ihren nicht-menschlichen Charakter zu enthüllen (ITA 2018). In einer groß angelegten internationalen Studie der Universität Oxford mit dem Titel „The Computational Propaganda Project"[21] wird die Manipulation der öffentlichen Meinung unter Nutzung von Social Media in neun Ländern untersucht (Woolley/Howard 2017). Ziel solcher Desinformationsinitiativen ist es laut Howard meist, durch verschiedene, auch widersprüchliche Aussagen, Konfusion in Debatten zu bringen. Ähnliche Strategien wurden inzwischen auf WählerInnen westlicher demokratischer Systeme angewendet, in weiterer Folge auch von PolitikerInnen in westlichen Demokratien selbst.

Untrennbar ist mit den Aktivitäten auch der Begriff „Fake News" verbunden, also bewusst verfälschte manipulative Nachrichten, die mehr oder weniger glaubwürdig die öffentliche Meinung beeinflussen oder irritieren sollen (Brodnig 2017). Nicht zu unterschätzen sind neue Technologien, die das beschriebene Problem verstärken und die gesamte politische Debatte und Glaubwürdigkeit auf den Kopf stellen könnten: Als „Deep Fake" werden heute schon mithilfe von Künstlicher Intelligenz täuschend echte Fälschungen von Bildern und vor allem Videos produziert (Gudowsky 2018). Die zugrundeliegenden Technologien sind kostenlos erhältlich und einfach zu bedienen. Damit ist es potenziell beispielsweise möglich, einem Politiker am Abend vor einer Wahl eine von der Bevölkerung als Skandal empfundene Aussage in den Mund zu legen.

Die genannte Oxford-Studie befasst sich intensiv mit der Beeinflussung der öffentlichen Meinung in verschiedenen Ländern und ergab unter anderem, dass Bots nicht nur nachweislich mit dem Ziel eingesetzt wurden, die Ergebnisse der US-Präsidentschaftswahl zu beeinflussen, sondern dieses Ziel auch erreichten. Insbesondere die sogenannten sozialen Medien werden für Irritation und Manipulation der öffentlichen Meinung genutzt, sei es zur Durchsetzung politischer Interessen Außenstehender oder PolitikerInnen des betroffenen Landes selbst. So gilt die Beeinflussung des US-Präsidentschaftswahlkampfs 2016 durch russische Hacker und Bots aus Sicht von US-Geheimdiensten als erwiesen. Die Firma Cambridge Analytica hat im Auf-

[21] comprop.oii.ox.ac.uk.

trag von Präsidentschaftskandidaten nachweislich in den US-Wahlkampf eingegriffen und dabei NutzerInnendaten von Facebook und Twitter verwendet. Die Ermittlungen des US-Sonderermittlers Mueller ergaben, dass nach Kontakten des Wahlkampfteams von US-Präsident Trump mit Russland mehrere damit zusammenhängende Aktivitäten erfolgten.[22] Eine sog. Trollfabrik in Sankt Petersburg überflutete Twitter und Facebook mit Hassbotschaften und es wurden Facebook-Anzeigen in großem Ausmaß gekauft, mit dem „strategischen Ziel, Zwietracht im politischen System der USA zu säen" (Scheuermann 2018). Darüber hinaus hackte der russische Militärgeheimdienst GRU die E-Mail-Server der Demokraten, die dabei ausspionierten Informationen wurden später zu den schärfsten Waffen im Wahlkampf Donald Trumps wurden.

Doch nicht nur in den USA, auch in Europa gibt es deutliche Hinweise auf Manipulation der öffentlichen Meinung, etwa bei der Volksabstimmung zum Austritt Großbritanniens aus der Europäischen Union oder den letzten französischen Wahlen (Brodnig 2017, S. 120ff.). Auch in Österreich wurden während des letzten Nationalratswahlkampfs Internetaktivitäten bekannt, die auf die bewusste Manipulation der öffentlichen Meinung abzielten.[23] In einer Studie zur deutschen Bundestagswahl 2017 wurden zwar keine substanziellen Bot-Aktivitäten auf Twitter nachgewiesen, allerdings wurden dennoch rund 20 Prozent aller politischen Nachrichten als Fake oder Junk News identifiziert (Neudert 2017).

Auch wenn sich die Aktualität in Österreich und Deutschland bislang weniger brisant zeigt als in anderen Ländern, hat sich Deutschland dennoch als einer der Vorreiter im Kampf gegen Computational Propaganda etabliert. Die deutsche Regierung ergriff mehrere Maßnahmen. So wurde im Juni 2017 das Netzwerkdurchsetzungsgesetz (NetzDG 2017)[24] beschlossen, das sich gegen Hetze und Fake News in sozialen Netzwerken richtet. Darüber hinaus war auf Druck der deutschen Regierung Deutschland nach den USA das zweite Land, in dem Facebook im April 2017 gemeinsam mit dem Recherchezentrum Correctiv verschiedene Instrumente zur Erkennung von Fake News einführte. Allerdings werden diesbezügliche Initiativen auch kritisiert, da sie Facebook in eine Rolle des Gatekeepers für Information und deren Wahrheitsgehalt machen. Dies kann sowohl als Übernahme staatlicher Aufgaben durch Privatunternehmen als auch als Wahrnehmung der Verantwortung klassischer Medien interpretiert werden. Auch am Netzwerkdurchsetzungsgesetz besteht insbesondere wegen einer potenziellen Einschränkung der Meinungsfreiheit Kritik, unter anderem von Reporter ohne Grenzen (Moßbrucker 2017) sowie vom UN-Sonderberichterstatter für Meinungsfreiheit David Kaye, der in einem offenen Brief Verstöße gegen die Menschenrechte sieht (Kaye 2017).

Oxford-Studienleiter Phil Howard sieht in konzertierten Angriffen auf Fakten durch Fake News eine der größten Herausforderungen für Wissenschaft, Demokratie und Aufklärung. Dies stellt laut Howard eine tiefe Gefahr für unsere Fähigkeit dar, Fakten zu verstehen, das Gemeingut zu bedenken und vernunftbasierte Wahlentscheidungen zu treffen oder Verwaltungstätigkeiten durchzuführen (Howard 2017).

Als Zwischenfazit lässt sich somit festhalten, dass neue technische Möglichkeiten (Social Bots, Fake News, Deep Fakes etc., insbesondere im Rahmen von Social Media) zu einer ernsthaften Gefahr für die digitale Souveränität des politischen Systems geworden sind.

---

22 The Guardian, 18.04.2019, What the Mueller report tells us about Trump, Russia and obstruction, theguardian.com/us-news/ng-interactive/2019/apr/18/mueller-report-trump-russia-key-takeaways.

23 Profil, 22.12.2017, profil.at/oesterreich/silberstein-affaere-rueckblick-8589591.

24 Bundesministerium der Justiz und für Verbraucherschutz Deutschland, Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG), 2017, gesetze-im-internet.de/netzdg/BJNR335210017.html.

4.3.2 Strategien zur Vermeidung von Manipulation

Welche Ansätze gibt es, den beschriebenen Herausforderungen entgegenzuwirken und damit die staatliche digitale Souveränität im Bereich der Politik sicherzustellen?

Eine oft propagierte Möglichkeit ist mehr Beteiligung der BürgerInnen, um diese besser in Entscheidungen einzubinden. Erfolgreiche Partizipation ist allerdings sehr voraussetzungsvoll, vor allem was die im Vorfeld von partizipativen Ereignissen, etwa Referenden, verfügbare Informationen betrifft (siehe das Beispiel der Brexit-Volksabstimmung).

Zur Verringerung des Einflusses von Fake News hat Phil Howard unter dem Namen „Restoring Trust in Social Media Civic Engagement"[25] unter anderem ein Projekt lanciert, das der Öffentlichkeit ermöglichen kann, verdächtige Social-Media-Accounts zu erkennen. In diesem Bereich gibt es auch zahlreiche Fact-Checking-Initiativen, die interessierte BürgerInnen in die Lage versetzen sollen, Fakten von Fake zu unterscheiden.[26] Darüber hinaus regt Howard an, destruktiven demokratiefeindlichen AktivistInnen mit den eigenen Waffen zu begegnen und Technologien wie Bots und Künstliche Intelligenz für die Verbreitung von „Good Speech" und Fakten einzusetzen. Individuen werden dazu aufgerufen, ihre Daten anonymisiert an WissenschafterInnen zu „spenden" (anstatt nur an Social-Media-Unternehmen), um daraus relevante Erkenntnisse ableiten zu können.

Die Komplexität von technologiegestützten Gegenmaßnahmen zeigt einerseits das Projekt „Conversation AI" der Google-Tochter Jigsaw.[27] Darin wurde versucht, ein Bullying-Score von 0 bis 100 für natürlichsprachliche Sätze zu entwickeln. Aufgrund zu vieler fehlerhafter Einschätzungen (false positives) kam die Lösung nicht zu einem operativen automatisierten Einsatz. Stattdessen wurde die Lösung als Unterstützung für reale Personen adaptiert. Ähnliche Erfahrungen machte Facebook, das der Masse an Hate-Speech- und Fake-News-Meldungen nicht mit Technologien Herr wurde und daher im Jänner 2018 die Beschäftigung von 10.000 MitarbeiterInnen bei der Zensur von Hate-Speech angekündigt hat.[28]

Dies macht offensichtlich, dass eine Analyse der Wirksamkeit der zahlreichen Initiativen erforderlich ist, um weitere Handlungsoptionen auszuarbeiten. Welche Rolle hat hier der Staat? Bislang sind die meisten Initiativen in diesem Bereich zivilgesellschaftlicher oder privater, kommerzieller Natur. Welche wirksame und nicht nur symbolische Regulierung ist denkbar? Ähnlich wie im Bereich der Beleidigungen im Netz unter dem Deckmantel der Anonymität (jüngst etwa der Fall Sigrid Maurer[29]), sind die rechtlichen Möglichkeiten, gegen Fake News und sonstige Manipulationen zum Schaden eines demokratischen Diskurses vorzugehen, noch sehr unterentwickelt (Brodnig 2017).

Viele Vorschläge, die in diesem Zusammenhang gemacht werden, richten sich an die Individuen als mündige KonsumentInnen von Nachrichten in den Sozialen Medien (z. B. Brodnig 2017, S. 187ff.). Aus unserer Sicht ist das zwar wichtig, jedoch ist der Staat selbst gefordert, Maßnahmen zu setzen, um die digitale Souveränität im Sinne von nicht manipulierten demokratischen Prozessen so weit wie möglich sicherzustellen.

---

25 oii.ox.ac.uk/research/projects/restoring-trust-in-social-media-civic-engagement/.

26 Z. B. mimikama.at, correctiv.org/echtjetzt/ oder faktenfinder.tagesschau.de/.

27 jigsaw.google.com/projects/.

28 Siehe z. B. Wiener Zeitung vom 23.01.2018 wienerzeitung.at/dossiers/netzpolitik/942815_10.000-neue-Leute-fuer-Kampf-gegen-Hetze.html.

29 Siehe z. B. Die Presse vom 09.10.2018 diepresse.com/home/panorama/wien/5510137/ExGruene-Sigrid-Maurer-wegen-uebler-Nachrede-schuldig-gesprochen.

Folgende Überlegungen könnten dabei eine Rolle spielen:

Wäre etwa eine aus demokratiepolitischen Überlegungen eingerichtete und mit ausreichenden Ressourcen ausgestattete öffentlich-rechtliche und unabhängige Fact-Checking-Plattform eine Lösung? Die bloße Existenz einer solchen Plattform reicht zwar nicht aus, um die Wirkung von Fake News auszugleichen, weil sie die ursprünglichen KonsumentInnen der Falschmeldungen nur zum Teil erreichen, wie man an zahlreichen Beispielen etwa in den USA erkennen kann. Dennoch könnte eine solche unabhängige Plattform präventiv wirken, auch wenn manche Menschen dem Staat grundsätzlich misstrauen oder Verschwörungstheorien anhängen. Jedenfalls müsste eine solche Plattform umsichtig gestaltet werden, um deren Legitimität bestmöglich und in den Augen der überwiegenden Mehrheit zu gewährleisten.

Felix Sühlmann-Faul und Stephan Rammler empfehlen in ihrer Untersuchung zu den Auswirkungen der Digitalisierung aus Nachhaltigkeitsperspektive zum Schutz und zur Erhaltung der Demokratie, dass der Staat (die Politik) die Sozialen Netzwerke aktiv nutzt, indem er einen „großen Stab an UserInnen aktiviert, die sich als Sprachrohr und Ansprechpartner der Politik beteiligen“ und gleichsam als „Gesandte“ fungieren, nicht aber versuchen, die Themenhoheit zu behalten. Außerdem raten sie zu massiven Investitionen in Institutionen zur Aufdeckung von Fake News und dafür, dass Angriffe auf die Demokratie im Netz reguliert werden müssen, da Rechtsdurchsetzung eine öffentliche Aufgabe ist (Sühlmann-Faul/Rammler 2018, S. 151ff.).

Aufgrund der begrenzten Reichweite von Anti-Fake-News-Plattformen, steht somit die staatliche Aufgabe im Raum, sich vor diesen Angriffen auf seine digitale Souveränität auch regulierend zu schützen. Ähnlich wie es Regeln gegen unlauteren Wettbewerb in der Wirtschaft gibt, Betrug unter Strafsanktion steht, und üble Nachrede geklagt werden kann, ist vorstellbar, auch den demokratischen Prozess über das bisher notwendige hinaus zu reglementieren. Es gibt genaue Vorschriften darüber, wie Wahlen formal abzulaufen haben, Wahlkampfkosten und Großspenden müssen transparent gemacht werden, in manchen Ländern ist Wahlwerbung kurz vor den Wahlen nicht mehr zulässig, usw. Es könnte überlegt werden, für demokratiepolitisch relevante Aktivitäten im Netz ebenfalls Regeln aufzustellen, die auch entsprechend sanktionsbewährt und damit präventiv wirken. So könnten etwa sog. Trollfabriken national verboten (und durch internationale Vereinbarungen geächtet) werden. Auch wenn nicht automatisch aufgrund der bloßen Existenz entsprechender Gesetze und Verträge Verstöße gegen diese verschwinden würden, könnte sich dennoch langfristig eine entsprechende demokratische Kultur auch im Netz einstellen, ähnlich wie sich in der Regel alle Wirtschaftssubjekte an die Regeln gegen unlauteren Wettbewerb halten (müssen). Die Grenzen solcher Regulierungen bestehen jedoch freilich auch darin, dass nicht alle Staaten demokratisch verfasst sind und überhaupt ein Interesse daran haben, sich dieses neuartigen Mittels der Ausübung von Souveränität (gegenüber anderen Staaten bzw. deren politischer Meinungsbildung, etwa in Hinblick auf Destabilisierung) zu begeben. Jedenfalls stellen sich bei der Formulierung solcher Regeln zweifellos gravierende verfassungsrechtliche Herausforderungen, muss doch gegen das Recht auf freie Meinungsäußerung abgewogen werden. Weiters ist auch die Möglichkeit der Verfolgung von Verstößen aufgrund von Anonymität und technischer Verschleierung des Ursprungs (und der Intentionen) eines Bruchs der digitalen Souveränität des Staates nicht trivial.

Darüber hinaus werden grundsätzlichere, technologische und systemische Ansätze diskutiert. So stellte der „Erfinder des Webs“ Tim Berners-Lee im August 2018 sein mit ExpertInnen des MIT entwickeltes Projekt Solid vor, mit dem er das Web technisch dezentralisieren und den NutzerInnen die Hoheit über ihre Daten zurückgeben will.[30] Im November 2018 folgte eine „Magna Charta für das Internet“. Darin werden neun, vorerst eher vage Prinzipien für ein neues

[30] solid.inrupt.com.

Internet festgehalten.[31] Zu den Unterstützern zählen auch Firmen wie Facebook und Google – Unternehmen, die mit für die aktuellen Entwicklungen verantwortlich sind, die Berners-Lee kritisiert. „*Wir brauchen einen neuen Vertrag für das Netz, mit klaren und harten Verantwortlichkeiten für jene, die die Macht besitzen, es zu verbessern*“, so Berners-Lee in einem Aufruf zu seiner Kampagne #ForTheWeb.[32]

Auch eine Schwerpunktausgabe der Technology Review des MIT vom September 2018 befasst sich mit dem Thema dieses Abschnitts und titelt „Technologie bedroht unsere Demokratie“. Um sie zu retten, schlägt Zeynep Tufekci, Professor an der University of North Carolina, verschiedene Maßnahmen vor, wobei nicht alle rein digitaler Natur sind. Einerseits sollte die Quasi-Monopol-Stellung weniger großer digitaler Unternehmen gebrochen und neue Regeln am digitalen Markt etabliert werden. Weiters sollte die allgegenwärtige Überwachung von NutzerInnen in Form massiver Datensammlungen beendet werden. Darüber hinaus sieht Tufekci allerdings die Politik als Ganzes gefordert, die realen sozialen, wirtschaftlichen und machtpolitischen Verhältnisse in den einzelnen Ländern zu verbessern, um zukünftige Finanzkrisen zu vermeiden, Ungleichheit zu minimieren und die Zufriedenheit der Bevölkerung zu erhöhen und so die Angriffsfläche auf demokratische Systeme zu minimieren (Tufekci 2018).

Die obige – nicht vollständige – Darstellung der bisherigen Vorschläge zeigt deutlich, dass bislang weniger konkret und lösungsorientiert gedacht wurde, als vielmehr das gravierende Problem der Demokratiegefährdung und damit der Souveränitätsschwächung identifiziert wurde.

Offene Fragen in Bezug auf die Vermeidung von Manipulation:

- Welche rechtlichen Möglichkeiten hat der Staat, jenen wachsenden Teil des demokratischen Prozesses, der sich in den Sozialen Medien abspielt, zu regulieren?
- Stellen öffentlich finanzierte Anti-Fake-News-Plattformen eine Lösung dar und wie könnten sie gestaltet werden?
- Wie könnte das Engagement des Staates in den Sozialen Medien zum Nutzen der Stärkung seiner digitalen Souveränität beitragen?
- Welche technischen und infrastrukturellen Maßnahmen sind zum Schutz gegen fremdgesteuerte, manipulative Angriffe auf den demokratischen Diskurs denkbar?
- Können digitale Partizipationsplattformen eine fakten- und vernunftorientierte öffentliche Meinung bzw. Entscheidung fördern? Und wenn ja, wie müssen diese gestaltet sein?
- Welche Bedrohungspotentiale ergeben sich durch digitale Plattformen für die souveräne, politisch eigenständige Meinungsbildung?

31 contractfortheweb.org.

32 webfoundation.org/2018/11/join-us-and-fight-fortheweb/.

5 Der Staat als Ermöglicher digitaler Souveränität seiner BürgerInnen

Während sich die vorangegangenen Kapitel auf den Staat bzw. das Gemeinwesen insgesamt, also auf die Verwaltung und die politischen Prozesse bezogen haben, fokussieren wir in diesem Kapitel auf die staatliche Rolle bei der Ermöglichung digitaler Souveränität der StaatsbürgerInnen. Wie bereits einleitend (Abschnitt 1) beschrieben, wird der Begriff der digitalen Souveränität vielfach ausschließlich auf den Fragenkomplex bezogen, wie denn der Einzelne digital souverän werden könnte. Wir haben jedoch nicht die individuelle Ebene im Blick, sondern das, was der Staat in diesem Bereich bewirken kann.

5.1 Regulierung der digitalen Selbstbestimmung

Ein ganz wesentliches Recht zur Erlangung digitaler Souveränität auf individueller Ebene ist die informationelle Selbstbestimmung. Hier wurde regulierungsseitig seit dem ersten Datenschutzgesetz in Umsetzung der Europäischen Menschenrechtskonvention (EMRK) den BürgerInnen ein Bündel an Rechten eingeräumt, die den Schutz der Privatsphäre garantieren sollen, sodass sie selbst über die Preisgabe und Verwendung ihrer personenbezogenen Daten bestimmen können. Diese Regeln gelten sowohl für Privatpersonen untereinander als auch gegenüber dem Staat. Dabei geht es nicht in erster Linie um die rechtliche Anpassung an die Dynamik der Entwicklung digitaler Dienste (wobei bisweilen erstere der technischen Entwicklung hinterherhinkt), sondern vor allem auch um die Durchsetzung bestehenden Rechts.

Das Funktionieren dieses Schutzes bzw. die Privatsphäre der Menschen in Österreich ist nicht nur für sie persönlich von großer Bedeutung, sondern auch für das Funktionieren der Demokratie in Österreich unerlässlich. Vom Schutz des eigenen Heims über den Artikel von Warren und Brandeis Ende des 19. Jahrhunderts (Warren/Brandeis 1890), die Charta der Menschenrechte, das Volkszählungsurteil 1983 in Deutschland bis hin zur aktuell gültigen Datenschutzgrundverordnung der EU (DSGVO) waren demokratische Staaten bemüht, sich mit dem Wesen der Privatsphäre auf unterschiedlichen Ebenen der Gesetzgebung, der Rechtsprechung und -durchsetzung auseinanderzusetzen und einen Schutzraum für ihre BürgerInnen bereitzustellen, der sie zu freien Individuen macht, die selbstbestimmt Entscheidungen treffen und ihre Vorstellungen von einem gelungenen Leben umsetzen können.

Gerade mit dem Einsetzen der Digitalisierung, also in einer Zeit, in der immer mehr Daten anfallen und Begehrlichkeiten daran von vielen Seiten erwachsen, muss der Staat besonders sorgfältig darauf achten, dass dieser Schutz gewahrt bleibt. Dabei kommt es nicht nur darauf an, die Gesetze zu vollziehen oder konkret die DSGVO in Österreich der Intention des europäischen Gesetzgebers folgend umzusetzen, sondern auch die damit betrauten Stellen mit den nötigen Ressourcen auszustatten und letztendlich Datenschutz auch zum Thema im gesellschaftlichen Diskurs zu machen. Auf all diesen Ebenen ist der Staat gefordert, seine BürgerInnen in dem Bestreben zu unterstützen, souverän in der Umbruchsphase der Digitalisierung zu bestehen.

Offene Fragen zur digitalen Selbstbestimmung:

- Ist die mit der Durchsetzung des Datenschutzes betraute Behörde mit ausreichenden Ressourcen ausgestattet?
- Wie könnten im österreichischen Recht Informationsfreiheit, Verwaltungstransparenz und Auskunftspflicht gestärkt werden, um die digitale Souveränität der BürgerInnen sicherzustellen?
- Welche internationalen Best-Practice-Beispiele gibt es in diesem Bereich?

5.2 Der Staat als Provider der digitalen Grundversorgung der BürgerInnen

Der Staat ist nicht nur Beschaffer (Abschnitt 3.3) jener digitalen Infrastrukturen, die er für die Durchführung seiner Kernaufgaben (insbesondere die Verwaltung des Gemeinwesens, als Provider kritischer Infrastrukturen und für den politischen Prozess) benötigt, sondern gestaltet durch Regulierung und sonstige Maßnahmen (Investitionen, Förderungen, Public-Private-Partnerships) auch die digitale Infrastruktur entscheidend mit, auf der seine BürgerInnen in der Verfolgung ihrer kommerziellen und privaten Interessen tätig werden. In der Tat ist der Staat teils selbst indirekt Betreiber solcher Infrastrukturen, etwa wenn staatliche Unternehmen oder öffentliche Einrichtungen diese betreiben (z. B. das Internet-Backbone ACONET für die Wissenschaft). In anderen Fällen tritt er als Marktregulator auf (z. B. im Bereich der Telekommunikation, die mittlerweile auch das Anbieten von Internetdienstleistungen einschließt) oder als Normsetzer, sei es direkt über Gesetze oder Verordnungen, sei es indirekt über Standards, die wiederum in der Regulierung anerkannt werden.

Ganz ähnlich wie bei sonstigen Infrastrukturen, etwa der Herstellung einer funktionierenden und sicheren Mobilitätsinfrastruktur oder Energieversorgung kann es als Staatsaufgabe angesehen werden, den BürgerInnen eine sichere, neutrale Netzwerkinfrastruktur zur Verfügung zu stellen. Damit wird der Rahmen geschaffen, innerhalb dessen BürgerInnen digital souverän agieren können. Der Staat kann diese Aufgaben entweder outsourcen und als Regulator kontrollieren oder selbst als Provider auftreten. Ein Beispiel für Letzteres war etwa Anfang der 2000er-Jahre der Versuch, eine digitale europäische Bibliothek als Gegenprojekt zur flächendeckenden Digitalisierung durch Google Books aufzubauen.[33]

Eine extreme Form der Regulierung zur Aufrechterhaltung bzw. Wiederherstellung der digitalen Souveränität (des Staates, aber auch seiner BürgerInnen) ist der Versuch der „Reterritorialisierung“. Dabei geht es darum, Teile der Datenströme, nämlich jene, die zwischen Knotenpunkten bzw. Individuen auf einem bestimmten Territorium stattfinden, entgegen der aktuellen Internetarchitektur innerhalb dieses Territoriums zu halten. Dies wird als sog. nationales oder Schengen-Routing (SNR) verhandelt und ist sowohl ökonomisch umstritten als auch technisch voraussetzungsvoll (ausführlich nachvollzogen in Pittroff et al. 2018). Russland verfolgt diese Strategie aus sicherheitspolitischem Interessen.[34]

---

[33] Das Projekt „The European Library“ ist mittlerweile wieder eingeschlafen und teilweise im Projekt „Europeana“ aufgegangen; die Website theeuropeanlibrary.org/tel4/ war im Februar 2019 noch online.

[34] RuNet – kapselt sich das russische Internet ab? de.euronews.com/2019/02/12/runet-das-russische-internet.

Einen anderen Aspekt betrifft die Diskussion um die Ermöglichung von Zugang zu digitalen Dienstleistungen. So kann die digitale Infrastruktur bzw. der Zugang zu dieser in vielen Bereichen bereits als von der Definition der Universaldienste umfasst begriffen werden, mit anderen Worten, der Staat hat hier einen Versorgungsauftrag, der durch Universaldienstverpflichtungen für die Provider, ähnlich wie beim Telefonnetz, umgesetzt werden könnte. Es könnte also eine Liste von Basistechnologien und Services/Anwendungen definiert werden, zu dem alle BürgerInnen jedenfalls, gegebenenfalls sogar gratis, Zugang haben sollen. Das könnten etwa Internetanbindungen im ganzen Staatsgebiet, abhörsichere Text-, Audio- und Videokommunikationskanäle oder sichere Cloud-Services umfassen. Angesichts der immer größer werdenden Bedeutung Sozialer Medien wäre auch eine Diskussion zu führen, ob und in welcher Weise diese zum Kanon der Basisdienste der digitalen Gesellschaft gehören sollten. In Hinblick auf die Aufrechterhaltung einer funktionierenden digitalen Demokratie (siehe Abschnitt 5.2) könnte der Staat nicht nur als Förderer einer unabhängigen Qualitätspresse und als Garant eines starken öffentlich-rechtlichen Segments in der Medienlandschaft auftreten, sondern auch als Provider oder zumindest Regulator einer unabhängigen Plattform zur Enttarnung von Falschmeldungen auftreten.

Eine besondere Aufgabe in diesem Zusammenhang wäre es, staatlicherseits dafür Sorge zu tragen, dass diese Infrastrukturen so aufgebaut und gewartet sind, dass die Kommunikation und Datenhaltung (revisions-)sicher und nicht manipulierbar ist, mit anderen Worten, dass die digitale Souveränität der BürgerInnen, also ihr Selbstbestimmungsrecht über die eigenen Daten, gewährleistet wird.

Offene Fragen zur digitalen Grundversorgung:

- Wie könnte eine konsumentInnenschutzrechtliche Regulierung von Geschäftsbedingungen der Internetdienste über den Datenschutz hinaus, z. B. in Hinblick auf Zugangsregelungen, aussehen?
- Welche Ausweitung der Universaldienstverpflichtung auf jene Dienste, die in der Informationsgesellschaft des 21. Jahrhunderts als unbedingt notwendig erachtet werden, damit sich alle BürgerInnen am zivilen und politischen Leben beteiligen können, sind nötig?
- Wo steht Österreich im internationalen Vergleich im finanziellen Engagement bei der Bereitstellung von Basisinfrastrukturen?

5.3 Aufgaben im Bildungswesen

Die meisten Beiträge zur digitalen Souveränität (siehe insbesondere die Beiträge in Friedrichsen/Bisa 2016) kommen zu dem Schluss, dass digitale Souveränität nichts Selbstverständliches ist, weder was die Rahmenbedingungen (technisch, regulatorisch, ökonomisch, kulturell) anlangt noch in Hinblick auf die Fähigkeiten der Individuen, diese Souveränität auch sozusagen „souverän“ wahrnehmen zu können. Dafür braucht es, wie die Erfahrungen der letzten Jahre mit einer in Bezug auf Privatsphäre und Sicherheit zunehmend gedankenlosen Internetnutzung deutlich gemacht haben, entsprechende Fähigkeiten und einen hohen Bewusstseinsstand, weil es in der Regel viel bequemer bzw. sozial erwünscht ist, die eigene digitale Souveränität zu vernachlässigen, um sich nicht sozial zu isolieren.

Der Staat wird zwar legitimerweise keinen direkten Einfluss darauf nehmen können und wollen, ob sich seine StaatsbürgerInnen digital souverän verhalten oder nicht, aber es ist in den Augen vieler seine vornehmliche Aufgabe, entsprechende Bildungsangebote sowohl in den

Schulen als auch in der Erwachsenenbildung zu machen, um potenziell den Bewusstseinsstand in dieser Hinsicht zu erhöhen ebenso wie die dafür notwendigen praktischen Fähigkeiten zu verbreiten. Diese Bildungsangebote, sollten über die Beherrschung von Software hinausgehen und allgemein einen souveränen Umgang mit Daten und Informationen – seien sie digital oder analog – zum Ziel haben (vgl. Sühlmann-Faul/Rammler 2018, S. 88ff.; Tauber 2016; Müller-Lietzkow 2016; Brodnig 2017, S. 187ff.).

Diese besondere Aufgabe des Staates kann auch mit einem Vergleich aus der Gesundheitspolitik untermauert werden: Der souveräne Umgang der/des einzelnen Bürgers/in ist, ähnlich wie etwa die Herstellung der regionalen Immunität gegen ansteckende Krankheiten durch lückenloses Impfen, nicht nur eine individuelle Frage, sondern hat auch eine gesellschaftliche Dimension, da achtloser Umgang mit dem Internet, sei es in Hinblick auf Sicherheit, sei es in Hinblick auf die Preisgabe von Daten, indirekt auch die KommunikationspartnerInnen und letztlich alle anderen BürgerInnen betrifft.

Offene Fragen zur digitalen Bildung:

- Wie kann der Wissensstand der Bevölkerung in Hinblick auf die Ausübung ihrer vom Staat geschützten digitalen Souveränität nachhaltig gehoben werden?
- Kann zusätzliche Regulierung im Bereich des Schutzes der Privatsphäre und der Daten dazu beitragen, dass sich ein Bewusstseinswandel in Richtung aktiver Wahrnehmung von (individueller) digitaler Souveränität vollzieht?

6 Fazit

Die Digitalisierung der Verwaltung ist im vollen Umfang sowohl im Bewusstsein der Politik, als auch in der Verwaltungspraxis angekommen. Dies zeigt die Einrichtung eines Ministeriums für Digitalisierung und Wirtschaftsstandort 2017. Zahlreiche punktuelle Kommunikationskanäle zwischen BürgerInnen und Verwaltung wie Apps, Chatbots sowie die Förderung von digitalen Start-ups sind geplant, doch fehlt eine gesellschaftspolitische, strategische Diskussion über die Auswirkungen einer digitalisierten Verwaltung bzw. des digitalen Staates im Allgemeinen. Dieser Artikel steckt einen Rahmen ab, der über die Automatisierung der Verwaltung, das sogenannte Plattform-Government in Konkurrenz zu globalen Plattformen und den Schutz kritischer Infrastrukturen bis hin zur digitalen Transformation der Demokratie selbst reicht.

Auch wenn, wie einleitend festgestellt, staatliche Souveränität nie absolut sein kann, weil sie notwendigerweise auf die Souveränitätsansprüche anderer Staaten trifft, konnte diese in vordigitalen und nicht-globalisierten Zeiten territorial zu einem hohen Maße unbeeinflusst ausgeübt werden. Dies hat sich im 21. Jahrhundert grundlegend geändert: Nicht nur sind mächtige nicht-staatliche Akteure hinzugetreten, die die Auswirkungen der territorialen Souveränität gekonnt umgehen können, sondern staatliche Grenzen spielen in der virtuellen Welt des internationalen Warenverkehrs, der globalen Dienstleistungen, der transnationalen Informationsbereitstellung und der ubiquitären und grenzenlosen Kommunikation eine immer kleinere Rolle. Wie sich in den letzten zwei Dekaden gezeigt hat, haben diese „Grenzenlosigkeit“ und damit der Verlust an souveräner Macht der einzelnen Staaten positive wie negative Folgen für seine BürgerInnen und Institutionen. Zu ersteren zählen etwa der nun auch für KonsumentInnen grenzenlose Marktplatz und der weltweite Zugang zu Informationen für alle. Zu letzteren gehört, dass die Potenziale der Staaten schwinden, für seinen prinzipiellen Machtbereich Regeln durchzusetzen und sich und seine BürgerInnen vor ungewollter Beeinflussung oder gar Unterwanderung zu schützen. Unser Beitrag hält keine Patentlösungen bereit; vielmehr war es unser Ziel, für diese große Herausforderung Bewusstsein zu schaffen, damit auf der politischen Ebene wichtige Debatten angestoßen werden und rasch zu entsprechenden Gegenmaßnahmen führen.

Dennoch ist die Antwort auf die im Titel gestellte Frage aus unserer Sicht ohne weitere Untersuchungen nicht zu geben. Vermutlich heißt die Antwort: Ja, es kann in gewissem Ausmaß eine digitale Souveränität Österreichs geben, aber ohne konsequentes Agieren auf verschiedenen Ebenen (national und international), sowohl in technischer und organisatorischer als auch in regulativer Hinsicht und nicht zuletzt im öffentlichen Diskurs könnte staatliche Souveränität im digitalen Zeitalter schon sehr bald ein Auslaufmodell sein. Ob die Strategie des „demokratischen Protektionismus“, also der „Versuch, territorial-nationale Logiken ins Zeitalter der Digitalvernetzung zu retten“ (Cheney-Lippolds 2018, S. 156) erfolgreich sein wird bzw. kann, bleibt eine offene Frage.

Die Setzung dieses Rahmens hat jedoch eine tiefe Bedeutung für die Zukunft unseres Zusammenlebens und wirft komplexe Fragen zu langfristigen Entscheidungen auf. Ein „Hineinstolpern“ ohne eine umfassende Digitalisierungsstrategie hieße, die Gestaltungsmacht abzugeben und zum Spielball der „First Mover“ zu werden. Punktuelle Maßnahmen ohne strategisches Gesamtkonzept könnten dazu führen, dass der Blick für das Ganze verloren geht, was beispielsweise zu Lock-ins oder kritischen Sicherheitslücken führen kann, aber auch dazu, dass das Vertrauen der Gesellschaft in die nachhaltige Sicherung der digitalen Souveränität verloren gehen kann. Die für diese Diskussion notwendige Faktenbasis und Ausarbeitung von Handlungsoptionen konnte hier nur angerissen werden, bedarf aber einer tiefergehenden Analyse

und Diskussion. Dieses Papier soll der Anstoß für eine öffentliche und wissenschaftliche Auseinandersetzung mit den gesellschaftlichen Implikationen sein. Aus Sicht der Autoren sollten als erster Schritt die offenen Fragen in den jeweiligen Abschnitten von den zuständigen Verwaltungseinheiten und ExpertInnen genauer beleuchtet und die jeweiligen Vorgehensweisen analysiert werden. Parallel dazu erscheint es uns essentiell, dass sich Politik und Zivilgesellschaft die aufgeworfenen Themen bewusst machen und eine umfassende Diskussion in Hinblick auf eine umsichtig überlegte, demokratisch gesteuerte digitale Souveränität führen.

7 Literatur

Al-Ani, A. und Stenzel, J., 2018, *Verteidigungsplattformen als Streitkräfte der Zukunft*; Webartikel; [Aufgerufen am: 22.12. 2018]; deutschland-und-die-welt-2030.de/de/beitrag/verteidigungsplattformen-als-streitkraefte-der-zukunft/.

Baums, A., 2016, Digitale Standortpolitik in der Post-Snowden-Welt, in: Friedrichsen, M. und Bisa, P.-J. (Hg.): *Digitale Souveränität. Vertrauen in die Netzwerkgesellschaft*, Wiesbaden: Springer, 223-236.

BITKOM, 2015, *Digitale Souveränität. Positionsbestimmung und erste Handlungsempfehlungen für Deutschland und Europa*, Berlin: Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.

BITKOM, 2018, Digitale Souveränität. Positionsbestimmung und erste Handlungsempfehlungen für Deutschland und Europa, *Datenschutz und Datensicherheit (5)*, 294-300.

Brodnig, I., 2017, *Lügen im Netz. Wie Fake News, Populisten und unkontrollierte Technik uns manipulieren*, Wien: Branstätter.

Buhr, L., Hammer, S. und Schlözel, H. (Hg.), 2018, *Staat, Internet und digitale Gouvernementalität*, Wiesbaden: Springer.

Cheney-Lippolds, J., 2018, Jus Algoritmi. Wie die National Security Agency die Staatsangehörigkeit neu erfand, in: Buhr, L., Hammer, S. und Schlözel, H. (Hg.): *Staat, Internet und digitale Gouvernementalität*, Wiesbaden: Springer, 211-238.

EPTA (European Parliamentary Technology Assessment), 2016, *The Future of Labour in the Digital Era. Ubiquitous Computing, Virtual Platforms, and Real-time Production*, Mai, Wien: ITA; epub.oeaw.ac.at/ita/ita-projektberichte/EPTA-2016-Digital-Labour.pdf.

Eubanks, V., 2018, *Automating Inequality: How High-tech Tools Profile, Police and Punish the Poor*, New York: St. Martins's Press.

Frey, C. B. und Osborne, M. A., 2013, *The Future of Employment: How Susceptible are jobs to compute-risation*, Oxford; oxfordmartin.ox.ac.uk/downloads/academic/The_Future_of_Employment.pdf.

Friedrichsen, M. und Bisa, P.-J. (Hg.), 2016, *Digitale Souveränität. Vertrauen in die Netzwerkgesellschaft*, Wiesbaden: Springer.

Goldacker, G., 2017, *Digitale Souveränität*, November, Berlin: Kompetenzzentrum Öffentliche IT, Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS.

Greenwald, G., 2014, *No place to hide – Edward Snowden, the NSA and the Surveillance State*, London: Penguin.

Gudowsky, N., 2018, Deepfakes – Perfekt gefälschte Bilder und Videos, in: Nentwich, M., Schaper-Rinkel, P., Capari, L., Gudowsky, N., Peissl, W. und Wasserbacher, D. (Hg.): *Foresight und Technikfolgenabschätzung: Monitoring von Zukunftsthemen für das Österreichische Parlament. Berichtsversion: November 2018*, Wien: ITA-AIT, 19-22; parlament.gv.at/ZUSD/PDF/FTA_03.pdf.

Howard, P., 2017, Accepting 2017 NDI Democracy Award on Behalf of the Oxford Internet Institut, *National Democratic Institute*, 3.11.; https://www.youtube.com/watch?v=Av0r9I8eeU4.

ITA, 2018, Manipulation in Sozialen Medien. ITA-Dossier Nr. 38 (Juli 2018; Autoren: David Heckenberg, Niklas Gudowsky), Wien; epub.oeaw.ac.at/ita/ita-dossiers/ita-dossier038.pdf.

Kamis, B., 2018, Europäisches Cyberrecht zwischen Schwert und Norm: Reifizierte Gewalt und Herrschaft im Kontext der postnationalen Gouvrenementalität, in: Buhr, L., Hammer, S. und Schlözel, H. (Hg.): *Staat, Internet und digitale Gouvernementalität*, Wiesbaden: Springer, 181-209.

Kaye, D., 2017, *Stellungnahme zum Regierungsentwurf des Gesetzes zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (NetzDG)*: Hochkommissariat für Menschenrechte der Vereinten Nationen; ohchr.org/Documents/Issues/Opinion/Legislation/OL-DEU-1-2017.pdf.

Kehl, D., Guo, P. und Kessler, S., 2017, *Algorithms in the Criminal Justice System: Assessing the Use of Risk Assessments in Sentencing. Responsive Communities*, July; cyber.harvard.edu/publications/2017/07/Algorithms.

Köchler, H., 2016, Souveränität, Recht und Demokratie versus Machtpolitik, in: Friedrichsen, M. und Bisa, P.-J. (Hg.): *Digitale Souveränität. Vertrauen in die Netzwerkgesellschaft*, Wiesbaden: Springer, 93-110.

Kurz, C. und Rieger, F., 2018, *Cyberwar. Die Gefahr aus dem Netz*, München: Bertelsmann.

Lee, F., 2017, Die AAA-Bürger, *Zeit Online*, 30.11.; zeit.de/digital/datenschutz/2017-11/china-social-credit-system-buergerbewertung.

Maciag, M., 2018, What Will Automation mean for Government-Jobs, *Blog GovTech.com* 4.1.; govtech.com/workforce/What-Will-Automation-Mean-for-Government-Jobs.html.

Mayer-Schönberger, V. und Ramge, T., 2017, *„Das Digital". Markt, Wertschöpfung und Gerechtigkeit im Datenkapitalismus*, Berlin: Econ Verlag.

Moechel, E., 2001, Die ETSI-Dossiers, *Telepolis*, 26.3.; heise.de/tp/features/Die-ETSI-Dossiers-3448017.html.

Moßbrucker, D., 2017, *Stellungnahme zum Regierungsentwurf des Gesetzes zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (NetzDG)*: Reporter ohne Grenzen e.V.

Müller-Lietzkow, J., 2016, Quo Vaids Digitale Bildung?, in: Friedrichsen, M. und Bisa, P.-J. (Hg.): *Digitale Souveränität. Vertrauen in die Netzwerkgesellschaft*, Wiesbaden: Springer, 305-324.

Münkler, H. und Straßenberger, G., 2016, *Politische Theorie und Ideengeschichte – eine Einführung*, München: Verlag C.H.Beck.

Neudert, L.-M. N., 2017, *Computational Propaganda in Germany: A Cautionary Tale*. Working Paper Nr. 2017.7, Oxford, UK: Project on Computational Propaganda; blogs.oii.ox.ac.uk/politicalbots/wp-content/uploads/sites/89/2017/06/Comprop-Germany.pdf.

O'Neil, C., 2017, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, London: Penguin.

O'Reilly, T., 2010, Government as a Plattform, in: Lathrop, D. und Ruma, L. (Hg.): *Open Government: Collaboration, Transparency, and Participation in Practice*: O'Reilly Media; mitpressjournals.org/doi/pdf/10.1162/INOV_a_00056.

Pasquale, F., 2018, Tech Platforms and the Knowledge Problem, *American Affairs II(2)*, 3ff.

Pavone, V., Degli-Esposti, S. und Santiago, E., 2015, *Key factors affecting public acceptance and acceptability of SOSTs, Deliverable D 2.4 of the EU project SurPrise*, im Auftrag von: Commission, E., January: SurPrise consortium; surprise-project.eu/wp-content/uploads/2015/02/SurPRISE-D24-Key-Factors-affecting-public-acceptance-and-acceptability-of-SOSTs-c.pdf.

Pittroff, F., Ochs, C., Lamla, J. und Büttner, B., 2018, Digitale Reterritorialisierung als politische Strategie. Die Reaktionsweisen der Demokratie in den Neuverhandlungen der Privatheit, in: Buhr, L., Hammer, S. und Schlözel, H. (Hg.): *Staat, Internet und digitale Gouvernementalität*, Wiesbaden: Springer, 141-165.

Plantera, F., 2018, The role of the state in a digital society; e-estonia.com/rethinking-the-role-of-the-state-in-a-digital-society/.

Scheuermann, C., 2018, Trump und die Russlandaffäre. Ein Skandal in Zeitlupe, *Der Spiegel*, 24.8.; spiegel.de/plus/donald-trump-und-die-russland-connection-ein-skandal-in-zeitlupe-a-00000000-0002-0001-0000-000159070547.

Schwartz, J., 2018, The Vulnerabilities of Our Voting Machines. When Americans go to the polls, will hackers unleash chaos?, *Scientific America (online)*, 1.11.; scientificamerican.com/article/the-vulnerabilities-of-our-voting-machines/.

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. und Peissl, W. (Hg.): *Surveillance, Privacy and Security. Citizens´ Perspectives*, Abingdon, Oxon; New York, NY: Routledge, 255-272.

Strauß, S. und Krieger-Lamina, J., 2017, *Digitaler Stillstand: Die Verletzlichkeit der digital vernetzten Gesellschaft – Kritische Infrastrukturen und Systemperspektiven. Projekt-Endbericht*, Nr. ITA 2017-01, 2017-03-31, Wien; epub.oeaw.ac.at/ita/ita-projektberichte/2017-01.pdf.

Sühlmann-Faul, F. und Rammler, S., 2018, *Der blinde Fleck der Digitalisierung. Wie sich Nachhaltigkeit und digitale Transformation in Einklang bringen lassen*, München: Oekom-Verlag.

Tate, R., 2010, The 6 delusions of Google's arrogant leaders, *Blog Business Insider;* businessinsider.com/the-6-delusions-of-googles-arrogant-leaders-2010-3?IR=T.

Tauber, P., 2016, 'Viel zu lernen du noch hast' – Medienkompetenz frei nach Yoda, in: Friedrichsen, M. und Bisa, P.-J. (Hg.): *Digitale Souveränität. Vertrauen in die Netzwerkgesellschaft*, Wiesbaden: Springer, 113-118.

Tufekci, Z., 2018, How social media took us from Tahrir Square to Donald Trump, *MIT Technology Review*, 14.8.; echnologyreview.com/s/611806/how-social-media-took-us-from-tahrir-square-to-donald-trump/.

Warren, S. D. und Brandeis, L. D., 1890, The Right to Privacy, *Harvard Law Review 4(5)*, 193-220; links.jstor.org/sici?sici=0017-811X%2818901215%294%3A5%3C193%3ATRTP%3E2.0.CO%3B2-C.

Woolley, S. C. und Howard, P. N., 2017, *Computational Propaganda Worldwide: Executive Summary*. Working paper Nr. 2017.11, Oxford: Project on Computational Propaganda; blogs.oii.ox.ac.uk/politicalbots/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf.

Zarzer, B., 2001, Österreich: Standardisierte Überwachung mit ETSI spätestens 2005, *Telepolis*, 15.12.; heise.de/tp/features/Oesterreich-Standardisierte-Ueberwachung-mit-ETSI-spaetestens-2005-3422963.html.

Zetter, K., 2014, An Unprecedented Look at Stuxnet, the World's First Digital Weapon, *Wired;* wired.com/2014/11/countdown-to-zero-day-stuxnet/.

Zuboff, S., 2016, Google as a Fortune Teller: The Secrets of Surveillance Capitalism, *FAZ*, 5.3.; faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshana-zuboff-secrets-of-surveillance-capitalism-14103616.html.

Zuboff, S., 2018, *Das Zeitalter des Überwachungskapitalismus*, Frankfurt: Campus.

Seit 2003 erschienene manu:scripte

ITA-03-01 Jörg Flecker und Sabine Kirschenhofer (01/2003): IT verleiht Flügel? Aktuelle Tendenzen der räumlichen Verlagerung von Arbeit. <www.oeaw.ac.at/ita/pdf/ita_03_01.pdf>

ITA-03-02 Gunther Tichy (11/2003): Die Risikogesellschaft – Ein vernachlässigtes Konzept in der europäischen Stagnationsdiskussion. <www.oeaw.ac.at/ita/pdf/ita_03_02.pdf>

ITA-03-03 Michael Nentwich (11/2003): Neue Kommunikationstechnologien und Wissenschaft – Veränderungspotentiale und Handlungsoptionen auf dem Weg zur Cyber-Wissenschaft. <www.oeaw.ac.at/ita/pdf/ita_03_03.pdf>

ITA-04-01 Gerd Schienstock (1/2004): Finnland auf dem Weg zur Wissensökonomie – Von Pfadabhängigkeit zu Pfadentwicklung. <www.oeaw.ac.at/ita/pdf/ita_04_01.pdf>

ITA-04-02 Gunther Tichy (6/2004): Technikfolgen-Abschätzung: Entscheidungshilfe in einer komplexen Welt. <www.oeaw.ac.at/ita/pdf/ita_04_02.pdf>

ITA-04-03 Johannes M. Bauer (11/2004): Governing the Networks of the Information Society – Prospects and limits of policy in a complex technical system. <www.oeaw.ac.at/ita/pdf/ita_04_03.pdf>

ITA-04-04 Ronald Leenes (12/2004): Local e-Government in the Netherlands: From Ambitious Policy Goals to Harsh Reality. <www.oeaw.ac.at/ita/pdf/ita_04_04.pdf>

ITA-05-01 Andreas Krisch (1/2005): Die Veröffentlichung des Privaten – Mit intelligenten Etiketten vom grundsätzlichen Schutz der Privatsphäre zum Selbstschutz-Prinzip. <www.oeaw.ac.at/ita/pdf/ita_05_01.pdf>

ITA-05-02 Petra Grabner (12/2005): Ein Subsidiaritätstest – Die Errichtung gentechnikfreier Regionen in Österreich zwischen Anspruch und Wirklichkeit. <epub.oeaw.ac.at/ita/ita-manuscript/ita_05_02.pdf>

ITA-05-03 Eva Buchinger (12/2005): Innovationspolitik aus systemtheoretischer Sicht – Ein zyklisches Modell der politischen Steuerung technologischer Innovation. <www.oeaw.ac.at/ita/pdf/ita_05_03.pdf>

ITA-06-01 Michael Latzer (6/2006): Medien- und Telekommunikationspolitik: Unordnung durch Konvergenz – Ordnung durch Mediamatikpolitik. <epub.oeaw.ac.at/ita/ita-manuscript/ita_06_01.pdf>

ITA-06-02 Natascha Just, Michael Latzer, Florian Saurwein (9/2006): Communications Governance: Entscheidungshilfe für die Wahl des Regulierungsarrangements am Beispiel Spam. <epub.oeaw.ac.at/ita/ita-manuscript/ita_06_02.pdf>

ITA-06-03 Veronika Gaube, Helmut Haberl (10/2006): Sozial-ökologische Konzepte, Modelle und Indikatoren nachhaltiger Entwicklung: Trends im Ressourcenverbrauch in Österreich. <epub.oeaw.ac.at/ita/ita-manuscript/ita_06_03.pdf>

ITA-06-04 Maximilian Fochler, Annina Müller (11/2006): Vom Defizit zum Dialog? Zum Verhältnis von Wissenschaft und Öffentlichkeit in der europäischen und österreichischen Forschungspolitik. <epub.oeaw.ac.at/ita/ita-manuscript/ita_06_04.pdf>

ITA-06-05 Holger Floeting (11/2006): Sicherheitstechnologien und neue urbane Sicherheitsregimes. <epub.oeaw.ac.at/ita/ita-manuscript/ita_06_05.pdf>

ITA-06-06 Armin Spök (12/2006): From Farming to „Pharming" – Risks and Policy Challenges of Third Generation GM Crops. <epub.oeaw.ac.at/ita/ita-manuscript/ita_06_06.pdf>

ITA-07-01 Volker Stelzer, Christine Rösch, Konrad Raab (3/2007): Ein integratives Konzept zur Messung von Nachhaltigkeit – das Beispiel Energiegewinnung aus Grünland. <epub.oeaw.ac.at/ita/ita-manuscript/ita_07_01.pdf>

ITA-07-02 Elisabeth Katzlinger (3/2007): Big Brother beim Lernen: Privatsphäre und Datenschutz in Lernplattformen. <epub.oeaw.ac.at/ita/ita-manuscript/ita_07_02.pdf>

ITA-07-03 Astrid Engel, Martina Erlemann (4/2007): Kartierte Risikokonflikte als Instrument reflexiver Wissenspolitik. <epub.oeaw.ac.at/ita/ita-manuscript/ita_07_03.pdf>

ITA-07-04 Peter Parycek (5/2007): Gläserne Bürger − transparenter Staat? Risiken und Reformpotenziale des öffentlichen Sektors in der Wissensgesellschaft. <epub.oeaw.ac.at/ita/ita-manuscript/ita_07_04.pdf>

ITA-07-05 Helge Torgersen (7/2007): Sicherheitsansprüche an neue Technologien – das Beispiel Nanotechnologie. <epub.oeaw.ac.at/ita/ita-manuscript/ita_07_05.pdf>

ITA-07-06 Karen Kastenhofer (9/2007): Zwischen „schwacher" und „starker" Interdisziplinarität. Die Notwendigkeit der Balance epistemischer Kulturen in der Sicherheitsforschung zu neuen Technologien. <epub.oeaw.ac.at/ita/ita-manuscript/ita_07_06.pdf>

ITA-07-07 Ralf Lindner, Michael Friedewald (9/2007): Gesellschaftliche Herausforderungen durch „intelligente Umgebungen. Dunkle Szenarien als TA-Werkzeug. <epub.oeaw.ac.at/ita/ita-manuscript/ita_07_07.pdf>

ITA-07-08 Alfons Bora (11/2007): Die disziplinären Grundlagen der Wissenschaft. <epub.oeaw.ac.at/ita/ita-manuscript/ita_07_08.pdf>

ITA-08-01 Alexander Degelsegger (5/2008): „Frames" in sozialwissenschaftlichen Theorieansätzen. Ein Vergleich aus der Perspektive der Technikforschung. <epub.oeaw.ac.at/ita/ita-manuscript/ita_08_01.pdf>

ITA-08-02 Jens Hoff (11/2008): Can The Internet Swing The Vote? Results from a study of the 2007 Danish parliamentary election. <epub.oeaw.ac.at/ita/ita-manuscript/ita_08_02.pdf>

ITA-09-01 Georg Aichholzer, Doris Allhutter (2/2009): e-Participation in Austria: Trends and Public Policies. <epub.oeaw.ac.at/ita/ita-manuscript/ita_09_01.pdf>

ITA-09-02 Michael Nentwich (11/2009): Cyberscience 2.0 oder 1.2? Das Web 2.0 und die Wissenschaft. <epub.oeaw.ac.at/ita/ita-manuscript/ita_09_02.pdf>

ITA-09-03 Hilmar Westholm (12/2009): Wandel der Formen politischer Partizipation und der Beitrag des Internet. Schlussfolgerungen aus Bevölkerungsbefragungen in Deutschland. <epub.oeaw.ac.at/ita/ita-manuscript/ita_09_03.pdf>

ITA-10-01 Iris Eisenberger (12/2010): Kleine Teile, große Wirkung? Nanotechnologieregulierung in der Europäischen Union. <epub.oeaw.ac.at/ita/ita-manuscript/ita_10_01.pdf>

ITA-10-02 Alexander Degelsegger and Helge Torgersen (12/2010): Instructions for being unhappy with PTA. The impact on PTA of Austrian technology policy experts' conceptualisation of the public. <epub.oeaw.ac.at/ita/ita-manuscript/ita_10_02.pdf>

ITA-10-03 Ernest Braun (12/2010): The Changing Role of Technology in Society. <epub.oeaw.ac.at/ita/ita-manuscript/ita_10_03.pdf>

ITA-10-04 Fritz Betz (12/2010): E-Partizipation und die Grenzen der Diskursethik. <epub.oeaw.ac.at/ita/ita-manuscript/ita_10_04.pdf>

ITA-11-01 Peter Parycek, Judith Schoßböck (1/2011): Transparency for Common Good. Offener Zugang zu Information im Kontext gesellschaftlicher und strategischer Spannungsfelder. <epub.oeaw.ac.at/ita/ita-manuscript/ita_11_01.pdf>

ITA-11-02 Georg Aichholzer und Doris Allhutter (6/2011): Online forms of political participation and their impact on democracy. <epub.oeaw.ac.at/ita/ita-manuscript/ita_11_02.pdf>

ITA-11-03 Mahshid Sotoudeh, Walter Peissl, Niklas Gudowsky, Anders Jacobi (12/2011): Long-term planning for sustainable development. CIVISTI method for futures studies with strong participative elements. <epub.oeaw.ac.at/ita/ita-manuscript/ita_11_03.pdf>

ITA-12-01 Xiao Ming (1/2012): e-Participation in Government Decision-Making in China. Reflections on the Experience of Guangdong Province. <epub.oeaw.ac.at/ita/ita-manuscript/ita_12_01.pdf>

ITA-12-02 Stephan Bröchler, Georg Aichholzer, Petra Schaper-Rinkel (Hrsg.) (9/2012): Theorie und Praxis von Technology Governance. <epub.oeaw.ac.at/ita/ita-manuscript/ita_12_02_Sondernummer.pdf>

ITA-12-03 Iris Eisenberger (10/2012): EU-Verhaltenskodex Nanotechnologie: Rechtsstaatliche und demokratische Aspekte. <epub.oeaw.ac.at/ita/ita-manuscript/ita_12_03.pdf>

ITA-12-04 Julia Haslinger, Christiane Hauser, Peter Hocke, Ulrich Fiedeler (10/2012): Ein Teilerfolg der Nanowissenschaften? Eine Inhaltsanalyse zur Nanoberichterstattung in repräsentativen Medien Österreichs, Deutschlands und der Schweiz. <epub.oeaw.ac.at/ita/ita-manuscript/ita_12_04.pdf>

ITA-13-01 Helge Torgersen, Alexander Bogner, Karen Kastenhofer (10/2013): The Power of Framing in Technology Governance: The Case of Biotechnologies. <epub.oeaw.ac.at/ita/ita-manuscript/ita_13_01.pdf>

ITA-13-02 Astrid Mager (11/2013): In search of ideology. Socio-cultural dimensions of Google and alternative search engines. <epub.oeaw.ac.at/ita/ita-manuscript/ita_13_02.pdf>

ITA-13-03 Petra Wächter (12/2013): Aspekte einer nachhaltigen Energiezukunft. <epub.oeaw.ac.at/ita/ita-manuscript/ita_13_03.pdf>

ITA-14-01 Renate Mayntz (8/2014): Technikfolgenabschätzung – Herausforderungen und Grenzen. <epub.oeaw.ac.at/ita/ita-manuscript/ita_14_01.pdf>

ITA-14-02 Michael Narodoslawsky (11/2014): Utilising Bio-resources: Rational Strategies for a Sustainable Bio-economy. <epub.oeaw.ac.at/ita/ita-manuscript/ita_14_02.pdf>

ITA-14-03 Petra Wächter (12/2014): Ökonomik in der Technikfolgenabschätzung – eine Bestandsaufnahme. <epub.oeaw.ac.at/ita/ita-manuscript/ita_14_03.pdf>

ITA-15-01 Reinhard Grünwald (5/2015): Stromnetze: Bedarf, Technik, Folgen. <epub.oeaw.ac.at/ita/ita-manuscript/ita_15_01.pdf>

ITA-15-02 Christine Chaloupka, Robert Kölbl, Wolfgang Loibl, Romain Molitor, Michael Nentwich, Stefanie Peer, Ralf Risser, Gerd Sammer, Bettina Schützhofer, Claus Seibt (6/2015): Nachhaltige Mobilität aus sozioökonomischer Perspektive – Diskussionspapier der Arbeitsgruppe „Sozioökonomische Aspekte" der ÖAW-Kommission „Nachhaltige Mobilität". <epub.oeaw.ac.at/ita/ita-manuscript/ita_15_02.pdf>

ITA-15-03 Sabine Pfeiffer (10/2015): Auswirkungen von Industrie 4.0 auf Aus- und Weiterbildung. <epub.oeaw.ac.at/ita/ita-manuscript/ita_15_03.pdf>

ITA-15-04 Sabine Pfeiffer (11/2015): Effects of Industry 4.0 on vocational education and training. <epub.oeaw.ac.at/ita/ita-manuscript/ita_15_04.pdf>

ITA-16-01 Lorenzo Del Savio, Alena Buyx & Barbara Prainsack (3/2016): Opening the black box of participation in medicine and healthcare. <epub.oeaw.ac.at/ita/ita-manuscript/ita_16_01.pdf>

ITA-16-02 Michael Nentwich (10/2016): Parliamentary Technology Assessment Institutions and Practices. <epub.oeaw.ac.at/ita/ita-manuscript/ita_16_02.pdf>

ITA-17-01 Helge Torgersen (3/2017): Neuroenhancement – (k)ein TA-Thema? <epub.oeaw.ac.at/ita/ita-manuscript/ita_17_01.pdf>

ITA-18-01 Karen Kastenhofer, Katharina Novy (6/2018): Vom Wissen zum Können, vom Lehren zum Forschen? Der Wandel biologischer Wissenschaftskultur am Universitätsstandort Wien. <epub.oeaw.ac.at/ita/ita-manuscript/ita_18_01.pdf>

ITA-18-02 Elias Moser (10/2018): Normative Leitbilder in der Technikfolgenabschätzung. <epub.oeaw.ac.at/ita/ita-manuscript/ita_18_02.pdf>

ITA-19-01 Michael Nentwich, Wilfried Jäger, Gerhard Embacher-Köhle und Jaro Krieger-Lamina (06/2019): Kann es eine digitale Souveränität Österreichs geben? Herausforderungen für den Staat in Zeiten der digitalen Transformation. <epub.oeaw.ac.at/ita/ita-manuscript/ita_19_01.pdf>