Europas digitale Souveränität. Bedingungen und Herausforderungen internationaler politischer Handlungsfähigkeit

Annegret Bendiek und Jürgen Neyer

1 Souveränität im Wandel

Die Europäische Union sieht sich heute einer grundlegend neuen Herausforderung gegenüber. Nachdem die letzten sechzig Jahre des Integrationsprozesses wesentlich von internen Herausforderungen wie der Krise des leeren Stuhls, der Eurosklerose und der Finanzkrise gekennzeichnet waren, steht heute zunehmend die internationale Politik im Fokus. In einer Vielzahl von Politikfeldern, vom Kampf gegen Hassreden bis zur Ächtung von autonomen Waffensystemen, von der Debatte über das Verbot der Gesichtserkennung bis zur Regulierung der künstlichen Intelligenz lassen sich internationale und innereuropäische Regelsetzungsprozesse kaum noch voneinander trennen. China, die USA, Russland und Europa befinden sich heute in einem intensiven Regulierungswettbewerb, in dem unterschiedliche normative Modelle über globale Marktprozesse und internationale politische Regulierungsinstanzen vermittelt sind. Die Globalisierung der europäischen Datenschutzbestimmungen (etwa die Datenschutzgrundverordnung, DSGVO), die Verfolgung von Verantwortlichkeitsregelungen für Online-Plattformen (in D, das NetzDG) und die Förderung einer rechtsstaatlich orientierten, vorsorgenden Technologie-Governance im Bereich der künstlichen Intelligenz sind eindeutige

A. Bendiek (✉)
Stiftung Wissenschaft und Politik, Berlin, Deutschland
E-Mail: annegret.bendiek@swp-berlin.org

J. Neyer
Europa Universität Viadrina, Frankfurt/Oder, Deutschland
E-Mail: neyer@europa-uni.de

M. Oswald und I. Borucki (Hrsg.), *Demokratietheorie im Zeitalter der Frühdigitalisierung*, https://doi.org/10.1007/978-3-658-30997-8_6

Beispiele für diesen Prozess. In allen diesen Feldern geht es nicht nur um die ökonomisch motivierte Internationalisierung eigener EU-Standards und damit den Versuch der Externalisierung eigener Anpassungskosten, sondern letztlich um die Aufrechterhaltung des eigenen, europäischen Gesellschaftsmodells in einem zunehmend umkämpften Umfeld. Um in diesem neuen Umfeld bestehen zu können, so der weit verbreitete Tenor, müsse Europa sich so verhalten wie andere Großmächte auch, d. h. lernen, wie eine geopolitische Macht zu denken und eine neue Form von Souveränität zu entwickeln (Timmers 2019a; European Commission and European External Action Service 2017; European Commission 2018; Leonard und Shapiro 2019a; Leonard und Shapiro 2019b).

Was aber genau ist unter digitaler Souveränität eigentlich zu verstehen? Und wie gut ist die Europäische Union darauf eingestellt, digitale Souveränität auszuprägen? Nachdem im folgenden Abschnitt der Begriff der digitalen Souveränität näher erläutert wird, beschreibt Kap. 3 wie sich Europa in der internationalen Politik der Herausforderung stellt, seine Wirtschafts- und Gesellschaftsordnung gegenüber konkurrierenden Mächten zu bewahren, auf globale Standardsetzungen Einfluss zu nehmen und technologisch wettbewerbsfähig zu bleiben. Kap. 4 geht auf die interne Dimension von digitaler Souveränität ein. Es beschreibt die innenpolitische Herausforderung, unter den Bedingungen sozialer und kommunikativer Fragmentierung inklusive Prozesse der sozialen Integration und der Meinungsbildung zu gestalten. Beiden Herausforderungen, so das abschließende Kap. 5, lässt sich im Rahmen eines europäischen digitalen Souveränitätsverständnisses begegnen, das die externe und die interne Betonung europäischer Werte als wesentliche Bestandteile europäischer Politik kombiniert.

2 Digitale Souveränität

Der Begriff der digitalen Souveränität wird bislang noch kaum für die wissenschaftliche Analyse der Fähigkeit der EU zur politischen Interessenswahrnehmung verwandt. Und wenn doch, dann wird digitale Souveränität bisher fast ausschließlich in Expertisen politiknaher Stiftungen und Beratungsinstitutionen genutzt, um die Fähigkeit von BürgerInnen und Unternehmen, informationell selbstbestimmt digitale Technologien nutzen zu können, zu beschreiben (Gräf et al. 2018; BITKOM 2015; SVR (2017). Für die Beschreibung der Fähigkeit der Europäischen Union zur Artikulation und Durchsetzung ihrer Interessen mit (und gegen) Andere(n) finden allerdings eine Reihe verwandter Begriffe wie ‚technologische Souveränität' (Leonard und Shapiro 2019a), ‚strategische Autonomie'

(European Commission 2019) oder ‚digitale Autonomie' (Voss 2020) durchaus Verwendung.

In diesem Text gehen wir davon aus, dass es sinnvoll ist, die Beschreibung der Fähigkeit der EU zur Selbstbehauptung entlang der beiden Begriffe von ‚digital' und ‚Souveränität' auszubuchstabieren. Der Begriff des Digitalen greift den Umstand auf, dass wir es heute in der Politik mit einer umfassenden algorithmischen Erfassung und Verarbeitung von Sachverhalten in den drei Sachbereichen der Herrschaft, der Wohlfahrt und der Sicherheit zu tun haben.[1] Sachverhalte werden zunehmend ermittelt über algorithmische Abbildungen wahrgenommen und in Form digitaler Strategien bearbeitet (Nassehi 2019).[2] Hierdurch verändert sich nicht nur die Ausdrucksform politischer Gegenstände, sondern auch ihr Inhalt und damit ihr Konfliktpotential. Digitale Souveränität ist so verstanden die Fähigkeit der Europäischen Union, interne Entscheidungsprozesse in algorithmisch geprägten Umgebungen zu realisieren und extern in entsprechende Politikergebnisse zu überführen. Dieses Begriffsverständnis kombiniert drei Traditionen der Interpretation des Souveränitätskonzeptes:[3] Rechtliche Souveränität bezieht sich in der Tradition von Jean Bodin auf die Befugnis, für alle anderen verbindlich kraft autoritativer Entscheidung Recht setzen zu dürfen. Souverän ist demzufolge derjenige, der das unumschränkte Recht hat, Recht zu setzen (Hillgruber 2014). Rechtliche Souveränität kennt weder moralische noch politische Grenzen; sie beschreibt schlicht einen rechtlichen Zustand, der gegeben ist oder auch nicht. Politische Souveränität bezieht sich im Anschluss an AutorInnen wie Carl Schmitt auf einen Zustand der faktischen Fähigkeit, verbindliche Regelungen zu erlassen, völlig unabhängig davon, ob diese rechtlich abgesichert sind oder auch nicht. „Souverän", so das berühmte Diktum von Schmitt, „ist wer über den Ausnahmezustand entscheidet"

[1] Für einen Überblick s. (Hofmann et al.2019).

[2] Am Beispiel der Corona-Krise von 2020 lässt sich dieser Sachverhalt gut illustrieren. Die Ausbreitung des Virus wird von der Politik als algorithmisch abgebildeter Prozess der zeitlichen Veränderung der Anzahl Neuinfizierter verstanden. Politische Maßnahmen der Intensivierung oder Erleichterung von Kontaktsperren werden entsprechend daran ausgerichtet, wie diese Messzahl sich verändert. Auch die Maßnahmen selbst sind stark digital geprägt. In China werden inzwischen alle Personen mit einem personalisierten QR-Code ausgestattet, der es erlaubt, ihren Gesundheitszustand, ihre Bewegungsprofile und ihre sozialen Kontakte zu erfassen. Digitale Instrumente sind damit sowohl für die Beschreibung und damit Wahrnehmung der Pandemie als auch für wesentliche Instrumente zu ihrer Bekämpfung zuständig.

[3] Grundsätzlich hierzu vgl. (Grimm 2009).

(Schmitt 1922, S. 9). Ein drittes Verständnis von Souveränität lässt sich mit Rousseau als Volkssouveränität beschreiben. Souveränität ist hier die Qualität eines Volkes (oder moderner: der Gesamtheit der Staatsangehörigen), einen gemeinsamen Willen auszubilden (Maus 2011). Souveränitätskonzepte lassen sich weiterhin danach unterscheiden, ob sie die innere oder die äußere Dimension von Staatlichkeit thematisieren. Innere Souveränität bezieht sich auf die staatliche Eigenschaft einer Überordnung öffentlicher Autorität gegenüber allen Individuen und Organisationen, die innerhalb seiner Grenzen leben oder arbeiten. Äußere Souveränität bedeutet, dass in der Gemeinschaft der Staaten kein Staat einer anderen Autorität untergeordnet ist und, dass kein anderer Staat und keine internationale Organisation die Herrschaft über einen Staat für sich beanspruchen.

Für ein angemessenes Verständnis von europäischer Souveränität unter Bedingungen der Digitalisierung braucht es die Entwicklung eines komplexen Souveränitätsbegriffes, der alle diese Verständnisse in sich aufnimmt. Komplexe Souveränität beinhaltet zuerst einmal eine rechtliche Dimension der formalen inneren und äußeren Zuständigkeit. Politik in Europa ist Politik innerhalb der Rechtsgemeinschaft – und damit außerhalb rechtlicher Verfahren kaum möglich. Die geringe Effektivität von intergouvernementalen Politiken wie der GASP unterstreicht diese Abhängigkeit deutlich. Die Teilhabe Europas an politischen Prozessen in der *International Telecommunication Union* (ITU) oder anderen internationalen Gremien wird zudem erst dann politisch relevant, wenn Akteure wie die Europäische Kommission ihre formalen inneren und äußeren Kompetenzen entweder gegen andere oder im Zusammenspiel mit diesen umsetzen können. Hierzu gehört sowohl Verhandlungsmacht gegenüber anderen Staaten als auch die innereuropäische Fähigkeit, Einigungen zwischen den Mitgliedstaaten zu etablieren. Die Vergangenheit hat deutlich gezeigt, dass diese Dimension alles andere als unwichtig ist. Mitgliedstaatliche Uneinigkeiten werden leicht von anderen Staaten dazu ausgenutzt, diese gegeneinander auszuspielen und gemeinsame europäische Politiken zu blockieren. Komplexe Souveränität bezieht sich somit auf die innere und äußere Fähigkeit der EU, rechtliche Kompetenzen sowohl innereuropäisch als auch international auf der Basis erfolgreicher europäischer Meinungsbildungsprozesse effektiv ausüben zu können.

3 Europas digitale Souveränität in der internationalen Politik

Der globale Kontext Europas hat sich in den letzten zwanzig Jahren deutlich verändert. Das erste Jahrzehnt des 21. Jahrhunderts wurde von der Idee eines ‚Raumes der Ströme' geprägt, der den alten ‚Raum der Orte' zunehmend über-

lagert (Castells 1996).[4] Die Kategorie des Territoriums schien ihre Bedeutung für das Verständnis und die Funktionsweise der globalisierten Wirtschaft verloren zu haben (Ohmae 1995).[5] Die wissenschaftliche und politische Diskussion dieser Zeit drehte sich um das Konzept einer ‚flachen Welt' (Friedman 2007), in der die Distanzen zwischen den Kulturen und Nationen verschwinden würden und eine neue transnationale und durch globale Kommunikationsströme integrierte Elite die Kontrolle übernähme. TheoretikerInnen der internationalen Politik schrieben über eine ‚unpolare' Welt, in der die Macht so weit verbreitet wäre, dass kein Staat mehr Kontrolle über die Ergebnisse der Politik habe (Nye 2011, S. 113). Digitale Libertäre stellten alle Formen staatlicher Interventionen infrage, gaben eine ‚Unabhängigkeitserklärung' des Internets ab und plädierten für eine Form der politischen Organisation, die auf dem Modell der *Multi-Stakeholder-Governance* basiert (Barlow 1996). Mueller behauptete sogar, dass ‚die Menschen des Internets' eine transnationale, von der staatlichen Autorität unabhängige Volkssouveränität bilden sollten (Mueller 2017, S. 134). Diese neue Souveränität sollte die Nationalstaaten in allen Fragen der Regulierung des Internets verdrängen und eine eigene politische Identität entwickeln.

3.1 Konfliktive Re-Territorialisierung

Seitdem hat sich viel geändert. In der ganzen westlichen Welt erleben wir heute eine erneute Betonung von Territorium und Nation als wichtige politische Kategorien (Wimmer 2019; Snyder 2019; Goldsmith und Wu 2008). Die Entwicklung riskanter Technologien hat die moderne Gesellschaft in eine „Risikogesellschaft" transformiert, „in der der Ausnahmezustand zum Normalzustand zu werden droht" (Beck 1986, S. 31). Moderne Infrastrukturen sind gekennzeichnet von Konnektivität (umfassende Vernetzung mit resultierenden Kaskadeneffekten), Komplexität (vielfach überlagerte und interdependente Kausalitäten) und damit einhergehender Kontingenz (beschränkte Vorhersehbarkeit). Die zunehmende Konnektivität und Komplexität unterschiedlicher Lebensbereiche hat zu einem

[4]Castells described the emergence of a new world being organized "in networks pertaining to a space of flows that links them up around the world, while fragmenting subordinate functions, and people, in the multiple space of places, made of locales increasingly segregated and disconnected from each other" (S. 476).

[5]"[…] traditional nation states have become unnatural, even impossible, business units in a global economy" (S. 5).

Zustand „systemischer Vulnerabilität“ (Edwards 2013) geführt. Das Systemversagen ist das Erwartbare geworden, welches das Zufällige infrage stellt (Virilio 2009).[6] Die Maßgabe lautet, „sich auf das forcierte Bewusstsein ungewisser Zukünfte einzustellen und sich auf das Nicht-Vorbereitbare vorzubereiten“ (Blum et al. 2016, S. 155).

Wenn Sicherheit nicht mehr als Zustand, sondern nur noch als Prozess gedacht werden kann, dann erfordert sie ein Denken in Kategorien permanenter Herausforderung und der Bereitschaft zur Anerkennung struktureller Unsicherheit: wir können nicht wissen, was morgen auf uns zukommen wird (Vgl. Scharte und Thoma 2016, S. 132 f.). Nicht bloß Prävention gegenüber dem Wiederauftreten des Bekannten, sondern Reaktionsfähigkeit gegenüber dem Unbekannten ist die zentrale Herausforderung in der Gestaltung moderner offener Infrastrukturen. In der neuen Welt von Konnektivität, Komplexität und Kontingenz kann sich die Frage der sicheren Gestaltung von Infrastrukturen nicht mehr auf die Minimierung von Wahrscheinlichkeit und Risiko beschränken, sondern muss in Begriffen von Möglichkeit und Plausibilität gedacht werden. Das Denken in Kategorien des Konfliktmanagements von der Vorsorge bis hin zur Nachsorge wird abgelöst durch ein Denken in den Kategorien von Resilienz[7]. Transnationale Netzwerke werden in diesem Kontext heute zunehmend als Orte der Gefährdung, der harten Machtpolitik und des Ringens um Einfluss verstanden (Leonard 2016, S. 95).[8] Sie generieren aufgrund der ungleich verteilten Einflusskanäle und Knotenpunkte die Möglichkeit, Informationsflüsse zu steuern und Interdependenz als Waffe in der internationalen Politik zu benutzen (Farrell und Newman 2019).

Beispielsweise sind komplexe Systeme wie die Netzwerktechnik für 5G in diesem Kontext sehr viel mehr als bloße Technologien. Sie werden für Jahrzehnte in den Infrastrukturen eines Staates verbaut und drohen bei einer Auftragsvergabe an Unternehmen aus unfreundlich gesinnten oder autoritären Staaten

[6]Paul Virilio spricht vom»integralen Unfall«: Ob Blackout, Börsencrash oder Bevölkerungsexplosion, ob Stau oder Super-GAU, Server-Breakdown, nervous breakdown oder neuerdings der»Klimakollaps« (Virilio 2009, S. 7) siehe auch (Perrow 1999).

[7]Resilienz wird daher auch als „a technology of governing the unknowable“ verstanden (Kaufmann 2013, S. 65). Einen guten Überblick über die aktuelle Forschungslandschaft in unterschiedlichsten wissenschaftlichen Disziplinen bieten (Wink 2016) und (Karidi et al. 2018).

[8]„Schlachtfeld ist die vernetzte Infrastruktur der globalen Wirtschaft und als Waffe dient die Unterbrechung oder Reduzierung unserer globalen Verknüpfungen: Handel und Investitionen, internationales Recht, Internet, Transportwege und Personenfreizügigkeit. Willkommen im Zeitalter der Verknüpfungskriege.“

unwillkommener fremder politischer Kontrolle zu unterliegen. Netzwerkprodukte entwickeln sich derzeit zu einer im Wesentlichen durch Software definierten Technologie weiter, deren regelmäßige Updates für den einsetzenden Betreiber kaum nachvollziehbare Funktionalitätsveränderungen bringen. Gleichzeitig verändert die digitale Transformation alle Marktsegmente, von landwirtschaftlichen Produkten, über die Medizintechnik bis zum Maschinenbau. Kaum noch ein wichtiges Produktsegment existiert heute komplett außerhalb des Internets, anspruchsvoller Algorithmen und damit jenseits von technologischen Abhängigkeiten gegenüber großen US-amerikanischen oder – zunehmend – chinesischen Konzernen. Handelsfragen werden immer stärker mit dem Ringen um digitale Kontrollfähigkeit verschränkt (vgl. Bendiek und Schallbruch 2019).

Die Relevanz der aktuellen wirtschafts- und handelspolitischen Konflikte zwischen den USA, China und der EU geht daher weit über rein ökonomische Fragen hinaus. Digitale Technologien sind die Kommunikationsinfrastruktur hochentwickelter Informationsgesellschaften. Wer die Kontrolle über Hard- und Software hat, bestimmt auch, wer zu welchem Zeitpunkt und zu welchem Preis Zugriff auf welche Informationen hat. Mit der Digitalisierung geht eine neue Konflikthaftigkeit in der globalen Politik, eine neue Auseinandersetzung um global gültige Standards und damit letztlich auch um die Gültigkeit europäischer Werte einher.

Diese Auseinandersetzung findet derzeit nur wenig konstruktive Begleitung in der internationalen Politik. Globale Normen und Regulierungen in Fragen der Cybersicherheit sind nach über zehn Jahren erfolgloser Verhandlungen in einem Klima der Cyberrivalität zwischen den USA und China stecken geblieben. Die Debatten über staatliches Verhalten im Cyberraum, die globale Ächtung oder Beschränkung von Cyberangriffen und eine völkerrechtlich abgesicherte Organisation zur Cyberabwehr wurden zwar in fünf Verhandlungsrunden der Gruppe von Regierungsexperten auf VN-Ebene (Group of Governmental Experts GGE) verhandelt, blieben aber erfolglos. In der aufgeladenen Konfliktsituation zwischen den USA und China und aufgrund der erheblichen Interessendivergenzen zwischen liberalen Demokratien und autoritären Staaten sind baldige Fortschritte der derzeitigen Verhandlungsrunden der GGE und der von Russland und China initiierten Open Ended Working Group (OEWG) auch weiter unwahrscheinlich.

Die neue Konflikthaftigkeit ist zuerst einmal eng mit dem Aufstieg Chinas zur technologischen Großmacht verbunden. Über die chinesische Marktmacht erhalten auch die in chinesischer Technologie von Huawei und ZTE aufgehobenen Werte Einzug nach Europa. Gesichtserkennungssoftware, *Social Scoring* und andere Überwachungsinstrumente werden bereits auf dem

europäischen Markt angeboten und können leicht von interessierten Staaten (selbst in der Europäischen Union) für die Kontrolle oppositioneller Gruppen angewandt werden. Der Aufstieg der USA zur globalen Hegemonialmacht ging nach 1945 mit einer Ausbreitung des *American Way of Life* einher. Genauso könnte der Aufstieg Chinas eine vergleichbare Attraktivität seines Gesellschaftsmodells nach sich ziehen. Das chinesische Cybersicherheitsgesetz von 2017 hat hier für viel Irritation gesorgt. Es sieht u. a. die Registrierung von Vollnamen für InternetnutzerInnen vor und verbietet *Virtul Private Networks* (VPN), verlangt verschärfte Sicherheitsauflagen für kritische Infrastrukturen und für Anbieter ‚kritischer Informationsinfrastruktur' (vgl. auch Langer in diesem Band). Der Staat behält sich das Recht vor, die privaten Datenschutzansprüche seiner BürgerInnen dann einzuschränken, wenn Fragen der nationalen Sicherheit oder der nationalen Wirtschaft berührt sind. Individuelle Freiheitsrechte stehen hiermit faktisch unter dem Vorbehalt ihrer Vereinbarkeit mit staatlichen Interessen. Hinzu kommt, dass chinesische Unternehmen unter einem Generalverdacht stehen, von der chinesischen Regierung ferngesteuert zu sein oder sich zumindest im Konfliktfall einer derartigen Instrumentalisierung nicht entziehen zu können. Am Streit um den chinesischen Technologiekonzern Huawei ist diese Befürchtung jüngst deutlich geworden.[9] Das Angebot Huaweis, auf dem europäischen Markt den Aufbau der 5G Infrastruktur mit voranzutreiben, stößt auf massive Vorbehalte seitens der US-amerikanischen sowie einer Reihe europäischer Regierungen. Die US-Regierung betrachtet Huawei als das trojanische Pferd einer gegnerischen Regierung, deren Politik mit den amerikanischen Interessen unvereinbar sei (Marcus 2019). Der Konflikt um Huawei droht einen grundlegenden Bruch mit der Logik einer globalen Marktwirtschaft zu signalisieren. Er könnte eine neue Phase des internationalen Merkantilismus einleiten, in der der Gewinn einer Partei als identisch mit dem Verlust einer anderen Partei verstanden wird (Marcus 2019). In dieser neuen Wahrnehmung des Nullsummenaustauschs ist die Konvergenz der Märkte nicht mehr nur eine Chance für Wohlstand, sondern zunehmend eine Bedrohung für die öffentliche Sicherheit. Neue Konzepte wie technologische Souveränität und wirtschaftliche Verwundbarkeit beginnen den Glauben an eine globale Wirtschaftsordnung des gemeinsamen Marktes zu ersetzen.

[9]Dokumentationen des Konfliktes sind zu finden in (Johnson und Groll n.d.; Rühlig et al. 2019).

Die neue Konflikthaftigkeit in der digitalisierten Politik beschränkt sich allerdings nicht auf die Beziehungen zwischen dem Westen und China. Auch in den transatlantischen Beziehungen sind die normativen Vorstellungen oftmals nur schwer in Einklang zu bringen.[10] Die vielbeschworene transatlantische Wertegemeinschaft kollidiert immer häufiger mit grundlegend unterschiedlichen Vorstellungen zum Umgang mit Daten, der Regulierung des Wettbewerbs und dem Schutz von Privatheit. Während die US-Regierung für ihre Sicherheitsdienste den Zugriff auch auf sensible Daten fordert, im Verhältnis zwischen Konzernen und KonsumentInnen die Vertragsfreiheit betont und sich gegen die Regulierung des Marktes durch europäische Institutionen wehrt, sind die Europäer stolz darauf, in allen diesen Bereichen ihre eigenen Wertvorstellungen zum Ausdruck zu bringen. Ein klares Beispiel für die zunehmende Kluft zwischen den USA und Europa ist die Reaktion der Regierung Trump auf die Strafen, die die Europäische Kommission *Google* wiederholt wegen Verstößen gegen das europäische Wettbewerbsrecht auferlegt hat. Unter völliger Missachtung der verfassungsrechtlichen und regulatorischen Gründe für diese Entscheidungen bewertete US-Präsident Donald Trump sie als eine reine Racheaktion einer „tax lady who hates the US" (Becker 2018). Dies ist mehr als ein Tweet. Es ist ein Beweis für die Lücke zwischen zunehmend schwierig zu vereinbarenden Regulierungsphilosophien auf beiden Seiten des Atlantiks.

3.2 Ethisch verantwortete digitale Souveränität

Der wachsenden internationalen Konflikthaftigkeit wird in Europa mit der Forderung nach mehr europäischer Eigenständigkeit und der Etablierung einer ‚digitalen Souveränität' (Benner 2010) und ‚strategischen Autonomie der EU'[11] begegnet. Die alte Idee einer globalen liberalen Ordnung, die auf der Basis konsentierter Werte und Normen einen rechtlichen Rahmen für die Etablierung globalen Regierens etabliert, tritt immer stärker in den Hintergrund und wird

[10]Für eine aufschlussreiche Analyse über die Ursachen der Krise der liberalen Ordnung siehe (Ikenberry 2018).

[11]Strategische Autonomie ist "the ability, in terms of capacity and capabilities, to decide and act upon essential aspects of one's longer-term future in the economy, society and their institutions" (Timmers 2019b, S. 2).

zunehmend von der Forderung nach einem selbstbewussteren Auftreten Europas, verstärkter ‚Datensouveränität' oder gar ‚digitalen Grenzkontrollen' überlagert.[12]

Die Europäische Union ist auf Denktraditionen aufgebaut, denen protektionistische und auf Abschottung ausgerichtete Ideen zuerst einmal fremd sind. Sie basiert auf einer engen Verbindung zwischen ethischen Normen, abstrakten Verfassungsgrundsätzen und konkreten rechtlichen Anforderungen. In Art. 3 und 10 EUV betont die EU die individuelle Selbstbestimmung der europäischen Bürgerinnen und Bürger durch ihr Bekenntnis zu Marktfreiheit und Demokratie. Sie realisiert eine politische Ordnung, die zu grundlegenden ethischen Fragen Stellung nimmt, ohne den Anspruch auf eine universelle Wahrheit zu erheben. Dieses ethisch fundierte Gesellschaftsverständnis findet sich auch in aktuellen Positionspapieren der europäischen Institutionen zu den Chancen und Herausforderungen der digitalen Gesellschaft. Der Europarat (Council of Europe 2019a), der Europäische Rat (Council of Europe 2019b) und die Europäische Kommission (European Commission 2018) haben eine Reihe von Erklärungen und Positionspapieren verabschiedet, die die Idee einer demokratischen digitalen Gesellschaft zum Ausdruck bringen, die sowohl sozial als auch individuell zentriert ist. In all diesen Papieren wird der technologische Fortschritt als eine von Menschen gemachte Chance gesehen, die grundsätzlich offen ist für die Verbesserung der Gesellschaft. Neue Technologien müssen nicht nur effizient sein, sondern auch zu Demokratie und Menschenrechten beitragen.

Ein deutliches Beispiel für diesen besonderen europäischen Ansatz ist die Haltung der EU zur künstlichen Intelligenz (KI). KI wird von der Kommission nicht als Selbstzweck verstanden, sondern als ein Instrument, das im Dienst der Menschheit und des öffentlichen Wohls steht. Im Juni 2018 setzte die Kommission eine Expertengruppe ein, die die Aufgabe hat, ethische Richtlinien für eine ‚vertrauenswürdige KI' zu entwickeln. Der im April 2019 veröffentlichte Abschlussbericht der Gruppe betont die Notwendigkeit, die menschliche Autonomie zu bewahren, Schaden von Menschen zu vermeiden und generell die Prinzipien der Fairness und Verständlichkeit zu berücksichtigen.[13] In ähnlicher Weise fordert der Europäische Rat die Einführung einer Bewertung der Auswirkungen der KI auf die Menschenrechte. KI-Systeme sollten verständlich und

[12]In Deutschland gibt es mit GAIA-X inzwischen konkrete Pläne, der deutschen und europäischen Industrie eine eigene europäische Datenplattform anzubieten, die nach deutschen Sicherheitsstandards und damit – so die Bundesregierung – „unter vertrauenswürdigen Bedingungen" funktioniert.

[13]European Commission (2019).

leicht abschaltbar sein (Council of Europe 2019a). Der Europarat fordert darüber hinaus, dass den technologiebedingten Machtverschiebungen in der Gesellschaft und dem Verhältnis zwischen Staat und Gesellschaft besondere Aufmerksamkeit geschenkt werden sollte.[14]

Der europäische Ansatz zur Regulierung der digitalen Gesellschaft spiegelt sich auch in wichtigen neueren EU-Rechtsakten zur digitalen Gesellschaft wider. Die Datenschutz-Grundverordnung (DSGVO)[15] setzt neue Standards für die Erhebung und Nutzung von Daten und ein angemessenes Gleichgewicht zwischen dem Schutz personenbezogener Daten und der Schaffung eines freien Datenverkehrs im Binnenmarkt. Auch die vom Rat im April 2019 verabschiedete Urheberrechtsrichtlinie[16] bringt europäische Werte zum Ausdruck. Sie schützt die Interessen von AutorInnen und KünstlerInnen vor der Verwertung durch die großen *Social-Media*-Plattformen, indem sie sie zur Zahlung fairer Gebühren verpflichtet. Sie sieht außerdem für öffentliche Interessen wie Online-Bildung und die Erhaltung und Verbreitung des kulturellen Erbes besondere Ausnahmen von ehrgeizigen urheberrechtlichen Bedenken vor.

Auch in der internationalen Politik verfolgt die EU einen wertebasierten Ansatz, der sich keinem einfachen Unilateralismus zuordnen lässt. Die Kommission betont das Prinzip der Anwenderneutralität und lehnt jede Diskriminierung aufgrund nationaler Herkunft ab. Es müsse anstelle dessen darum gehen, die Kontrolle des Datenverkehrs und eine transparente Softwarebereitstellung zu verbessern, Redundanzen in Mobilfunknetzen zu stärken, Rechenzentren zu dezentralisieren und Monokulturen in Netz- und Systemkomponenten zu vermeiden (Rühlig et al. 2019, S. 4 f.). Die kürzlich verabschiedete europäische Richtlinie zur Sicherheit von Netz- und Informationssystemen (NIS-Richtlinie) folgt diesem Weg bereits.[17] Sie fördert den Informations-

[14] „(P)articular attention should be paid to the significant power that technological advancement confers to those–be they public entities or private actors – who may use such algorithmic tools without adequate democratic oversight or control", Declaration by the Committee of Ministers on the Manipulative Capabilities of Algorithmic processes (Adopted by the Committee of Ministers on 13 February 2019 at the 1337th meeting of the Ministers' Deputies).

[15] Regulation on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (Data Protection Directive).

[16] (European Parliament und Council of the European Union 2019).

[17] (Das Europäische Parlament und Rat der Europäischen Union 2016).

austausch zwischen den Mitgliedstaaten, um eine rasche und wirksame operative Zusammenarbeit bei Cybersicherheitsvorfällen und den Austausch von Informationen über Risiken zu fördern. Die NIS-Richtlinie folgt damit der Idee einer Steigerung von Resilienz ohne unnötige Konfrontationen und Abschottungen aufzubauen.

Es gibt Stimmen, die diesen europäischen Weg „naiv“ nennen und befürchten, dass die hohen Standards der EU Wettbewerbsnachteile bedeuten. KonsumentInnen wollten effektive Produkte und wären nicht bereit, für anspruchsvolle Standards zu bezahlen. Wie zuvor schon beim Datenschutz stellt sich auch hier die Frage der Relevanz und Durchsetzungsfähigkeit europäischer Vorgaben: Muss Europa erst globaler Technologieführer werden, um sich anspruchsvolle lokale Standards leisten und diese auch international durchsetzen zu können? Die Realität spricht hier eine offensichtlich andere Sprache. Der Vorbildcharakter der Datenschutzgrundverordnung der EU für andere Staaten (so z. B. Japan, Brasilien und Kalifornien) und seine positive Bewertung seitens des Bundesdatenschutzbeauftragten kann als Beispiel für die Möglichkeit einer Bewahrung europäischer Werte bei gleichzeitiger Verfolgung einer Strategie der Verflechtung verstanden werden. Die Datenschutzgrundverordnung zielt darauf ab, Unternehmen auf einen sparsamen und die Privatheit respektierenden Umgang zu verpflichten. Sie ist damit erst einmal nur auf den europäischen Markt ausgerichtet und beansprucht keine Geltung für außereuropäische Räume. Gleichzeitig allerdings setzt die Datenschutzgrundverordnung Maßstäbe, die von vielen Unternehmen außerhalb Europas angewendet werden (Bendiek und Römer 2019, S. 37). Die Auswirkungen der Datenschutzgrundverordnung auf den US-amerikanischen Markt sind bereits heute für viele BeobachterInnen verblüffend. „Ironically, many Americans are going to find themselves protected from a foreign law” (Romm et al.2018). Die EU hat sich als die mächtigste Regulierungsbehörde des Silicon Valley herauskristallisiert: Sie ist dort eingetreten, „where Washington has failed or simply has been unwilling – to limit some of the United States’ most lucrative and politically influential companies” (ibid.). Der wesentliche Grund für diesen sogenannten „Brüssel-Effekt“ (Bradford 2012; Bendiek und Römer 2019) findet sich zuerst einmal darin, dass es für globale Unternehmen wie *Google, Facebook* oder *Amazon* weder eine Option ist, den europäischen Markt zu verlassen, noch ihr Geschäft nach zwei unterschiedlichen gesetzlichen Vorschriften zu organisieren. Die inhärente Mobilität von Daten erfordert de facto eine transnationale Regulierung, auch wenn dies auf einigen Märkten politisch nicht erwünscht ist. Es ist für Unternehmen oftmals weitaus kosteneffizienter, die anspruchsvollen europäischen Vorschriften auf globaler Ebene umzusetzen, als auf unterschiedlichen Märkten

mit unterschiedlichen Standards zu operieren. Im Ergebnis erweitert die EU de facto die territoriale Reichweite ihres Datenschutzrechts und stellt starke Anreize für ausländische Marktteilnehmer bereit, sich auch außerhalb der EU an das EU-Recht zu halten. Das Beispiel zeigt, dass in der globalen Produktregulierung die gleiche Logik gilt wie in der EU: Hohe Standards verdrängen niedrige Standards, wenn sie in relevanten Teilmärkten rechtsverbindlich sind (Vogel 2009, S. 250).

4 Europas interne digitale Souveränität

Souveränität, verstanden als die Fähigkeit, eigene normative Vorstellungen in einem umstrittenen internationalen Umfeld umzusetzen, ist in Europa nicht nur von externen, sondern auch von internen Vorbedingungen abhängig. Damit die EU machtvoll gegenüber Dritten auftreten kann, muss sie intern einig sein. Interne Einigkeit hat in Europa wiederum zumindest zwei Vorbedingungen, die von der Digitalisierung direkt betroffen sind und sich als die soziale und die kommunikative Herausforderung der Digitalisierung beschreiben lassen.

4.1 Die soziale Herausforderung der Digitalisierung

Ethische Richtlinien für den Datenschutz oder die Verwendung von künstlicher Intelligenz und anspruchsvolle Produktstandards sind von wesentlicher Bedeutung, um die globale Entwicklung anspruchsvoller digitaler Technologien im Einklang mit den politischen Werten und kulturellen Traditionen Europas zu halten. Sie sind eine notwendige Voraussetzung, um die soziale Akzeptanz einer potenziell disruptiven Technologie zu sichern. Ethische Richtlinien sind alleine jedoch nicht ausreichend. Der Aufstieg der digitalen Revolution und der künstlichen Intelligenz (KI) signalisiert eine zweite große Transformation des Kapitalismus mit erheblichen sozialen Auswirkungen, die nur mit der Industrialisierung vergleichbar sind. Es stimmt, dass niemand heute ihre zukünftige Bedeutung mit Sicherheit vorhersagen kann. Es stimmt aber auch, dass die künstliche Intelligenz zunehmend „lebenswichtig für alles“ (Franke 2019) wird. Die KI ermöglicht die Entwicklung selbstoptimierender Maschinen. Schon heute ist KI in der Lage, anspruchsvolle intellektuelle Aufgaben wie die Mustererkennung, Personalrekrutierungen, Finanzentscheidungen und vieles mehr zu vollführen. Die KI ersetzt den Menschen bei der automatisierten Entscheidungsfindung in Bereichen wie der Genehmigung von Krediten, der Ent-

scheidung, ob ein Kunde mit an Bord eines Flugzeugs genommen werden soll oder der Identifizierung von Korruption und Finanzkriminalität. Es überrascht nicht, dass in einer Reihe von Beiträgen über das langfristige Entstehen einer allgemeinen Intelligenz nachgedacht wird, die zumindest im Prinzip Probleme jeder Art aus eigener Kraft lösen kann: Autoren wie Chace argumentieren, dass die Fähigkeit der KI exponentiell wächst und in der Zukunft zwei „Singularitäten" hervorbringen könnte (Chace 2018).[18] Sich wiederholende, gefährliche und langweilige Arbeit würde von Maschinen erledigt werden, und kein Mensch in digitalisierten Gesellschaften würde für seinen Lebensunterhalt arbeiten müssen. Die neuen Technologien könnten zudem von einer starken Nachfrage nach Menschen mit Fachkenntnissen in Bereichen wie neuronalen Netzen und maschinellem Lernen begleitet werden. Es würden viele neue Jobs von App-EntwicklerInnen bis hin zu Cloud-Computing-IngenieurInnen, DesignerInnen von Nutzererfahrungen und DatenvisualisierungsexpertInnen entstehen, die es bis zu diesem Jahrhundert nicht gab. Eine aktuelle Studie des *World Economic Forum* (WEF) schätzt, dass bis 2025 die von Maschinen geleistete Arbeit von 29 % auf über 50 % steigen wird (Centre for the New Economy and Society 2018). In ähnlicher Weise schätzt das *McKinsey Global Institute,* dass etwa dreißig bis sechzig Prozent der Arbeitsplätze vollständig automatisiert werden können (Bughin et al. 2017).

Es ist jedoch bei weitem nicht sicher, dass die neuen Technologien zu besseren Lebensbedingungen für alle Menschen führen werden. Bereits heute ersetzen von KI angetriebene Maschinen eine große Anzahl an Menschen, die in ‚automatisierbaren' Berufen arbeiten, wie VerwaltungsassistentInnen, KundenbetreuerInnen, BuchhalterInnen, FahrerInnen, TelemarketerInnen, Fast-Food-Köche oder Köchinnen und PraktikantInnen und Elektro-/MaschinentechnikerInnen. Fahrerlose Autos und vollautomatisierte *Convenience Stores* ohne menschliche Kasse sind Realität. Sogar Menschen in anspruchsvolleren Berufen wie RadiologInnen, AnwältInnen und JournalistInnen werden allmählich ersetzt. Die KI lernt zunehmend, anspruchsvolle intellektuelle Aufgaben zu erfüllen, wie das Erkennen komplexer Muster, das Synthetisieren von Informationen, das Ziehen von Schlussfolgerungen und die Erstellung von Prognosen, von denen vor nicht allzu langer Zeit angenommen wurde, dass sie menschliche Kognition erfordern.

[18] „[T]he very real potential to democratize manufacturing, transforming how we make (unmake and remake) Things and empower billions of people to make what they consume" (Gershenfeld et al. 2017, S. 183).

Alle diese Entwicklungen werden nicht ohne Auswirkungen auf die Demokratie bleiben. Sinnhafte Beschäftigungen sind ein wesentliches Element für die subjektive Identifikation der Menschen mit der Gesellschaft, in der sie leben. Eine Gesellschaft, in der Menschen ökonomisch ‚überflüssig' werden, gerät schnell in Schwierigkeiten, den sozialen Zusammenhalt zu bewahren. Technische Innovationen wie die *Blockchain* und ausgeklügelte virtuelle Realitäten könnten es Unternehmen zudem ermöglichen, sich der Regierungsautorität zu entziehen, Firmengewinne in Offshore-Oasen zu deponieren und demokratische Regulierungen zu umgehen. Einige spekulieren bereits über das Entstehen eines Oligopols von Megakonzernen und DatenmilliardärInnen, die von Algorithmen geschaffenen Reichtum ernten und den Nachkriegskonsens einer sozial ausbalancierten Gesellschaft zerstören (Xiang 2018).

Es ist durchaus möglich, dass diese Spekulationen eher in den Bereich von Science-Fiction gehören. Sicher ist das aber nicht. Zahlreiche Studien des Weltwirtschaftsforums, der europäischen politischen Institutionen und der Vereinten Nationen beschreiben ihre Wahrscheinlichkeit. Um die sozialen und politischen Konsequenzen der digitalen Transformation zu glätten, muss Europa seine Sozialpolitik ausweiten und die wirtschaftlich schwächeren Mitgliedstaaten mit zusätzlichen Investitionen und Ausbildungsprogrammen sowie mit Mitteln für diejenigen unterstützen, die nicht in der Lage sind, ihren Rückstand aufzuholen. Andernfalls dürften nicht nur die sozio-ökonomischen Disparitäten, sondern auch die hiermit einhergehenden politischen Konflikte zwischen den Mitgliedstaaten der EU zunehmen. Die interne Dimension politischer Souveränität und die Fähigkeit zur Formulierung einer gesamteuropäischen politischen Position zu Fragen der Regulierung von KI, der Besteuerung US-amerikanischer Technologiekonzerne oder auch des Zugangs Chinas zum europäischen Markt würden hiervon mit hoher Wahrscheinlichkeit negativ betroffen werden.

4.2 Mediale Emanzipation in der digitalen Gesellschaft

Anspruchsvolle soziale Politiken entstehen nur selten ohne politische Mobilisierung der Betroffenen. Wie aber steht es um die Mobilisierungsfähigkeit Betroffener in der digitalen Gesellschaft? Hat die Idee der internen Souveränität unter den Bedingungen digitaler Vergesellschaftung eine realistische Perspektive? Aktuelle soziologische Analysen sind hier eher skeptisch und beschreiben eine generelle „Krise des Allgemeinen" (Reckwitz 2017). Der Einzelne würde sich zunehmend als egozentrischer Performer in einem Wettbewerb um Aufmerksamkeit präsentieren und habe nur noch wenig Bereitschaft zur Übernahme

von sozialer Verantwortung. Alte Klassen- und Gruppenidentitäten verlören mit dem Untergang des Industriekapitalismus an Prägekraft. An ihre Stelle träte ein neues Vergesellschaftungsmodell, das sich um so genannte „Neo-Communities" (Reckwitz 2017, S. 261) oder „Communities of Practice" (Stalder 2016, S. 135) organisiere. Felix Stalder beschreibt einen „vernetzten Individualismus", wonach „Menschen in westlichen Gesellschaften […] ihre Identität immer weniger über die Familie, den Arbeitsplatz oder andere stabile Kollektive definieren, sondern zunehmend über ihre persönlichen sozialen Netzwerke, also über die gemeinschaftlichen Formationen, in denen sie als Einzelne aktiv sind und in denen sie als singuläre Personen wahrgenommen werden" (Stalder 2016, S. 144). Diese neuen sozialen Gruppen weisen im Vergleich zur ehemaligen nationalstaatlichen Gesellschaft des Industriezeitalters einen sehr viel geringeren Verpflichtungsgrad gegenüber der nationalen Gemeinschaft auf. Es sind keine „Erinnerungs-, Erfahrungs- und Traditionsgemeinschaften" (Kielmannsegg 2003) mehr und auch keine tief ins kollektive Bewusstsein implantierten „imagined communities" (Anderson 1983). Die neuen partikularen Vergesellschaftungsformen sind vielmehr funktional ausgerichtet und üben nur solange Verbindlichkeit für ihre Teilnehmer *(User)* aus, wie sie vom Einzelnen anerkannt werden (vgl. auch Borucki und Oswald in diesem Band).

Die Idee einer von der digitalen Vernetzung beförderten Krise des Allgemeinen wird ebenfalls in den beiden verwandten Begriffen der Filterblase (Pariser 2012) und der Echokammer (Sunstein 2007) aufgegriffen. Eli Pariser und Cass Sunstein zufolge bricht der einst allumfassende öffentliche Raum in eine Vielzahl paralleler Echokammern auf, in denen jeder Einzelne sich nur noch solche DiskurspartnerInnen aussucht, die das Gleiche denken, die gleichen Vorlieben haben und die gleichen Interessen verfolgen. Der Prozess des öffentlichen Vernunftgebrauches, der ehemals die Vielzahl der unterschiedlichen Meinungen in der Demokratie immer wieder aufs Neue zusammengefügte und „Solidarität unter Fremden" (Brunkhorst 1997) schuf, degeneriere zu einer Vielzahl paralleler Diskursuniversen. Die Bewohner dieser partikularen Universen überzeugten sich nicht mehr von abweichenden Meinungen, sondern bestätigten nur noch ihre Vorurteile. Sie lebten in Filterblasen, in denen alles Abweichende und Irritierende ausgefiltert werde. Gemeinschaft entsteht hier nur noch unter Gleichen, ohne dass das Abweichende und Andere mitintegriert würde. In der Konsequenz, so die Befürchtung, bröckele der kommunikative Kitt gesamtgesellschaftlicher Verständigung und dünne sich die Identifikation von BürgerInnen mit der Gesellschaft insgesamt aus. Aus der ehemaligen nationalen Gemeinschaft werde so eine „dissonante Öffentlichkeit" (Knüpfer et al. in diesem Band) ohne übergreifende Verständigungsfähigkeit.

Der hier zum Ausdruck kommende Pessimismus über die Fähigkeit der digitalisierten Gesellschaft, interne Souveränität in Form von Verantwortung und Gemeinschaftsbewusstsein zu generieren, ist allerdings nicht unbestritten. Gerade die digitalaffine junge Generation zeichnet sich durch ein hohes Maß an politischem Aktivismus sowohl on- als auch offline aus. Der aktuellen Shell-Jugendstudie zufolge halten es mehr als ein Drittel aller Jugendlichen heute für wichtig, sich politisch zu engagieren; ein Wert, der höher ist als jemals zuvor in den letzten fast zwanzig Jahren. Der Protest gegen die Überwachungspraktiken der USA und ihrer europäischen Partner im Zuge der Enthüllungen des ehemaligen NSA-Mitarbeiters Edward Snowden, der Kampf gegen die Einführung von Upload-Filtern und für ein freies Internet bringen regelmäßig Millionen junger Menschen auf die Straße. Die Proteste gegen die Urheberrechtsrichtlinie haben in mehr als 80 Städten in ganz Europa Kundgebungen ausgelöst (Biselli 2019). Die Bewegung *Fridays for Future* hat am 15. Mai 2019 weltweit mehr als 1,7 Mio. DemonstrantInnen auf die Straße gebracht. In Deutschland erhielt ein politischer Videoclip 2019 des damals 27jährigen Rezo mit dem Titel *Die Zerstörung der CDU* mehr als 15 Mio. Klicks innerhalb von weniger als zwei Wochen.

Hier entwickelt sich eine neue Form interner politischer Souveränität an der Schnittstelle zwischen analoger und digitaler Welt. Viele analoge politische Praktiken werden durch Online-Aktivitäten überhaupt erst angeregt. Menschen, die nie für etwas gekämpft hätten, können eine geeignete Online-Community finden und so offline soziale Veränderungen und Solidarität fördern. Spezielle Plattformen für den lokalen Gebrauch wie *Ozeanhousing* oder *Nebenan* können die lokalen Beziehungen stärken. Eine ganz ähnliche Logik ist in der Teilhabe an der Entwicklung von *Open-Source-Software* sowie Projekten wie der *Wikipedia* oder *Open Data* zu beobachten. Stalder sieht hier das Potential für „eine radikale Erneuerung der Demokratie“ (Stalder 2016, S. 205). Kommunikationsintensive und horizontale Prozesse ließen sich mit den digitalen Technologien sehr viel effektiver organisieren als noch zuvor. Die ehemals an Koordinierungskosten scheiternde politische Organisation von Betroffenen werde zu einer konkreten Möglichkeit.

Die Digitalisierung ermöglicht ebenfalls eine neue Hinwendung zu Europa. BürgerInnen aus ganz Europa treffen sich heute bei #Europe, #EUelections, #GDPR und Hunderten von anderen Kommunikationsknoten auf *Twitter*. Sie können individuelle Portfolios von Nachrichten gestalten, kommentieren, mit anderen online diskutieren und damit zu einem aktiven ProsumentInnen für Nachrichten und Debatten werden (Toffler 1980; vgl. auch Borucki und Oswald in diesem Band). *Youtube, Twitter, Facebook* und viele Online-Vertriebskanäle

früherer Offline-Zeitungen beginnen das zu bilden, was in Europa in den letzten sechs Jahrzehnten fehlte: einen wirklich europäischen öffentlichen Raum, der weitaus lebendiger, vielfältiger und dynamischer ist als alles, was die europäische Demokratie bisher gesehen hat.

Benkler erklärt diesen Prozess der Fusion zwischen der alten Offline- und der neuen Online-Welt als „die Grunderfahrung, andere, auch Fremde, als potentielle Kooperationspartner zu behandeln (was, bdk/JN) zu einer Verdickung des Gefühls möglicher sozialer Bindungen über bloße Mitkonsumenten standardisierter Produkte hinaus beiträgt. Die Peer-Produktion kann eine neue Domäne mit relativ dichten Verbindungen zu anderen Menschen in der Ferne schaffen“ (Benkler 2006, S. 466 f.). Der Vermutung, dass soziale Medien eine Kultur der Singularitäten (siehe oben) angeregt haben könnten, werden empirische Belege entgegengehalten, die darauf hinweisen, dass soziale Medien von Vielen genutzt werden, um in Verbindung zu bleiben und sich zu informieren und eben nicht primär zur Selbstdarstellung genutzt werden (Alloway et al. 2014). Online-Kommunikation trägt zur Offline-Entwicklung von Vertrauen, Identität und Kooperation bei (Sherman et al. 2013). Die sozialen Medien sind somit zunehmend die Räume, in denen mächtige transnationale Interessengruppen politische Aktivitäten organisieren und in die analoge Welt hinausreichen, um Menschen und Entscheidungen zu treffen. Die Digitalisierung der Gesellschaft ist daher nur sehr verkürzt als eine Verringerung von Verantwortungsübernahme in der Gesellschaft zu verstehen. Sie erlaubt so sehr den Rückzug in private Welten der Selbstbezüglichkeit und des Narzissmus wie die Entwicklung aktiver ProsumentInnen in einer zunehmend offenen Gesellschaft (Alloway et al. 2014; Sherman et al. 2013; Vossen et al. 2016). Die grundlegende Erfahrung, andere, auch Fremde, als potenzielle KooperationspartnerInnen zu behandeln, trägt in der souveränen digitalisierten Gesellschaft dazu bei, eine über bloße Marktbeziehungen und die Selbstdarstellung hinausgehende neue Qualität sozialer Bindungen zu ermöglichen.

5 Komplexe digitale Souveränität als Integrationsaufgabe

Der Begriff der digitalen Souveränität dient in diesem Kapitel als begriffliche Orientierungshilfe für die Skizzierung wesentlicher Herausforderungen der digitalen Transformation und der Entwicklung von europäischen Antworten. Er

greift die durch die Digitalisierung induzierten veränderten internationalen und innereuropäischen Rahmenbedingungen auf und setzt sich von allen Souveränitätsverständnissen ab, die lediglich seine interne oder seine externe Dimension betonen. Digitale ‚komplexe' Souveränität ist sowohl für die rechtliche und die politische als auch die gesellschaftliche Dimension von Souveränität offen und bezieht diese auf die Frage nach der Handlungsfähigkeit Europas in einem herausfordernden Umfeld. Die Stärke dieses Begriffes ist seine Sensibilisierung für die vielfachen Herausforderungen, denen Europa heute in der digitalisierten Umwelt gegenübersteht. Er wirft ein Schlaglicht auf die disruptiven Auswirkungen digitaler Innovationen, des Aufstiegs der digitalen Megakonzerne und der Einführung von KI und stellt diese in den größeren europapolitischen Kontext. Die Europäische Union ist mit der Herausforderung konfrontiert, ihr Marktmodell so umzustellen, dass menschliche Arbeit nicht ersetzt, sondern ergänzt wird, dass die Autonomie der menschlichen Entscheidungsfindung nicht infrage gestellt wird und dass die internationalen Rahmenbedingungen eine innerstaatliche Entwicklung erlauben, die im Einklang mit den europäischen Werten steht. Die digitale Souveränität Europas wird von entscheidender Bedeutung dafür sein, ob das marktwirtschaftliche Modell seine soziale Kompetenz behalten und ob die liberale Demokratie und die europäische Integration ihre Glaubwürdigkeit als probate Instrumente auf dem Weg zu einer besseren Gesellschaft behalten werden. Beide beruhen auf Verfassungsprinzipien, die das Versprechen einer fairen Regelung für alle Bürgerinnen und Bürger in sich tragen. Ihre Legitimität hängt davon ab, dass sie nicht nur Innovationen, sondern auch ein solides Maß an sozialer Stabilität liefern. Wenn dieses Versprechen unplausibel wird, wird Europa einen Großteil seiner Legitimität verlieren. Die Rechtsstaatlichkeit, die Grundsätze der liberalen Demokratie und die Menschenrechte werden in einigen Mitgliedstaaten bereits heute infrage gestellt. Es ist nicht abwegig zu spekulieren, dass weitere gesellschaftliche Fragmentierungen die Kritik der Autoritären an der liberalen Ordnung und der digitalen Öffnung der europäischen Gesellschaften fördern werden. Europa wird seine politischen Ressourcen bündeln müssen, um innere Einigkeit zu erzielen und damit die Vorbedingungen externer digitaler Souveränität zu realisieren. In einer immer schneller zusammenwachsenden digitalen Welt lassen sich Innen- und Außenpolitik genauso wenig mehr voneinander trennen, wie die Technologie- und die Gesellschaftspolitik. Digitale Souveränität kann daher nur als komplexe Souveränität gedacht werden und stellt eine der zentralen Herausforderungen für den heutigen europäischen Integrationsprozess dar.

Literatur- und Quellenverzeichnis

Alloway, T., R. Runac, M. Qureshi, und G. Kemp. 2014. Is Facebook linked to selfishness? Investigating the relationships among social media use, empathy, and narcissism. *Social Networking* 3: 150–158.

Anderson, B. 1983. *Imagined communities: Reflections on the origin and spread of nationalism*. London: Verso.

Barlow, J.P. 1996. A declaration of the independence of cyberspace. *Electronic frontier foundation*. 8. Februar. https://www.eff.org/cyberspace-independence.

Beck, U. 1986. *Risikogesellschaft – Auf dem Weg in eine andere Moderne*. Frankfurt a. M.: Suhrkamp.

Becker, B. 2018. Your tax lady. *Politico*. Retrieved März 31, 2020, 6. November. https://www.politico.com/newsletters/morning-tax/2018/06/11/your-tax-lady-248338.

Bendiek, A., und M. Römer. 2019. Externalizing Europe: The global effects of European data protection. *Digital Policy, Regulation and Governance* 21 (1): 32–43.

Bendiek, A., und M. Schallbruch. 2019. Europas dritter Weg im Cyberraum – Der Beitrag der neuen Cybersicherheitsverordnung. *SWP Aktuell*. https://www.swp-berlin.org/10.18449/2019A60/.

Benkler, Y. 2006. *The wealth of networks. How social production transforms markets and freedo*. New Haven: Yale Univ Press.

Benner, T. 2010. Technological sovereignty: Blind rage against the US is not enough. *Global Public Policy Institute*. Abrufbar unter https://www.gppi.net/2015/02/01/technological-sovereignty-blind-rage-against-the-us-is-not-enough

Biselli, A. 2019. Upload-Filter: Alle Demos auf einen Blick. *Netzpolitik.org*. 1. März https://netzpolitik.org/2019/upload-filter-alle-demos-auf-einen-blick/.

BITKOM. 2015. Digitale Souveränität – Positionsbestimmung und erste Handlungsempfehlungen für Deutschland und Europa. *BITKOM*. https://www.bitkom.org/sites/default/files/file/import/BITKOM-Position-Digitale-Souveraenitaet.pdf.

Blum, S., M. Endreß, S. Kaufmann, und B. Rampp. 2016. Soziologische Perspektiven. In *Studien zur Resilienzforschung*, Hrsg. R. Wink. Wiesbaden: Springer Fachmedien Wiesbaden.

Bradford, A. 2012. The Brussels effect. *Northwestern University Law Review 107(1)*.

Brunkhorst, H. 1997. *Solidarität unter Fremden*. Frankfurt a. M.: Fischer Taschenbuch.

Bughin, J., E. Hazan, S. Ramaswamy, M. Chui, T. Alla, P. Dahlström, M. Trench. 2017. Artificial intelligence. The next digital frontier? *McKinsey Global Institute*. Juni. https://www.mckinsey.com/~/media/McKinsey/Industries/Advanced%20Electronics/Our%20Insights/How%20artificial%20intelligence%20can%20deliver%20real%20value%20to%20companies/MGI-Artificial-Intelligence-Discussion-paper.ashx.

Castells, M. 1996. *The network society. The information age: Economy, society and culture*, Bd. 1. Oxford: Blackwell.

Centre for the New Economy and Society. 2018. The Future of Jobs Report. *World Economic Forum*. https://www3.weforum.org/docs/WEF_Future_of_Jobs_2018.pdf.

Chace, C. 2018. *Artificial intelligence and the two singularities*. Boca Raton: Chapman & Hall.

Council of Europe. 2019a. Unboxing artificial intelligence: 10 steps to protect human rights. https://www.coe.int/en/web/commissioner/-/unboxing-artificial-intelligence-10-steps-to-protect-human-rights.

Council of Europe. 2019b. Declaration by the committee of ministers on the manipulative capabilities of algorithmic processes (adopted by the Committee of Ministers on 13 February 2019 at the 1337th meeting of the Ministers' Deputies). https://www.coe.int/en/web/artificial-intelligence.

Das Europäische Parlament, & Rat der Europäischen Union. 2016. Richtlinie (EU) 2016/1148 DES Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union. https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016L1148&from=EN.

Edwards, P.N. 2013. *A vast machine – Computer models, climate data and the politics of gobal warming (Infrastructures)*. Cambridge: MIT Press.

EUR-Lex. (n.d.). Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/EC.

Europ. Commission and Europ. External Action Serv. 2017. Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, JOIN(2017)250 final. 13. September.

European Commission. 2018. Artificial Intelligence for Europe – Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. *COM(2018) 237 final*.

European Commission. 2018. The hour of european sovereignty. 12. September https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-speech_en.pdf.

European Commission. 2019. Ethics guidelines for trustworthy AI. High-level expert group on artificial intelligence.

European Parliament, & Council of the European Union. 2019. DIRECTIVE (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC. 17 Mai https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0790

Farrell, H., und A. Newman. 2019. Weaponized interdependence: How global economic networks shape state coercion. *International Security* 44 (1): 42–49.

Franke, E. 2019. Harnessing Artificial Intelligence. In *Strategic Sovereignty: How Europe Can Regain the Capacity to Acr (ECFR Policy Brief, 2019)* Hrsg. M. Leonard und J. Shapiro, 49–60.

Friedman, T.L. 2007. *The world is flat: The globalized world in the twenty-first century*. London: Penguin Books.

Gershenfeld, N., A. Gershenfeld, und J. Gershenfeld-Cutcher. 2017. *Designing reality: How to survive and thrive in the third digital revolution*. New York: Basic Book.

Goldsmith, J., und T. Wu. 2008. *Who controls the internet. Illusions of a borderless world*. Oxford: Oxford University Press.

Gräf, E., H. Lahmann, P. Otto. 2018. Die Stärkung der digitalen Souveränität: Wege der Annäherung an ein Ideal im Wandel, Diskussionspapier von iRights.Lab. *Deutsches Institut für Vertrauen und Sicherheit im Internet – DIVSI*. Mai. https://irights-lab.de/wp-content/uploads/2018/05/Themenpapier_Souveraenitaet.pdf.

Grimm, D. 2009. *Souveränität. Herkunft und Zukunft eines Schlüsselbegriffs*. Berlin: Berlin Univ. Press.
Hillgruber, C. 2014. Die Souveränität der Staaten. *Der Staat* 53 (3): 475–493.
Hofmann, J., N. Kersting, C. Ritzi, und W.J. Schünemann (Hrsg.). 2019. *Politik in der digitalen Gesellschaft. Zentrale Problemfelder und Forschungsperspektiven*. Bielefeld: Transcript.
Ikenberry, G.J. 2018. The end of liberal international order? *International Affairs* 94 (1): 7–23.
Johnson, K., und E. Groll (n.d.). The Improbable Rise of Huawei – How did a private Chinese firm come to dominate the world's most important emerging technology? *Foreign Policy2019*. Retrieved Juli 7, 2019, https://foreignpolicy.com/2019/04/03/the-improbable-rise-of-huawei-5g-global-network-china/.
Karidi, M., M. Schneider, und R. Gutwald. 2018. *Resilienz. Interdisziplinäre Perspektiven zu Wandel und Transformation*. Wiesbaden: Springer.
Kaufmann, M. 2013. *Emergent Self-Organisation in Emergencies: Resilience Rationales in Interconnected Societies*, 53–68. Resilience: International Policies, Practices and Discourses.
Kielmannsegg, P. 2003. Integration und Demokratie. In *Europäische Integration*, Hrsg. M. Jachtenfuchs und B. Kohler-Koch, 49–84. Wiesbaden: Springer Fachmedien Wiesbaden.
Leonard, M. 2016. Interdependenz als Waffe. Die EU muss die Zeichen der geoökonomischen Zeit erkennen. *Internationale Politik*, 94–103 1. März.
Leonard, M., und J. Shapiro. 2019a. Empowering EU member states with strategic sovereignty. *European Council on Foreign Relations*. https://www.ecfr.eu/page/-/1_Empowering_EU_member_states_with_strategic_sovereignty.pdf.
Leonard, M., und J. Shapiro 2019b. Strategic sovereignty: How Europe can regain the capacity to act. *European Council on Foreign Relations*. https://www.ecfr.eu/publications/summary/strategic_sovereignty_how_europe_can_regain_the_capacity_to_act.
Marcus, J. 2019. What the Huawei battle tells us about US-China relations. *BBC News*. 25. Mai https://www.bbc.com/news/business-48397081.
Maus, I. 2011. *Über Volkssouveränität: Elemente einer Demokratietheorie*. Frankfurt a. M.: Suhrkamp.
Mueller, M. 2017. Will the internet fragment? Sovereignty, globalization, and cyberspace. Polity.
Nassehi, A. 2019. *Muster Theorie der digitalen Gesellschaft.* Beck.
Nye, J. 2011. *The future of power*. UK: Hachette.
Ohmae, K. 1995. *The end of the nation state: The rise of regional economies*. New York: Simon & Schuster.
Pariser, E. 2012. *Filter Bubble: Wie wir im Internet entmündigt werden*. München: Hanser.
Perrow, C. 1999. *Normal Accidents. Living with High-Risk Technologies*. Princeton: Princeton Paperbacks.
Reckwitz, A. 2017. *Die Gesellschaft der Singularitäten*. Berlin: Zum Strukturwandel der Moderne.
Rethinking Strategic Autonomy in the Digital Age. 2019. *European Commission – Strategic Note 30*. 18. Juli https://wayback.archive-it.org/12090/20191129072400/

https://ec.europa.eu/epsc/publications/strategic-notes/rethinking-strategic-autonomy-digital-age_en.

Romm, T., C. Timberg, und M. Birnbaum. 2018. Europe, not the U.S., is now the most powerful regulator of Silicon Valley. *The Washington Post*. 25. Mai. https://www.washingtonpost.com/business/technology/europe-not-the-us-is-now-the-most-powerful-regulator-of-silicon-valley/2018/05/25/f7dfb600-604f-11e8-8c93-8cf33c21da8d_story.html.

Rühlig, T., J. Seaman, und D. Voelsen. 2019. 5G and the US–China tech rivalry – A test for Europe's future in the digital age. *SWP Comment 29*. https://www.swp-berlin.org/10.18449/2019C29/.

Scharte, B., und K. Thoma. 2016. Resilienz – Ingenieurwissenschaftliche Perspektive. In *Multidisziplinäre Perspektiven der Resilienzforschung*, Hrsg. R. Wink, 123–150. Wiesbaden: Springer VS.

Schmitt, C. 1922. *Politische Theologie – Vier Kapitel zur Lehre von der Souveränität*. Berlin: Duncker & Humblot.

Sherman, L.E., M. Michikyan, und P.M. Greenfield. 2013. The effects of text, audio, video, and in-person communication on bonding between friends. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace,* 7 (2), *Article 3*. https://cyberpsychology.eu/article/view/4285/3330.

Snyder, J. 2019. The Broken Bargain – How nationalism came back. *Foreign Affairs*. https://www.foreignaffairs.com/articles/world/2019-02-12/broken-bargain.

Stalder, F. 2016. *Kultur der Digitalität*. Berlin: Suhrkamp.

Sunstein, C. 2007. *Republic.com 2.0.* Princeton Univ. Press.

SVR. 2017. Digitale Souveränität – Gutachten des Sachverständigenrats für Verbraucherfragen. https://www.svr-verbraucherfragen.de/wp-content/uploads/Gutachten_Digitale_Souver%C3%A4nit%C3%A4t_.pdf.

Timmers, P. 2019a. Ethics of AI and cybersecurity. *Minds & Machines* 29: 635–545.

Timmers, P. 2019b. Ethics of AI and cybersecurity when sovereignty is at stake. *Minds and Machines* 29: 1–11.

Toffler, A. 1980. *The third wave*. New York.

Virilio, P. 2009. Der integrale Unfall. In *Die Unordnung der Dinge. Eine Wissens- und Mediengeschichte des Unfalls*, Hrsg. C. Kassung. Bielefeld: Transcript.

Vogel, D. 2009. *Trading up: Consumer and environmental regulation in a global economy*. Cambridge: Harvard University Press.

Voss, A. 2020. Digital Autonomy. *The Parliament*. 17. März. https://www.theparliamentmagazine.eu/articles/opinion/digital-autonomy

Vossen, H., G.M. Valkenburg, und M. Patti. 2016. Do social media foster or curtail adolescents' empathy? A longitudinal study. *Computers in Human Behavior* 63: 118–124.

Wimmer, A. 2019. Why nationalism works. And why it isn't going away. *Foreign Affairs*, 27–35. https://www.foreignaffairs.com/articles/world/2019-02-12/why-nationalism-works

Wink, R. 2016. *Multidisziplinäre Perspektiven der Resilienzforschung*. Wiesbaden: Springer.

Xiang, F. 2018. AI will spell the end of capitalism. *The Washington Post*. 5. März.