Georg Glasze,
Eva Odzuck,
Ronald Staples (Hg.)

Was heißt digitale Souveränität?

Diskurse, Praktiken und Voraussetzungen »individueller« und »staatlicher Souveränität« im digitalen Zeitalter

[transcript] Politik in der digitalen Gesellschaft

Georg Glasze, Eva Odzuck, Ronald Staples (Hg.)
Was heißt digitale Souveränität?

Politik in der digitalen Gesellschaft | Band 3

Die freie Verfügbarkeit der E-Book-Ausgabe dieser Publikation wurde ermöglicht durch POLLUX – Informationsdienst Politikwissenschaft

und die Open Library Community Politik 2022 – einem Netzwerk wissenschaftlicher Bibliotheken zur Förderung von Open Access in den Sozial- und Geisteswissenschaften:

Vollsponsoren: Freie Universität Berlin – Universitätsbibliothek | Staatsbibliothek zu Berlin | Universitätsbibliothek der Humboldt-Universität zu Berlin | Universitätsbibliothek Bielefeld | Universitätsbibliothek der Ruhr-Universität Bochum | Universitäts- und Landesbibliothek Bonn | Staats- und Universitätsbibliothek Bremen | Universitäts- und Landesbibliothek Darmstadt | Sächsische Landesbibliothek Staats- und Universitätsbibliothek Dresden (SLUB) | Universitäts- und Landesbibliothek Düsseldorf | Universitätsbibliothek Frankfurt am Main | Justus-Liebig-Universität Gießen | Niedersächsische Staats- und Universitätsbibliothek Göttingen | Universitätsbibliothek der FernUniversität in Hagen | Staats- und Universitätsbibliothek Carl von Ossietzky, Hamburg | Gottfried Wilhelm Leibniz Bibliothek - Niedersächsische Landesbibliothek | Technische Informationsbibliothek (TIB Hannover) | Universitätsbibliothek Kassel | Universitätsbibliothek Kiel (CAU) | Universitätsbibliothek Koblenz · Landau | Universitäts- und Stadtbibliothek Köln | Universitätsbibliothek Leipzig | Universitätsbibliothek Marburg | Universitätsbibliothek der Ludwig-Maximilians-Universität München | Max Planck Digital Library (MPDL) | Universität der Bundeswehr München | Universitäts- und Landesbibliothek Münster | Universitätsbibliothek Erlangen-Nürnberg | Bibliotheks- und Informationssystem der Carl von Ossietzky Universität Oldenburg | Universitätsbibliothek Osnabrück | Universitätsbibliothek Passau | Universitätsbibliothek Vechta | Universitätsbibliothek Wuppertal | Vorarlberger Landesbibliothek | Universität Wien Bibliotheks- und Archivwesen | Zentral- und Hochschulbibliothek Luzern | Universitätsbibliothek St. Gallen | Zentralbibliothek Zürich

Sponsoring Light: Bundesministerium der Verteidigung | ifa (Institut für Auslandsbeziehungen), Bibliothek | Landesbibliothek Oldenburg | Ostbayerische Technische Hochschule Regensburg, Hochschulbibliothek | ZHAW Zürcher Hochschule für Angewandte Wissenschaften, Hochschulbibliothek

Mikrosponsoring: Stiftung Wissenschaft und Politik (SWP) - Deutsches Institut für Internationale Politik und Sicherheit | Leibniz-Institut für Europäische Geschichte

Die Reihe wird herausgegeben von Jeanette Hofmann, Norbert Kersting, Claudia Ritzi und Wolf J. Schünemann.

Georg Glasze, Eva Odzuck, Ronald Staples (Hg.)

Was heißt digitale Souveränität?

Diskurse, Praktiken und Voraussetzungen »individueller« und »staatlicher Souveränität« im digitalen Zeitalter

[transcript]

Die Forschungsgruppe »Diskurse & Praktiken digitaler Souveränität« wurde gefördert durch das EFI-Programm der FAU Erlangen-Nürnberg.

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Erschienen 2022 im transcript Verlag, Bielefeld

Umschlaggestaltung: Maria Arndt, Bielefeld
Lektorat: Katrin Viviane Kurten, geo-lektorat
Druck: Majuskel Medienproduktion GmbH, Wetzlar
Print-ISBN 978-3-8376-5827-9
PDF-ISBN 978-3-8394-5827-3
EPUB-ISBN 978-3-7328-5827-9
https://doi.org/10.14361/9783839458273
Buchreihen-ISSN: 2699-6626
Buchreihen-eISSN: 2703-111X

Gedruckt auf alterungsbeständigem Papier mit chlorfrei gebleichtem Zellstoff.
Besuchen Sie uns im Internet: *https://www.transcript-verlag.de*
Unsere aktuelle Vorschau finden Sie unter *www.transcript-verlag.de/vorschau-download*

Inhalt

Einleitung: Digitalisierung als Herausforderung – Souveränität als Antwort?

Konzeptionelle Hintergründe der Forderungen nach »digitaler Souveränität«

Georg Glasze, Eva Odzuck, Ronald Staples

Abstract *Ausgangspunkt der Einleitung sind die Problematisierungen von Digitalisierung, v.a. seit den 2000er-Jahren, welche Risiken digitaler Vernetzung betonen. Forderungen nach »digitaler Souveränität« reagieren auf diese Problematisierungen und greifen dabei auf ein neuzeitliches Konzept zurück, das mit Referenzen auf Eigenständigkeit und Abgrenzung noch vor wenigen Jahren vielfach als überkommen betrachtet wurde. Wir skizzieren daher zunächst eine Geschichte des Konzepts »Souveränität« und differenzieren dabei unterschiedliche Vorstellungen und Praktiken des »souveränen Staates« und des »souveränen Subjekts«. Forderungen nach Souveränität wurden und werden dabei von sehr unterschiedlichen Akteuren erhoben. So lässt sich zeigen, dass Souveränität einerseits mit emanzipativen Forderungen nach Selbstbestimmung verknüpft wurde, aber auch mit der Legitimation absoluter Herrschaft. »Souveränität« ist insofern ein zweischneidiges Schwert. Vor diesem Hintergrund betrachten wir es als Aufgabe der Geistes- und Sozialwissenschaften, im Dialog mit den Technikwissenschaften differenzierte Perspektiven auf Forderungen nach »(digitaler) Souveränität« herauszuarbeiten und damit Orientierungswissen für die gesellschaftliche Selbstverständigung im digitalen Zeitalter und für die Gestaltung der digitalen Transformation zu entwickeln. Die am Ende dieser Einleitung vorgestellten Beiträge dieses Bandes steuern dazu Perspektiven aus verschiedenen Disziplinen bei.*

1. Die neue Problematisierung von Digitalisierung

Der gesellschaftliche Blick auf die soziotechnischen Umbrüche, die als Digitalisierung bzw. richtiger als digitale Transformation beschrieben werden, hat

sich seit den 2000er-Jahren grundlegend verschoben – auch in Deutschland: Standen in den 1990er- und frühen 2000er-Jahren vielfach die *Möglichkeiten* einer potenziell universellen, digitalen Informationsverarbeitung (s. der Beitrag Benenson/Freiling/Meyer-Wegener 2022) und damit die gesellschaftlichen *Chancen* von neuen Vernetzungen sowie einer *Überwindung von Grenzen* im Fokus, so werden seit einigen Jahren vielmehr Risiken problematisiert. Neue Vernetzungen werden zunehmend als »*Entgrenzungen*« problematisiert. Neben Chancen und Möglichkeiten werden verstärkt »*Gefährdungen*«, »*Disruptionen*« und »*Abhängigkeiten*« betont (s. die historisch angelegte Diskursanalyse von Dammann/Glasze 2022 in diesem Band29).

Forderungen nach »digitaler Souveränität« reagieren auf diese Problematisierungen und greifen dabei auf ein neuzeitliches Konzept zurück, das mit Referenzen auf *Eigenständigkeit* und *Abgrenzung* noch vor wenigen Jahren zumindest teilweise als überkommen betrachtet wurde. Dabei lassen sich verschiedene Begriffsverwendungen differenzieren: einerseits Bezüge auf das Konzept des souveränen Staates und andererseits Bezüge auf das Konzept des souveränen Subjekts. Daneben wird der Begriff teilweise auch im Hinblick auf nicht staatliche Organisationen verwendet – also kollektive Akteure wie Unternehmen, zivilgesellschaftliche Organisationen oder Kommunen.

Vor dem Hintergrund der vielschichtigen und teilweise vehement vorgebrachten Forderungen nach »digitaler Souveränität« bietet der vorliegende Sammelband Angebote zur Systematisierung und Klärung aus verschiedenen wissenschaftlichen Disziplinen. Hervorgegangen ist der Band aus den Diskussionszusammenhängen in der interdisziplinären Forschungsinitiative »Diskurse und Praktiken digitaler Souveränität«, die 2019–2022 durch eine Anschubfinanzierung im »*Emerging Fields*«-Programm der FAU Erlangen-Nürnberg gefördert worden ist.

Diese Einleitung wirft dabei zunächst einen Blick auf die Geschichte des Begriffs »Souveränität«. Dabei wird deutlich, dass der Begriff kein einheitliches Konzept vermittelt, sondern in verschiedenen gesellschaftlichen Konstellationen und von verschiedenen Akteuren unterschiedlich verwendet wurde und wird. Die Verwendung des Begriffs ist daher selbst politisch (vgl. im Hinblick auf die staatstheoretische Debatte so bereits auch Schmitt 2008 [1922]: 25). Wir skizzieren im ersten Schritt, wie sich Konzepte und politische Praktiken souveräner Staatlichkeit entwickelt haben, bevor wir im zweiten Schritt danach fragen, wie eine Geschichte des Konzepts individueller Souveränität skizziert und dabei auch die Übertragung auf *kollektive* Akteure eingeordnet werden kann. Eine solche Perspektive hilft, die vielfältigen Funktionen des Be-

griffs »Souveränität« in den zeitgenössischen Forderungen nach einer »digitalen Souveränität« zu verstehen, und rahmt die disziplinären Beiträge im Sammelband, die wir am Ende dieser Einleitung vorstellen.

2. Eine kurze Geschichte des Konzepts »Souveränität«

2.1 Der »souveräne Staat« als neuzeitliches Konzept

Souveränität ist ein neuzeitliches Konzept, das vielfach als Übertragung bzw. »Säkularisierung« der christlichen Vorstellung eines allmächtigen Gottes auf weltliche, d.h. gesellschaftliche Verhältnisse interpretiert wurde (vgl. bspw. Derrida/Roudinesco 2006: 156; Schmitt 2008 [1922]; Klein 2016). In der neuzeitlichen Staatstheorie entwickelt sich in den Religionskriegen des 16. und 17. Jahrhunderts eine Konzeption von Souveränität als eine dem Staat und seinen Repräsentant*innen eigentümliche, höchste, allumfassende, nach außen und innen unbeschränkte Hoheitsgewalt über ein bestimmtes Territorium. Die Territorialität liefert erstens dabei die Grundlage für die Unterscheidung *einer Außendimension und einer Innendimension* des Souveränitätsbegriffs: Nach außen bezeichnet »Souveränität« hier eine Gleichrangigkeit souveräner Staaten im Völkerrecht – vor allem das Recht, selbst über Bündnisse, Außenpolitik und Krieg zu befinden. Nach innen bedeutet Souveränität hierbei rechtliche und politische Hoheitsgewalt, d.h. das Recht, Recht zu setzen, und das Recht und die Fähigkeit, alle auf dem Territorium lebenden Personen diesem Recht zu unterwerfen – notfalls mit Gewalt (vgl. zur Begriffsbestimmung Kiersch 1977). Selbstbestimmung über die inneren Angelegenheiten eines Staates ist dabei angewiesen auf die Freiheit von Fremdbestimmung in den Außenbeziehungen (vgl. Grimm 2009: 11). Deutlich wird an dieser Bestimmung zweitens, dass Souveränität in *eine Rechtsdimension und eine Machtdimension* zerfällt: das Recht zu souveräner Herrschaft einerseits und die Fähigkeit bzw. Macht zu souveräner Herrschaftsausübung andererseits. Betrachtet man holzschnittartig einige zentrale Entwicklungspunkte des modernen Souveränitätskonzepts, dann wird drittens deutlich, dass die Rechtsdimension des Souveränitätsbegriffs in praktisch-politischer Absicht sowohl zur *Begründung neuer als auch zur Ausweitung, Kritik oder Einhegung bestehender Machtverhältnisse* verwendet werden kann: Im 14. Jahrhundert wurden mit dem Souveränitätsbegriff Herrschaftsstrukturen von Kirche und Reich durch Städte und Fürsten zurückgewiesen. Die erste systematische Behandlung des neuzeitlichen Sou-

veränitätskonzepts in Jean Bodins *Six livres de la République* (1576) ist wiederum vor dem Konflikt zwischen Fürsten und König zu sehen – wobei Bodin klar Position für die Stärkung der Herrschaft des Königs bezieht. Souveränität umfasst bei ihm die folgenden Merkmale (vgl. Voigt 2016: 2):

a) Recht, über Krieg und Frieden zu entscheiden,
b) letztinstanzliche Gerichtsbarkeit,
c) Recht, Amtsträger ein- und abzusetzen,
d) Besteuerungsrecht,
e) Begnadigungs- und Dispensierungsrecht,
f) Recht, den Geldwert zu bestimmen,
g) Recht, einen Eid zu fordern.

Während bei Bodin der Herrscher in eine naturrechtliche Ordnung eingebunden war, löst ein weiterer zentraler Theoretiker des neuzeitlichen Souveränitätsgedankens – der englische Staatsphilosoph Thomas Hobbes – diese Begrenzung der Souveränität weiter auf: Als Ausleger des Naturrechts kann der Souverän bei Hobbes weitgehend selbst entscheiden – es ist die Autorität und nicht die Wahrheit, die Gesetze macht: »Auctoritas non veritas facit legem«, schreibt Hobbes im *Leviathan* (1651). Der Souverän ist weitgehend herausgelöst aus Bindungen und Verpflichtungen und besitzt unbeschränkte Gesetzgebungskompetenz *(legibus absolutus)*.

In der realpolitischen Entwicklung gilt der Westfälische Frieden von 1648 als Geburtsstunde des modernen Territorialstaates und als Durchbruch des modernen Souveränitätsdenkens. Durch den Vertrag wird der 30-jährige Krieg (1618–48) beendet und die Souveränität der europäischen Fürsten und deren Recht auf Kriegsführung anerkannt. Gegen die Idee der *unumschränkten* Fürstenherrschaft wird in der Zeit der Aufklärung die Idee der Volkssouveränität gerichtet. Die ideengeschichtliche und die realpolitische Entwicklung laufen dabei nicht immer parallel, weil Ideen der Volkssouveränität lange schon gedacht und vorbereitet wurden, bevor diese dann ihren exemplarischen Ausdruck in der französischen Revolution 1789 finden. Auf Hobbes, der mit seiner Vertragstheorie den Gedanken ausdrückte, dass sich Herrschaft vor dem als rational und frei begriffenen Individuum zu rechtfertigen hat, folgte ideengeschichtlich Locke (1632–1704), der in seiner Vertragstheorie die gesetzgebende Gewalt nicht als Souverän, sondern als *trustee* des Volkes bezeichnet. Rousseau kann in dieser Entwicklungslinie als zentraler Vordenker der Idee der »Volkssouveränität« begriffen werden, der gegen Locke

einwendet, dass die Souveränität nicht repräsentiert werden kann. Die gesetzgebende Gewalt, die in Demokratien beim Volk liegt, wird in liberalen Demokratien durch Prinzipien des Konstitutionalismus, Grundrechtsgarantien und Gewaltentrennung begrenzt und flankiert – was mancherorts zur These führte, der demokratische Verfassungsstaat kenne keinen Souverän mehr, bzw. was zur typologischen Unterscheidung von Volkssouveränität und Verfassungssouveränität führte (vgl. für einen Überblick Voigt 2016).

Bereits der kurze Blick auf die Geschichte des Begriffs »Souveränität« als staatstheoretischem Konzept offenbart also dessen *Funktionalität in sehr unterschiedlichen Kontexten*. Eine gegenwartsbezogene Auseinandersetzung mit Souveränität kann daher nicht sinnvoll als Auseinandersetzung mit einem vermeintlich gegebenen Wesenskern des Begriffs organisiert werden, sondern muss vielmehr sensibel für die verschiedenen politischen Funktionalisierungen und damit für die vielfältigen Forderungen und Ziele sein, die mit Souveränität verknüpft werden (vgl. dazu auch bereits Krasner 2001; Coleman 2009; Barkan 2015).[1]

Die mit dem Begriff der Souveränität erhobenen Forderungen und legitimierten Praktiken stehen zudem immer in einem Verhältnis zu historisch und geographisch *spezifischen soziotechnischen und soziomateriellen Kontexten*: So haben verschiedene Autor*innen darauf hingewiesen, dass die Durchsetzung von Konzept und Praxis moderner, staatlich-souveräner Herrschaft in der europäischen Neuzeit nicht zuletzt mit spezifischen Techniken der Erfassung und Verwaltung von Territorium und Bevölkerung verknüpft waren, die sich im späten 18. sowie dann v.a. im 19. Jahrhundert durchgesetzt haben: insbesondere die Entwicklung der exakt-vermessenden Kartographie und der Statistik (vgl. Hannah 2000; Elden 2013; Branch 2014). Ende der 1990er- und zu Beginn der 2000er-Jahre weisen zahlreiche Autor*innen darauf hin, dass im Kontext von Globalisierung und Digitalisierung der Nexus von staatlicher Herrschaft und Territorium herausgefordert werde und sich die *infrastructural power* des territorial organisierten Staates auflöse (vgl. Sassen 1996; Agnew 2005). Schlagworte vom »Ende des Nationalstaats« (vgl. bspw. Panić 1997; Dittgen 1999) oder einer »Postsouveränität« (vgl. MacCormick 1993; Gümplová 2015; Klein 2016) wurden laut. Vor diesem Hintergrund wurde vielfach ein Verlust an staatlicher Steuerungsfähigkeit und damit letztlich staatlicher

1 »So wenig ›Souveränität‹ daher einen überzeitlichen Sinn beanspruchen kann, sowenig handelt es sich um einen überörtlich gleichbleibenden Begriff. Vielmehr ist damit zu rechnen, dass sein Inhalt auch von Land zu Land wechselt.« (Grimm 2009: 9)

Souveränität konstatiert (August 2021). Mit der Etablierung supranationaler Organisationen und der Übertragung von Hoheitsrechten an diese Organisationen verbanden sich diesbezüglich Hoffnungen auf eine Wiedergewinnung von Steuerungsfähigkeit im Sinne einer *gobal governance* (vgl. Grimm 2009: 9).

Zu Beginn der 2020er-Jahre hat sich allerdings die Debattenlandschaft radikal verändert: In zahlreichen Kommentaren wird ein »Ende der Globalisierung« (vgl. bspw. Löw et al. 2021) sowie eine »Wiederkehr des Nationalstaates« (vgl. Engelbrekt et al. 2020) konstatiert bzw. eingefordert. Ansprüche zur Wiedergewinnung staatlicher Souveränität werden zahlreicher und scheinen politische Auseinandersetzungen oftmals zu bestimmen (vgl. dazu auch Agnew 2020).[2] Die Debatte um »digitale Souveränität« muss daher auch als Element sich verändernder politischer Diskurse zu Staatlichkeit und globalen politischen Ordnungen verstanden werden (s. dazu auch Abschnitt 3).

2.2 Das »souveräne Subjekt« als neuzeitliches Konzept

Wie bereits zu Beginn des Beitrags angedeutet, beziehen sich zahlreiche Forderungen nach »digitaler Souveränität« – insbesondere in der Debatte in Deutschland – nicht (nur) auf staatliche Souveränität, sondern vielfach auf eine Souveränität von Individuen sowie ggf. auch nicht staatlichen Organisationen, also handlungsmächtigen kollektiven Akteuren. Ein solches Konzept von selbstbestimmten Subjekten als souverän kann ebenfalls als ein dezidiert neuzeitliches Konzept verstanden werden (vgl. Reckwitz 2006; Behrens 2021). In gewisser Weise kann die neuzeitliche Vorstellung von Staaten als eigenständig, einheitlich und quasikörperlich abgegrenzt, wie wir sie oben rekonstruiert haben, damit als Übertragung der Vorstellung des körperlichen und selbst-bestimmten Subjekts interpretiert werden (vgl. dazu Coleman 2009; zur Ikonographie des souveränen Staates als Körper, bspw. bei Hobbes, vgl. Bredekamp 2003 – grundsätzlich vgl. bspw. Melzer/Norberg 1998; Skinner 2012; Münkler 2016): Der Staat wird beispielsweise bei Hobbes als *artificial man* betrachtet, der Wille des Souveräns ist Gesetz, das den *politischen Körper* bewegt. Die Metaphorik verweist auf einen engen Zusammenhang zwischen

2 Der kanadische Historiker und Politikwissenschaftler Ignatieff hat bereits 2012, vor dem Hintergrund der globalen Finanzkrise und den damit verbundenen Erschütterungen neoliberaler Leitbilder, in einem Rezensionsartikel einen »return of sovereignity« vorhergesagt.

dem Selbstbestimmungsrecht des als Quasiperson begriffenen Staates und dem Selbstbestimmungsrecht des Individuums: Hobbes' Vertragstheorie liegt die Idee des freien, selbstbestimmten Subjekts, das in Form eines freien, wechselseitigen Vertrags und damit durch seine individuelle, freiwillige Zustimmung eine staatliche Autorität erst schafft, zugrunde. Für die Tradition des europäischen Liberalismus ist die Idee individueller Souveränität zentral – also die Idee von individuellen Rechten und Grenzen, die der Staat nicht verletzen dürfe. So führt beispielsweise John Stuart Mill in seiner Schrift über die Freiheit, in der er das Schädigungsprinzip als Kriterium für legitimen staatlichen Zwang einführt, aus: »In dem Teil, der nur ihn selbst berührt, ist seine Unabhängigkeit im rechtlichen Sinn absolut. Über sich selbst, über seinen eigenen Körper und Geist, ist das Individuum souverän.« (Mill 1969: 17)

Eng verbunden mit einem derart auf das Individuum bezogenen Souveränitätsbegriff ist im moralischen und politischen Denken der Moderne der Begriff der Autonomie – der die Idee der Selbstbestimmung bzw. der Selbstgesetzgebung transportiert. Im Allgemeinen wird darunter eine Fähigkeit verstanden, moralische Prinzipien zu erkennen und auf sich selbst anzuwenden – eine Fähigkeit, die entsprechende Akteure moralisch verantwortlich macht, aber umgekehrt auch Achtung vor solchen moralfähigen Akteuren gebietet und zudem paternalistischen Eingriffen (auch solchen des Staates) enge Grenzen setzt. Im politischen Kontext bezeichnet Autonomie die Fähigkeit der Bürger*innen, die Regeln des Zusammenlebens selbst zu bestimmen (vgl. auch Christman 2008). Liberale Gerechtigkeitstheorien gehen in der Tradition des Gesellschaftsvertrags davon aus, dass sich staatliche Herrschaft vor dem Subjekt, das als frei, gleich und autonom begriffen wird, zu rechtfertigen hat – und dass liberale Staaten Integritätsrechte und die Privatsphäre von Individuen anerkennen und schützen müssen. Allerdings wurde an der Idee des autonomen Subjekts bzw. des liberalen Individuums bereits seit seiner Etablierung auch z.T. vehemente Kritik geübt: Seit der zweiten Hälfte des 20. Jahrhunderts bemängelten u.a. kommunitaristische und feministische Theorien die vermeintlich »hyperindividualistischen« Prämissen und Konsequenzen der Idee des liberalen Akteurs, und identitätspolitische Ansätze warnen vor den potenziell ausschließenden Effekten solcher abstrakten Konzepte der autonomen Person (vgl. Christman 2008: 101).

Unter dem Label »Poststrukturalismus« finden sich ab den 1960er-Jahren theoretische Ansätze, die ein autonomes Subjekt radikal infrage stellen. Es wird als eine Konstruktionsleistung oder gar historische Fiktion der modernen Gesellschaft beurteilt. Michel Foucault sieht das moderne Subjekt beispiels-

weise als Ergebnis von modernen Wissensordnungen und damit letztlich als eine »Erfindung« (1971 [1966]). Er weist darauf hin, dass die neuzeitlichen Vorstellungen von und Ansprüche an Autonomie letztlich uneinlösbar sind, da immer Machtverhältnisse vorgeschaltet sind, die das jeweilige historische Subjekt erst ermöglichen. Gegenwärtig wird vor allem in den *science and technology studies* um einen adäquaten Subjektbegriff gerungen[3]. Vor dem Hintergrund einer technisch durchdrungenen und in radikal gesteigerter Weise von Technik abhängigen Gesellschaft stellt beispielsweise die *actor network theory* die etablierte Vorstellung infrage, dass alleine der Mensch handlungsfähiges Subjekt sei, und betont die Verwobenheit der menschlichen Akteure in eine Vielzahl von weiteren nicht menschlichen Aktanten (vgl. Callon 1984; Latour 2007).

2.3 Vielschichtige Forderungen nach Souveränität – auch jenseits von Staat und Subjekt

Die Idee des souveränen Akteurs wurde jedoch nicht nur auf den Staat übertragen, sondern findet Anwendung auf ganz unterschiedliche nicht staatliche kollektive Akteure und Organisationen. Feindt, Gissibl und Paulmann haben 2021 vorgeschlagen, diese Vervielfältigung, Dezentrierung und Dynamisierung von Souveränitätsforderungen heuristisch mit dem Konzept einer »kulturellen Souveränität« zu fassen.

Dabei wird einerseits eine (zu) große Machtfülle nicht staatlicher Akteure kritisiert und diese als »neue Souveräne« problematisiert: so beispielsweise multinationale Konzerne (vgl. George 2015) oder die neuartigen Plattformunternehmen des digitalen Zeitalters (vgl. Grumbach/Zanin 2022). Gleichzeitig werden Ansprüche auf Selbstbestimmung im Namen von Organisationen mit dem Schlagwort der Souveränität verknüpft, wenn z.B. im Namen von Städten wie Berlin, Barcelona und Amsterdam[4] oder von Unternehmen selbst mehr »digitale Souveränität« gefordert wird. Die Souveränitätsansprüche haben dabei ganz unterschiedliche Reichweiten.

3 Dazu gehört auch eine seit den 1980ern geführte Auseinandersetzung von postfeministischer Seite, wie spätmoderne Akteurskonzepte aussehen können. Donna Haraways Arbeiten zu Cyborgs (1985) sind hier diskursstiftend gewesen.

4 Siehe den Zusammenschluss: https://citiesfordigitalrights.org/cities; 15.06.2022.

Als Kommune ist in Deutschland beispielsweise die Stadt München bekannt geworden mit ihrem Plan, die Verwaltung aus der Abhängigkeit von Microsoft-Produkten zu lösen und auf Linux-Anwendungen zu wechseln. 2020 wurde dieses Vorhaben allerdings rückabgewickelt – mit dem Hauptargument, dass spezielle Fachanwendungen immer parallel unter Windows gelaufen sind und Standardsoftwareprodukte die notwendige Voraussetzung sind zur Erfüllung der kommunalen Aufgaben[5]. Barcelona hat hingegen eine breit angelegte Digitalstrategie entwickelt. Kernbestandteil ist, dass Daten, die in der Verwaltung der Stadt anfallen, Daten der Bürger*innen sind und ihre Verwendung auch diesen (der Stadtentwicklung) zugutekommen sollen. Zusätzlich gibt es eine digitale Bildungsoffensive, eine weitreichende Mitbestimmungsplattform und eine Offensive zur Ansiedlung von Digitalwirtschaft (vgl. Lynch 2020). Datensouveränität spielt in beiden genannten Fällen eine Rolle, wobei es in München »nur« um die Verwaltungsinfrastruktur geht und in Barcelona um ein umfängliches Konzept, in welchem möglichst alle Stakeholder der Stadtgesellschaft partizipieren sollen.

Unternehmenszusammenschlüsse wie die des Branchenverbands der deutschen IT-Wirtschaft Bitkom haben »digitale Souveränität« zu einer zentralen Agenda ihrer Lobbyarbeit gemacht. Umfragen des Leibniz-Zentrums für Europäische Wirtschaftsforschung weisen zudem darauf hin, dass Fragen der Datenhoheit und der als zu groß empfundenen Abhängigkeit von anderen (v.a. asiatischen und US-amerikanischen Unternehmen) von zahlreichen Unternehmen als problematisch beschrieben werden. Gleichzeitig bauen allerdings neue Konzepte wie »Industrie 4.0« oder das »Internet of things« auf einer systematischen Vernetzung von datenproduzierenden Gegenständen auf, auch über Organisations- und Ländergrenzen hinweg. Souveränitätsforderungen, die einer eher traditionellen Semantik der abgeschlossenen Organisation nach außen folgen, stoßen hier an ihre Grenzen, wie beispielsweise im Open Innovation Paradigm gezeigt wird (vgl. Chesbrough 2003; s. dazu auch den Beitrag von Fritzsche 2022 in diesem Band).

5 Siehe hierzu die Berichterstattung in Publikumsmedien: https://www.zdnet.de/88288011/limux-muenchen-gibt-open-source-projekt-auf/oder auch https://www.spiegel.de/netzwelt/apps/muenchen-beendet-linux-experiment-a-1134670.html; 15.06.2022.

3. Souveränität als »produktiver Mythos« und die Frage seiner Gestaltung

Der Begriff »Souveränität« wird in der Neuzeit also vielfach verknüpft mit der Vorstellung von Autonomie bzw. Selbstbestimmung von Staaten, Individuen und teilweise auch nicht staatlichen kollektiven Akteuren. Allerdings wurden sowohl die Vorstellung eines souveränen, klar territorial definierten Staates mit einem vollständigen Gewaltmonopol nach Innen und einem von Nichteinmischung und Gleichheit geprägtem Außenverhältnis als auch die Vorstellung eines vollständig souverän-selbstbestimmten Subjekts, also Vorstellungen absoluter Souveränität, seit Mitte des 20. Jahrhundert in den Sozial- und Kulturwissenschaften als Mythos dekonstruiert (vgl. bspw. für staatliche Souveränität Krasner 2001; für das autonome Subjekt s. zusammenfassend Meißner 2014).[6]

So läuft die Vorstellung von Souveränität als einer Art absoluter Autonomie Gefahr, die *relationale Einbettung* jeglicher Handlungsfähigkeit auszublenden: Staatliche Herrschaft muss letztlich immer in Relation zu anderen Staaten, weiteren Akteuren und soziotechnischen Verhältnissen gedacht werden und lässt sich vielfach nicht eindeutig in eine Innen- und Außendimension unterscheiden. Und auch die Handlungsfähigkeit von Subjekten kann letztlich nur abhängig von der jeweiligen Einbettung in soziale und soziotechnische Beziehungen konzeptualisiert werden (so bspw. auch die kritische Debatte zur Konzeption von Privatheit und Subjekt im digitalen Zeitalter, vgl. Williams 2005; Weinberg 2017; Berger et al. 2021 und Lamla et al. 2022).

Vor dem Hintergrund dieser Kritik hat sich der wissenschaftliche Blick zunächst auf die Analysen der vielfältigen und vielstimmigen *Forderungen* nach Souveränität gerichtet sowie auf die damit verbundenen Auseinandersetzungen. Gleichzeitig gibt es jedoch auch Stimmen aus der Wissenschaft, welche die Vorstellungen des *souveränen Staates* auch im Kontext der Herausforderungen einer vernetzten Welt als eine letztlich unverzichtbare *normative Orientierung* beurteilen, da dieser »gerade durch seine kontrafaktische Behauptung eine politische Ordnung aufrechterhält« (Münkler/Straßenberger

6 In ähnlicher Weise lassen sich Vorstellungen souveräner Organisationen hinterfragen: So sind Organisationen vielfach in hohem Maße vernetzt – neue digitale Geschäftsmodelle benötigen beispielsweise systematische Vernetzung konstitutiv. Eine Orientierung an Vorstellungen von Souveränität als Autonomie erscheint daher vielfach paradox (s. dazu auch den Beitrag von Fritzsche 2022).

2016: 125). Dabei wird darauf verwiesen, dass Fragen einer angemessenen demokratischen Legitimation, des Konstitutionalismus und der Gewaltenteilung zumindest bislang nicht überzeugend ohne das Prinzip des souveränen, territorial gefassten Staates umgesetzt werden (vgl. Gümplová 2015). In ähnlicher Weise scheint das Operieren vieler gesellschaftlicher Teilbereiche geradezu darauf angewiesen zu sein, sich *normativ* an der Vorstellung eines *souveränen Subjekts* zu orientieren – d.h. eines Subjekts, dem Handlungsursachen zugerechnet werden können (bspw. als ökonomischer Akteur, als Träger*in individueller Bürger- oder Menschenrechte oder als Adressat bei der rechtlichen Sanktionierung von Straftaten).

In der politischen Praxis werden seit den 2010er-Jahren in ganz verschiedenen politischen Lagern Forderungen nach *mehr* staatlicher Souveränität prominent: So verknüpfen in zahlreichen Ländern rechtspopulistische Bewegungen Forderungen nach »mehr nationaler Souveränität« erfolgreich mit national-exkludierenden und autoritären Politiken (kritisch dazu im Kontext der Brexit-Debatte vgl. bspw. Agnew 2020). Gleichzeitig gibt es aber auch Bestrebungen von emanzipativ orientierten Bewegungen, das Konzept »nationaler Souveränität« im Sinne einer Re-Politisierung und demokratischen Legitimierung von Entscheidungsprozessen auszudeuten (vgl. Mitchell/Fazi 2017).

Der »Mythos Souveränität« (wenn man diese Bezeichnung teilen möchte) war und ist also durchaus produktiv – und dies in einer zweischneidigen Weise: So lässt sich zeigen, dass Souveränität einerseits mit emanzipativen Forderungen nach Selbstbestimmung und letztlich demokratisch legitimierter Herrschaft verknüpft wurde und wird – andererseits aber auch mit der Legitimation absoluter, autoritärer und nur territorial begrenzter Herrschaft (in diesem Sinne problematisiert Thiel 2021 auch die Verwendung von »digitaler Souveränität«; s. dazu auch die frühe und intensive Verwendung des Begriffs durch die Eliten autoritär regierter Staaten wie China und Russland). So scheint es von zentraler Bedeutung für die weitere Debatte um »digitale Souveränität« zu sein, Fragen der demokratischen Legitimation ins Blickfeld zu nehmen (vgl. dazu bspw. den Beitrag von Odzuck 2022). Für die Ebene individueller Subjekte sowie nicht staatlicher Organisationen knüpft der Begriff unmittelbar an neuzeitliche Konzepte von individueller und kollektiver Selbstbestimmung und von Grundrechten an – und bietet in diesem Sinne Orientierung. Gleichzeitig ist aber zumindest fraglich, ob die Orientierungen an Vorstellungen des selbstständigen Subjekts bzw. der autonomen Organisation in einer hochgradig soziotechnisch vernetzten Gegenwart nicht um stärker re-

lationale Konzepte ergänzt und erweitert werden müssen (zum Begriff einer relational gedachten Souveränität s. Stacy 2003 sowie die Beiträge von Müller/Kammerl 2022; Leyrer/Hagenhoff 2022; Sauer/Staples/Steinbach 2022).

Vor dem Hintergrund der Kritik an Vorstellungen einer absoluten Souveränität, der gleichzeitig fast alternativlosen Orientierung politischer Praxis an Souveränität als einem »produktivem Mythos« sowie nicht zuletzt der in jüngster Zeit in der politischen Praxis (wieder) zunehmenden Bezugnahmen auf Souveränität – und eben auch »digitaler Souveränität« –, wird es Aufgabe der Geistes- und Sozialwissenschaften, im Dialog mit den Technikwissenschaften differenzierte Perspektiven auf »(digitale) Souveränität« herauszuarbeiten und damit Orientierungswissen für die gesellschaftliche Selbstverständigung im digitalen Zeitalter und für die Gestaltung der digitalen Transformation zu entwickeln. Die im folgenden Abschnitt vorgestellten Beiträge dieses Bandes möchten dazu aus verschiedenen Disziplinen jeweils einen Anteil leisten.

4. »Digitale Souveränität« aus disziplinären Perspektiven

Der Sammelband führt konzeptionelle und empirische Auseinandersetzungen mit »digitaler Souveränität« aus verschiedenen Disziplinen der Geistes- und Sozialwissenschaften sowie der Informatik zusammen. Ausgangspunkt des ersten Beitrags aus der Politischen Geographie ist der Befund, dass sich »digitale Souveränität« in den 2010er- und 2020er-Jahren zu *dem* zentralen Leitmotiv nationaler und internationaler Digitalpolitik entwickelt hat. Auch in den politisch-öffentlichen Diskursen in Deutschland werden seither vielfach Ansätze einer »digitalen Souveränität« aufgegriffen – und dies in ganz unterschiedlichen gesellschaftlichen Bereichen. Dieser Rückgriff auf Souveränität muss zunächst verwundern, war die deutsche Telekommunikationspolitik doch seit den frühen 1990er-Jahren geprägt von Vorstellungen eines »schlanken Staates« und einer Überwindung nationaler Grenzen hin zu einer »globalen Informationsgesellschaft«. Ein Beharren auf staatlich-territoriale Souveränitätsprinzipien galt als überholt und wurde vielfach kritisiert. Wie lässt sich vor diesem Hintergrund die Rezeption von »digitaler Souveränität« in den 2010er-Jahren in Deutschland erklären? Zur Beantwortung dieser Fragen rekonstruieren Finn Dammann und Georg Glasze, ausgehend von der Kommerzialisierung des Internets in den 1990er-Jahren bis in die frühen 2020er-Jahre, jene historischen Brüche und (Dis-)Kontinuitäten im

digitalpolitischen Diskurs, die zur Konsolidierung einer spezifischen Diskursformation rund um das Schlagwort »digitale Souveränität« in Deutschland beigetragen haben – und situieren diese in den internationalen Kontext.

Der Beitrag *Soziotechnische Einflussfaktoren auf die »digitale Souveränität« des Individuums* der drei Informatiker*innen Zinaida Benenson, Felix Freiling und Klaus Meyer-Wegener geht von den technischen bzw. soziotechnischen Herausforderungen der Digitalisierung aus. Sie fassen »digitale Souveränität« als die Möglichkeit des*der Einzelnen, in einer digitalisierten Welt ein selbstbestimmtes und autonomes Leben zu führen, und fragen nach soziotechnischen Einflussfaktoren auf die »digitale Souveränität« des Individuums. Zur Beantwortung dieser Frage diskutieren sie drei Fallstudien: a) die zunehmende Abhängigkeit von wenigen großen Anbietern digitaler Dienste, die zwar für die Sicherheit der Nutzer*innen sorgen, aber gleichzeitig auch über die uneingeschränkte Macht über Daten und Geräte verfügen, b) das Fehlen einer menschenzentrierten Gestaltung von Schutzmechanismen, was die Wahrnehmung möglicher Bedrohungen erschwert und c) die unklaren Vorstellungen über die Genauigkeit und die Nützlichkeit digitaler Datenerhebungen.

Der dritte Beitrag »*Digitale Souveränität« als Kontrolle. Ihre zentralen Formen und ihr Verhältnis zueinander* möchte auf der Basis einer Analyse der wissenschaftlichen Debatte zur Klärung des Konzepts der »digitalen Souveränität« beitragen und eine ethische Positionierung entwickeln. Kernidee des Aufsatzes von Max Tretter ist, dass der Begriff der Kontrolle bzw. des Kontrollhandelns zum besseren Verständnis der Debatte um »digitale Souveränität« beitragen kann. Durch eine Analyse englischsprachiger wissenschaftlicher Fachaufsätze mit thematischem Bezug zu »*digital sovereignty*« werden im Aufsatz zentrale Akteure, Formen und Interdependenzen digitaler Kontrolle bzw. Souveränität herausgearbeitet. Aus der Literaturanalyse ergibt sich das Bild, dass in erster Linie Staaten als Akteure digitalen Kontrollhandelns »digitale Souveränität« ausüben – vor allem in den Bereichen IT-Architektur, Gesetzgebung und nationale Sicherheit. Interessanterweise zeigt sich, dass in der wissenschaftlichen Literatur zu »*digital sovereignty*« Souveränität in erster Linie mit Fragen von Kontrolle und Macht verknüpft wird und kaum mit Fragen von Legitimation. Der Aufsatz greift das Beispiel Russlands heraus, um Wechselbeziehungen zwischen verschiedenen Formen »digitaler Kontrolle« modellhaft zu rekonstruieren, und endet mit einer ethischen Einschätzung, die vor der Übertragbarkeit eines in autoritären Staaten entwickelten Souveränitätskonzeptes auf liberale Demokratien warnt und vor diesem Hintergrund

für die Notwendigkeit der Schaffung eines dezidiert liberal-demokratischen Konzepts »digitaler Souveränität« plädiert.

Eva Odzuck stellt sich in dem Beitrag *»Demokratische digitale Souveränität«. Plädoyer für einen normativen Begriff am Beispiel des digitalen Wahlkampfs* der Aufgabe, aus der Perspektive der Politischen Theorie einen normativen Begriff »digitaler Souveränität« zu entwickeln, der den spezifischen Legitimationskontext liberal-demokratischer Staatlichkeit berücksichtigt. Nach einem kurzen Blick in die Geschichte des Souveränitätsbegriffs und dessen Verschränkung von Macht- und Rechtsdimension fokussiert der Artikel auf die Praxis digitaler Wahlkämpfe, in denen digitale Tools für Parteien attraktive Ressourcen zur zielgruppengerechten Ansprache der Wählerschaft und damit Machtressourcen zur Stimmenmaximierung generieren. Durch Rückgriff auf Rawls' Konzept der deliberativen Demokratie zeigt Eva Odzuck anschließend auf, dass Parteien als prägende Akteure des öffentlichen Diskurses einer Pflicht zur Bürgerlichkeit unterliegen, die für den digitalen Wahlkampf als »demokratische digitale Souveränität« ausbuchstabiert werden kann. Auf einer allgemeinen Ebene plädiert der Aufsatz dafür, normative, demokratietheoretische Perspektiven in die Digitalisierungsdebatte einzuspeisen, weil liberale Demokratien für die angemessene Beurteilung und demokratiepolitisch verantwortliche Gestaltung der Digitalisierung auf ein entsprechendes normatives Vokabular angewiesen sind.

Der rechtswissenschaftliche Beitrag *Souveränität, Integrität und Selbstbestimmung – Herausforderungen von Rechtskonzepten in der digitalen Transformation* warnt vor einer unreflektierten Übertragung des im juristischen Fachdiskurs ursprünglich auf Staaten bezogenen Konzepts »Souveränität« auf die Individualebene. Christian Rückert, Christoph Safferling und Franz Hofmann plädieren dafür, für die Individualebene den Begriff »digitale Souveränität« zu ergänzen durch die etablierten Begriffe der »Integrität« und der »Selbstbestimmung« – die allerdings ebenfalls für digitale Kontexte ausgearbeitet werden müssen und in Relation zu setzen sind. Ausgehend vom Fall »Microsoft/Ireland« wird im ersten Teil des Beitrags aus Perspektive des Straf- und Strafverfahrensrechts argumentiert, dass a) mit einem Fokus auf Souveränität die Aspekte des Grund- und Menschenrechtsschutzes an den Rand gedrängt werden, b) die Übertragung des Souveränitätskonzeptes auf Daten generell problematisch ist und c) Souveränität von vornherein in der Relation zu Grund- und Menschenrechten begriffen und konzipiert werden muss. Souveränität sollte also funktional über den Schutz von Grund- und Menschenrechten und damit auch digitaler Integrität bestimmt werden. Im

zweiten Teil des Beitrags wird aus privatrechtlicher Perspektive das Phänomen der digitalen Selbstbestimmung beleuchtet und in Bezug auf das Verhältnis von Datenschutz und Selbstbestimmung diskutiert. Ausgehend von der kritischen Auseinandersetzung mit den Implikationen, Funktionen und Leerstellen des Souveränitätsbegriffs wird im Fazit dafür plädiert, die Debatte stärker als bisher unter der Perspektive der Individualrechte (Integrität, Selbstbestimmung) statt unter dem staatstheoretischen Begriff der Souveränität zu führen – was nicht nur als Grundsatzkritik am Begriff der »digitalen Souveränität« verstanden werden kann, sondern auch als Plädoyer, den Begriff der »digitalen Souveränität« von vornherein unter menschenrechtlichen und rechtsstaatlichen Perspektiven auszubuchstabieren.

Auch der Beitrag »*Digitale Souveränität«: Zielperspektive einer Bildung in Zeiten tiefgreifender Mediatisierung?* von Jane Müller und Rudolf Kammerl setzt sich aus einer pädagogischen Perspektive kritisch-konstruktiv mit dem Begriff der »digitalen Souveränität« in Wissenschaft und Gesellschaft auseinander. Vor dem Hintergrund terminologischer Überlegungen zur Unverzichtbarkeit des Bildungsbegriffs in der Pädagogik problematisiert der Beitrag die derzeit zu beobachtende Übertragung des Begriffs »digitaler Souveränität« auf die Mikroebene individuellen Medienhandelns. Die Autor*innen argumentieren, dass eine solche Übertragung Chancen bietet, aber auch mit Schwierigkeiten einhergeht. Unter kritisch-konstruktiven Vorzeichen analysieren sie Verkürzungen in der bestehenden wissenschaftlichen und öffentlichen Debatte und machen in der Konsequenz einen eigenen Vorschlag für ein komplexes, relationales Konzept »digitaler Souveränität«, das Relevanz für den bildungspolitischen Diskurs beansprucht und dazu beitragen kann, bestehende Forderungen nach »digitaler Souveränität« kritisch zu beurteilen und konstruktiv weiterzuführen.

Albrecht Fritzsche diskutiert in dem Beitrag *Konturenbildung im Gestaltungsraum der digitalen Transformation – eine Reflexion der Debatte über »digitale Souveränität« aus betriebswirtschaftlicher Sicht* ebenfalls Potenziale, aber auch blinde Flecken des Begriffs der »digitalen Souveränität« – hier im Hinblick auf die Gestaltung von Wertschöpfungsprozessen im Kontext der digitalen Transformation. Dabei skizziert er aus der Perspektive der Betriebswirtschaft und basierend auf wirtschaftsphilosophischen Grundlagen zunächst die Vielfalt neuer Gestaltungsoptionen für Wertschöpfungsprozesse. Den Diskurs über »digitale Souveränität« interpretiert er dabei als eine Form der »Konturenbildung«, die Orientierungspunkte bieten kann. Gleichzeitig weist der Beitrag allerdings darauf hin, dass mit dem Bezug auf Souveränität vielfach zumindest implizit

Vorstellungen territorialer Abgrenzung (in überkommener Weise konzeptualisiert als erdräumliche Abgrenzungen) und Kontrolle über Ressourcen (konzeptualisiert als materielle Rohstoffe) verknüpft werden, die für die Gestaltung von Wertschöpfungsprozessen in einer digital vernetzten Welt zu kurz greifen.

Der Beitrag aus den Buch- und Kommunikationswissenschaften wählt einen anderen Zugang zu »digitaler Souveränität«: Katharina Leyrer und Svenja Hagenhoff nutzen in ihrem Aufsatz »*Digitale Souveränität« in der medienvermittelten öffentlichen Kommunikation: die Beziehung zwischen Rezipient*in und Gatekeeper* den Begriff als prinzipiell produktiven Ausgangspunkt, um veränderte Voraussetzungen von Mediennutzung unter digitalen Vorzeichen zu diskutieren. Statt unreflektiert vor einem Verlust »digitaler Souveränität« in der Beziehung zwischen Rezipient*innen und Gatekeeper zu warnen, wollen sie Aussagen über Souveränitätsverluste digitaler Nutzer*innen auf einer kriteriengeleiteten Begriffsbestimmung und empirisch orientierten Vergleichsperspektive stützen. Der Beitrag entwickelt unter Rückgriff auf die Network-Gatekeeping-Theorie solche Kriterien und kommt anhand einer Fallanalyse zu dem Ergebnis, dass die »digitale Souveränität« von Nutzer*innen sowohl im analogen als auch digitalen Raum eingeschränkt ist und sowohl Bibliotheksnutzer*innen als auch Nutzer*innen von Suchmaschinen plattformspezifischen Einschränkungen unterliegen. In beiden Fällen werden »für« die Nutzer*innen Selektionen vorgenommen, die von diesen nur sehr bedingt nachvollzogen werden können. Generell gelte es, in der Diskussion um »digitale Souveränität« stärker relationale Aspekte mitzudenken und jeweils sehr genau deutlich zu machen, über welche Akteure, Relationen und Zeitpunkte jeweils gesprochen wird.

Die Idee, »digitale Souveränität« als spezifische Form von Beziehung zu denken, macht auch der arbeitssoziologische Beitrag mit dem Titel *Der relationale Charakter von »digitaler Souveränität«. Zum Umgang mit dem »Autonomie/Heteronomie«-Dilemma in sich transformierenden Arbeitswelten*. Ausgehend von der Feststellung, dass Arbeitsverhältnisse in der Regel von dem Verhältnis Autonomie/Heteronomie geprägt werden und sich weniger über Souveränitätszuschreibungen definieren, diskutieren Stefan Sauer, Ronald Staples und Vincent Steinbach die besonderen Voraussetzungen von gegenwärtigen Beschäftigungsverhältnissen. Gelingende Arbeitsorganisation – so wird gezeigt – hängt dann sowohl von der Gestaltung der Anerkennungsverhältnisse ab als auch von dem Gewähren von Vertrauen und einem Bewusstsein für die Spezifika moderner digitaler Kommunikation. Gleichzeitig soll Arbeit stabil und flexibel sein, um komplexe Probleme zu lösen. »Digitale Souveränität« veror-

ten die Autoren in diesen sehr voraussetzungsvollen Situationen, die zudem den konstitutiv relationalen Charakter von Souveränität unterstreichen.

Literaturverzeichnis

Agnew, John (2005): »Sovereignty regimes: Territoriality and state authority in contemporary world politics«, in: Annals of the Association of American Geographers 95 (2), S. 437–461.

Agnew, John (2020): »The contingency of sovereignty«, in: David Storey (Hg.), A Research agenda for territory and territoriality, Cheltenham: Edward Elgar, S. 43–60.

August, Vincent (2021): Technologisches Regieren: Der Aufstieg des Netzwerk-Denkens in der Krise der Moderne. Foucault, Luhmann und die Kybernetik, Bielefeld: transcript.

Barkan, Joshua E. (2015): »Sovereignty«, in: John Agnew/Virginie Mamadouh/Anna J. Secor/Joanne Sharp (Hg.), The Wiley Blackwell companion to political geography. Malden: John Wiley, S. 48–60.

Behrens, Melanie (2021): Komplexen Subjektivierungen auf der Spur. Ein methodologischer Ansatz zur Analyse von Machtverhältnissen, Bielefeld: transcript.

Benenson, Zinaida/Freiling, Felix/Meyer-Wegener, Klaus (2022): »Soziotechnische Einflussfaktoren auf die digitale Souveränität des Individuums«, in: Georg Glasze/Eva Odzuck/Ronald Staples (Hg.), Was heißt digitale Souveränität? Diskurse, Praktiken und Voraussetzungen »individueller« und »staatlicher Souveränität« im digitalen Zeitalter, Bielefeld: transcript, S. 61–87.

Berger, Franz X./Deremetz, Anne/Hennig, Martin/Michell, Alix (Hg.) (2021): Autonomie und Verantwortung in digitalen Kulturen. Privatheit im Geflecht von Recht, Medien und Gesellschaft, Baden-Baden: Academia.

Branch, Jordan (2014): The cartographic state. Maps, territories and the origin of sovereignty, Cambridge: Cambridge University Press.

Bredekamp, Horst (2003): Thomas Hobbes – Der Leviathan. Das Urbild des modernen Staates und seine Gegenbilder 1651–2001 (= Acta humaniora, Schriften zur Kunstwissenschaft und Philosophie), Berlin: Akademie Verlag.

Callon, Michel (1984): »Some elements of a sociology of translation: Domestication of the scallops and the fishermen of St Brieuc Bay«, in: The Sociological Review 32 (1), S. 196–233.

Chesbrough, Henry W. (2003): Open innovation. The new imperative for creating and profiting from technology, Boston: Harvard Business School Press.

Christman, John (2008): »Autonomie«, in: Stefan Gosepath/Wilfried Hinsch/Beate Rössler (Hg.), Handbuch der Politischen Philosophie und der Sozialphilosophie. Band 1: A–M, Berlin/Boston: de Gruyter, S. 96–102.

Coleman, Mathew (2009): »Sovereignty«, in: Rob Kitchin/Nigel Thrift (Hg.), International encyclopedia of human geography. Band 10: Political Geography, Amsterdam: Elsevier, S. 255–261.

Dammann, Finn/Glasze, Georg (2022): »›Wir müssen als Deutsche und Europäer unsere digitale Souveränität zurückgewinnen!‹ Historische Rekonstruktion und internationale Kontextualisierung der Diskurse einer ›digitalen Souveränität‹ in Deutschland«, in: Georg Glasze/Eva Odzuck/Ronald Staples (Hg.), Was heißt digitale Souveränität? Diskurse, Praktiken und Voraussetzungen »individueller« und »staatlicher Souveränität« im digitalen Zeitalter, Bielefeld: transcript, S. 29–60.

Derrida, Jacques/Roudinesco, Elisabeth (2006): Woraus wird Morgen gemacht sein? Ein Dialog, Stuttgart: Klett-Cotta.

Dittgen, Herbert (1999): »Grenzen im Zeitalter der Globalisierung. Überlegungen zur These vom Ende des Nationalstaates«, in: Zeitschrift für Politikwissenschaft 9 (1), S. 3–26.

Elden, Stuart (2013): The birth of territory, Chicago: University of Chicago Press.

Engelbrekt, Antonina Bakardjieva/Leijon, Karin/Michalski, Anna/Oxelheim, Lars (Hg.) (2020): The European Union and the return of the nation state. Interdisciplinary European Studies, Cham: Springer International Publishing.

Feindt, Gregor/Gissibl, Bernhard/Paulmann, Johannes (2021): »Introduction: Cultural sovereignty – claims, forms and contexts beyond the modern state«, in: Gregor Feindt/Bernhard Gissibl/Johannes Paulmann (Hg.), Cultural sovereignty beyond the modern state. Space, objects, and media (= European History Yearbook, Band 21), Berlin/Boston: de Gruyter, S. 1–20.

Foucault, Michel (1971 [1966]): Die Ordnung der Dinge: Eine Archäologie der Humanwissenschaften, Frankfurt a.M.: Suhrkamp.

Fritzsche, Albrecht (2022): »Konturenbildung im Gestaltungsraum der digitalen Transformation – eine Reflektion der Debatte über ›digitale Souverä-

nität‹ aus betriebswirtschaftlicher Sicht«. in: Georg Glasze/Eva Odzuck/Ronald Staples (Hg.), Was heißt digitale Souveränität? Diskurse, Praktiken und Voraussetzungen »individueller« und »staatlicher Souveränität« im digitalen Zeitalter, Bielefeld: transcript, S. 229–246.

George, Susan (2015): Shadow sovereigns. How global corporations are seizing power, New York: John Wiley & Sons.

Grimm, Dieter (2009): Souveränität. Herkunft und Zukunft eines Schlüsselbegriffs, Berlin: Berlin University Press.

Grumbach Stéphane/Zanin, Caroline (2022): »Platforms vs. states: A sovereignty conundrum«, in: Georg Glasze/Amaël Cattaruzza/Frédérick Douzet/Finn Dammann/Marie-Gabrielle Bertran/Clotilde Bômont/Matthias Braun/Didier Danet/Alix Desforges/Aude Géry/Stéphane Grumbach/Patrik Hummel/Kevin Limonier/Max Münßinger/Florian Nicolai/Louis Pétiniaud/Jan Winkler/Caroline Zanin (Hg.): Forum – Contested spatialities of digital sovereignty, in: Geopolitics, https://doi.org/10.1080/14650045.2022.2050070.

Gümplová, Petra (2015): »On sovereignty and post-sovereignty«, in: Philosophica Critica 1 (2), S. 3–18.

Hannah, Matthew G. (2000): Governmentality and the mastery of territory in nineteenth-century America (= Cambridge Studies in Historical Geography, Band 32), Cambridge: Cambridge University Press.

Haraway, Donna Jeanne (1985): »Manifesto for Cyborgs: Science, Technology, and Socialist Feminism in the 1980's«, in: Socialist Review 80, S. 65–108.

Ignatieff, Michael (2012): »The return of sovereignty«, in: The New Republic vom 25.01.2012. Online unter: https://newrepublic.com/article/100040/sovereign-equality-moral-disagreement-government-roth, abgerufen am 25.07.2022.

Kiersch, Gerhard (1977): »Souveränität«, in: Wichard Woyke (Hg.), Handwörterbuch internationale Politik, Opladen: Leske + Budrich, S. 281–284.

Klein, Rebekka (2016): »Imaginäre Subjekte der Macht: Zur Ablösung der Politischen Theologie im Zeitalter von Post-Demokratie und Post-Souveränität«, in: Ino Augsberg/Karl-Heinz Ladeur (Hg.), Politische Theologie(n) der Demokratie: Das religiöse Erbe des Säkularen, Wien/Berlin: Turia + Kant, S. 99–113.

Krasner, Stephen D. (2001): Sovereignty. Organized hypocrisy, Princeton: Princeton University Press.

Lamla, Jörn/Büttner, Barbara/Ochs, Carsten/Pittroff, Fabian/Uhlmann, Markus (2022): »Privatheit und Digitalität: Zur soziotechnischen Transforma-

tion des selbstbestimmten Lebens«, in: Alexander Roßnagel/Michael Friedewald (Hg.), Die Zukunft von Privatheit und Selbstbestimmung, Wiesbaden: Springer VS, S. 125–158.

Latour, Bruno (2007): Eine neue Soziologie für eine neue Gesellschaft. Einführung in die Akteur-Netzwerk-Theorie, Frankfurt a.M.: Suhrkamp.

Leyrer, Katharina/Hagenhoff, Svenja (2022): »›Digitale Souveränität‹ in der medienvermittelten öffentlichen Kommunikation: die Beziehung zwischen Rezipient*in und Gatekeeper«, in: Georg Glasze/Eva Odzuck/Ronald Staples (Hg.), Was heißt digitale Souveränität? Diskurse, Praktiken und Voraussetzungen »individueller« und »staatlicher Souveränität« im digitalen Zeitalter, Bielefeld: transcript, S. 247–286.

Löw, Martina/Sayman, Volkan/Schwerer, Jona/Wolf, Hannah (2021): Am Ende der Globalisierung. Über die Refiguration von Räumen, Bielefeld: transcript.

Lynch, Casey R. (2020): »Contesting digital futures: Urban politics, alternative economies, and the movement for technological sovereignty in Barcelona«, in: Antipode 52 (3), S. 660–680.

MacCormick, Neil (1993): »Beyond the sovereign state«, in: The Modern Law Review 56 (1), S. 1–18.

Meißner, Hanna (2014): Jenseits des autonomen Subjekts. Zur gesellschaftlichen Konstitution von Handlungsfähigkeit im Anschluss an Butler, Foucault und Marx (= Gender Studies), Bielefeld: transcript.

Melzer, Sara E./Norberg, Kathryn (1998): From the royal to the republican body. Incorporating the political in seventeenth- and eighteenth-century France, Berkeley: University of California Press.

Mill, John S. (1969): Über Freiheit. Aus dem Englischen übertragen und mit einem Anhang versehen von Achim v. Borries, Frankfurt a.M.: Europäische Verlagsanstalt.

Mitchell, William/Fazi, Thomas (2017): Reclaiming the state. A progressive vision of sovereignty for a post-neoliberal world, London: Pluto Press.

Müller, Jane/Kammerl, Rudolf (2022): »›Digitale Souveränität‹: Zielperspektive einer Bildung in Zeiten tiefgreifender Mediatisierung?«, in: Georg Glasze/Eva Odzuck/Ronald Staples (Hg.), Was heißt digitale Souveränität? Diskurse, Praktiken und Voraussetzungen »individueller« und »staatlicher Souveränität« im digitalen Zeitalter, Bielefeld: transcript, S. 201–228.

Münkler, Laura (2016): »Metaphern im Recht. Zur Bedeutung organischer Vorstellungen von Staat und Recht«, in: Der Staat 55 (2), S. 181–211.

Münkler, Herfried/Straßenberger, Grit (2016): Politische Theorie und Ideengeschichte. Eine Einführung (= C.H. Beck Paperback 1817), München: C.H. Beck.

Odzuck, Eva (2022): »›*Demokratische* digitale Souveränität‹. Plädoyer für einen normativen Begriff am Beispiel des digitalen Wahlkampfs«, in: Georg Glasze/Eva Odzuck/Ronald Staples (Hg.), Was heißt digitale Souveränität? Diskurse, Praktiken und Voraussetzungen »individueller« und »staatlicher Souveränität« im digitalen Zeitalter, Bielefeld: transcript, S. 127–158.

Panić, Mica (1997): »The end of the nation state?«, in: Structural Change and Economic Dynamics 8 (1), S. 29–44.

Reckwitz, Andreas (2006): Das hybride Subjekt. Eine Theorie der Subjektkulturen von der bürgerlichen Moderne zur Postmoderne, Weilerswist: Velbrück.

Sassen, Saskia (1996): Losing control. Sovereignty in the age of globalization (= University Seminars: Leonard Hastings Schoff Memorial lectures), New York: Columbia University Press.

Sauer, Stefan/Staples, Ronald/Steinbach, Vincent (2022): »Der relationale Charakter von ›digitaler Souveränität‹. Zum Umgang mit dem ›Autonomie/Heteronomie‹-Dilemma in sich transformierenden Arbeitswelten«, in: Georg Glasze/Eva Odzuck/Ronald Staples (Hg.), Was heißt digitale Souveränität? Diskurse, Praktiken und Voraussetzungen »individueller« und »staatlicher Souveränität« im digitalen Zeitalter, Bielefeld: transcript, S. 287–315.

Schmitt, Carl (2008 [1922]): Politische Theologie, München/Leipzig/Berlin: Duncker & Humblot.

Skinner, Quentin (2012): Die drei Körper des Staates (= Frankfurter Vorträge, Band 2), Göttingen: Wallstein Verlag.

Stacy, Helen (2003): »Relational sovereignty«, in: Stanford Law Review 55 (45), S. 2019–2059.

Thiel, Thorsten (2021): »Das Problem mit der digitalen Souveränität«, in: FAZ vom 26.01.2021. Online unter: https://www.faz.net/aktuell/wirtschaft/digitec/europa-will-in-der-informationstechnologie-unabhaengiger-werden-17162968.html, abgerufen am 16.06.2022.

Voigt, Rüdiger (2016): Staatliche Souveränität. Zu einem Schlüsselbegriff der Staatsdiskussion, Wiesbaden: Springer VS.

Weinberg, Lindsay (2017): »Rethinking privacy: A feminist approach to privacy rights after Snowden«, in: Westminster Papers in Communication and Culture 12 (3), S. 5–20.

Williams, Robert W. (2005): »Politics and self in the age of digital (re)producibility«, in: Fast Capitalism 1 (1), S. 104–121.

»Wir müssen als Deutsche und Europäer unsere digitale Souveränität zurückgewinnen!«[1]

Historische Rekonstruktion und internationale Kontextualisierung der Diskurse einer »digitalen Souveränität« in Deutschland

Finn Dammann, Georg Glasze

Abstract *»Digitale Souveränität« hat sich in den 2010er- und 2020er-Jahren zu dem zentralen Leitmotiv nationaler und internationaler Digitalpolitik entwickelt. Auch in den politisch-öffentlichen Diskursen in Deutschland werden seither vielfach Ansätze einer »digitalen Souveränität« aufgegriffen – und dies in ganz unterschiedlichen gesellschaftlichen Bereichen. Diese Rückbesinnung auf Souveränität über digitale Informations- und Kommunikationssysteme muss zunächst verwundern, war die deutsche Telekommunikationspolitik doch seit den frühen 1990er-Jahren geprägt von Vorstellungen eines »schlanken Staates« und einer Überwindung nationaler Grenzen hin zu einer »globalen Informationsgesellschaft«. Gerade ein Beharren auf Prinzipien staatlich-territorialer Souveränität galt als überholt und wurde vielfach kritisiert. Wie lässt sich vor diesem Hintergrund die Rezeption von »digitaler Souveränität« in den 2010er-Jahren in Deutschland erklären? Zur Beantwortung dieser Fragen rekonstruieren wir in diesem Beitrag ausgehend von der Kommerzialisierung des Internets in den 1990er-Jahren bis in die frühen 2020er-Jahre jene historischen Brüche und (Dis-)Kontinuitäten im digitalpolitischen Diskurs, die zur Konsolidierung einer spezifischen Diskursformation rund um das Schlagwort »digitale Souveränität« in Deutschland beigetragen haben – und situieren diese in den internationalen Kontext.*

1 Der damalige Bundesminister für Verkehr und Digitalisierung, Alexander Dobrindt, im Spiegel vom 23. Dezember 2013.

1. Einleitung: »digitale Souveränität« als Leitmotiv einer neuen Digitalpolitik

»Digitale Souveränität« hat sich in den 2010er- und 2020er-Jahren zu *dem* zentralen Leitmotiv nationaler und internationaler Digitalpolitiken entwickelt. Wie eine Reihe von Studien gezeigt hat, wird dabei in verschiedenen geographischen Kontexten vor Gefahren einer digitalen Überwachung und Beeinflussung durch *ausländische* Unternehmen und Regierungen gewarnt – sowie neu entstandene Abhängigkeiten kritisiert (für einen Überblick s. Couture/Toupin 2019, Thumfart 2021, Hummel et al. 2021 sowie Glasze et al. 2022a; für Russland Nocetti 2015, Ermoshina/Musiani 2017; für China Hong/Goodnight 2020, Creemers 2020, Liu 2021; für die formale EU-Politik Pohle/Thiel 2020). Diese diskursiven Problematisierungen gehen vielfach einher mit konkreten politischen Praktiken: Internet-Shutdowns, nationale Firewalls, Netzsperren, staatliche Eingriffe in das Routing von Datenpaketen, umfangreiche Überwachungsbefugnisse nationaler Sicherheitsbehörden, gesetzliche Verpflichtungen zur Speicherung und Prozessierung von Daten innerhalb nationaler Territorien und Planungen für nationale Netzprotokolle werden zu Beginn der 2020er-Jahre wiederholt mit Hinweisen auf »digitale Souveränität« begründet und legitimiert (für einen Überblick zu nationalen Datenpolitiken im Kontext »digitaler Souveränität« s. Lambach 2019).

Auch in den politisch-öffentlichen Diskursen in Deutschland werden seit den frühen 2010er-Jahren Ansätze einer »digitalen Souveränität« aufgegriffen – und dies in ganz unterschiedlichen gesellschaftlichen Bereichen: in verschiedenen Feldern und Maßstabsebenen der Politik[2] sowie von zahlreichen Organisationen über Unternehmensverbände (s. bspw. Bitkom 2015; Open Source Business Alliance 2021) bis hin zu dezidiert kritisch-zivilgesellschaftlich orientierten Gruppen[3]. Diese Rezeption von Diskursen und Politiken einer »digitalen Souveränität« in Deutschland kann zunächst überraschen: So waren die politischen Leitbilder in vielen Ländern des Westens Ende des

2 So wird »digitale Souveränität« zu einem zentralen Leitbild der deutschen EU-Ratspräsidentschaft 2020 (Auswärtiges Amt 2020), Publikationen aus dem deutschen Wirtschafts-, Innen- und Verteidigungsministerium sowie zahlreicher Landesregierungen und Kommunen beziehen sich Ende der 2010er- und Anfang der 2020er-Jahre regelmäßig auf »digitale Souveränität«.

3 Ein breites Bündnis zivilgesellschaftlicher Organisationen veröffentlicht 2021 vier Forderungen für eine »digital souveräne Gesellschaft« (https://digitalezivilgesellschaft.org/; 10.01.2022).

20. und zu Beginn des 21. Jahrhunderts geprägt von Leitbildern einer Vernetzung und Überwindung von Grenzen sowie einer Zurückdrängung des Staates. Gerade auch die Debattenlandschaft in Deutschland war in hohem Maße geprägt von Leitbildern einer europäischen und globalen Integration.[4] Konzepte staatlicher Souveränität galten in diesem Kontext als überkommen und wenig geeignet, in einer (digital) vernetzten Welt Orientierung zu geben.[5] Staatlich durchgesetzte Netzsperren oder Verpflichtungen zur Speicherung von Daten innerhalb nationaler Territorien wurden bis in die 2010er-Jahre daher weitgehend als Praktiken autoritärer »Überwachungsstaaten« verurteilt. Wie lässt sich vor diesem Hintergrund die Rezeption von »digitaler Souveränität« in den 2010er-Jahren in Deutschland erklären? Zur Beantwortung dieser Frage rekonstruieren wir Kontinuitäten und Brüche des digitalpolitischen Diskurses in Deutschland – ausgehend von der Kommerzialisierung des Internets in den 1990er-Jahren bis in die 2020er-Jahre. Dazu führt unser Beitrag eigene empirische Arbeiten (Glasze/Dammann 2021;

4 Die bundesrepublikanische Außenpolitik war und ist bspw. von einer expliziten Orientierung auf internationale Kooperation und Europäisierung geprägt. Der Politikwissenschaftler Maull hat 2007 diese Selbstpositionierung als »Zivilmacht« charakterisiert.

5 So lässt sich nachzeichnen, wie in der zweiten Hälfte des 20. Jahrhunderts in hohem Maße Leitbilder staatlicher Souveränität zugunsten von Vorstellungen von dezentraler und vernetzter Steuerung verdrängt wurden und dabei eine Orientierung an einem Denken in Netzwerken und neo-liberale Vorstellungen zusammenwirkten (August 2021; zu den Grundlagen dieses Denkens in der Kybernetik auch: Seibel 2016). Sozialwissenschaftliche Analysen konstatierten den Siegeszug einer »Netzwerkgesellschaft« und die Ablösung territorialer Raumordnungen durch einen »space of flows« (prominent bspw. formuliert durch Castells 1994 und 2000). Das Wachstum der Datenströme und die breitere digitale Transformation wurden dabei vielfach als wichtige Triebkräfte und Beschleuniger einer globalen Integration sowie der Entstehung einer post-territorialen Welt beschrieben. Es gab Vorhersagen, dass Datenströme und Netzwerke die traditionelle territoriale Ordnung der Staaten letztlich ersetzen werden (emblematisch für diese Perspektive Friedman 2007). Arbeiten aus der Politischen Geographie kritisierten solche Vorhersagen schon früh als ungenau und naiv (z.B. Toal 1999). Gleichzeitig wurde in der akademischen Debatte schon früh differenziert über die Herausforderungen diskutiert, die transnationale Datenströme für die territorialstaatliche Organisation des Rechtssystems und damit für die Konzepte staatlicher Jurisdiktion und Souveränität darstellen (prominent hierzu Perritt 1998). Sozialwissenschaftlerinnen und -wissenschaftler wie bspw. maßgebend Sassen diskutieren ebenfalls bereits Mitte der 1990er-Jahre die Herausforderung des Internets für staatliche Souveränität (Sassen 1996).

Winkler/Dammann 2022; Dammann/Glasze 2022) sowie Arbeiten weiterer Wissenschaftler*innen (Steiger/Schünemann/Dimmroth 2017; Pohle/Thiel 2020) zu einer überblicksartigen Diskursgeschichte zusammen und situiert diese in den internationalen Kontext.

Der Beitrag gliedert sich nachfolgend in drei Teile: Abschnitt 2 rekonstruiert die »Vorgeschichte digitaler Souveränität in Deutschland«. Hier zeigen wir, dass die Digitalpolitik in den 1990er- und 2000er-Jahren v.a. von Vorstellungen einer Integration in globale Zusammenhänge und einer Begrenzung staatlicher Aktivität dominiert war. Jedoch gibt es in den 2000er-Jahren bereits erste Stimmen, die diese Entwicklung problematisieren und letztlich nach mehr staatlichen Interventionen in die Gestaltung der Digitalisierung rufen. Das Schlagwort einer »digitalen Souveränität« wird allerdings nicht in Deutschland geprägt. Auf der Basis einer Literaturstudie zum internationalen Kontext zeigen wir in Abschnitt 3, dass »digitale Souveränität« als Leitmotiv von Digitalpolitiken zunächst in diskursiven Zusammenhängen v.a. in China und Russland ausgearbeitet und propagiert wird. Wie wir in Abschnitt 4 erläutern, wird in Deutschland das Schlagwort erst in den empörten Reaktionen auf die Enthüllungen Edward Snowdens 2013 aufgegriffen. Dabei werden zunächst vielfach Vorstellungen staatlich-territorialer Souveränität reproduziert und auf eine zukünftige Gestaltung des Digitalen übertragen. Das Leitmotiv einer »digitalen Souveränität« wird in der politischen Öffentlichkeit in Deutschland jedoch rasch auch breiter gefasst und über ein staatsorientiertes und territoriales Verständnis hinausgehend auf Fragen nach der Souveränität von deutschen Unternehmen sowie insbesondere nach der Souveränität individueller Nutzer*innen übertragen. Dabei wird an Vorstellungen von Souveränität als Handlungsfähigkeit, Autonomie und Selbstbestimmung angeknüpft (s. hierzu auch die Einleitung Glasze/Odzuck/Staples 2022 in diesem Band).

2. Die Vorgeschichte »digitaler Souveränität« in Deutschland: Forderungen nach einer »Integration in die globale Informationsgesellschaft« in den 1990er- und 2000er-Jahren – und erste Problematisierungen

Wie in vielen Ländern etablierte sich das Internet in den 1990er-Jahren auch in Deutschland rasch als neues Kommunikationssystem: 1994 wurde in München der erste deutsche Internetknoten eröffnet. Ein Jahr später ging in

Frankfurt a.M. der heute weltweit größte Internetknoten online. Zunehmend traten private Anbieter von Personal Computern, Netzinfrastrukturen, Internetdienstleistern und Software für verschiedene Internetdienste (z.B. veröffentlichte Microsoft 1995 seinen Internet Explorer) in den deutschen Telekommunikationsmarkt ein. Hatte 1994 nur knapp ein Prozent der Bevölkerung in Deutschland Zugang zum Internet, waren es im Jahr 2000 bereits 30 Prozent.[6]

Diese Ausweitung des digitalen Datenverkehrs war eingebettet in ein Regierungsprogramm zur Liberalisierung des deutschen Telekommunikationsmarktes und zur Privatisierung der bisher staatlich organisierten Telekommunikationsinfrastruktur. Bereits Ende der 1980er-Jahre wurde die ehemalige Deutsche Bundespost in die drei öffentlichen Unternehmen Postdienst, Postbank und Telekom aufgeteilt, die 1994 in Aktiengesellschaften umgewandelt wurden. 1995 verabschiedete die deutsche Regierung das Telekommunikationsgesetz (TKG), das die vollständige Privatisierung der gesamten Kommunikations- und Internetinfrastruktur ermöglichte. Im selben Jahr trat mit dem Informations- und Kommunikationsdienstegesetz (IUKDG) das erste umfassende Regelwerk für datenbasierte (Online-)Dienste in Kraft. Dieses Gesetz stärkte die Rechte privater (ausländischer und inländischer) Betreiber und Anbieter digitaler Infrastrukturen gegenüber den staatlichen Behörden, indem es die Unternehmen weitgehend von der Haftung für (illegalisierte) digitale Inhalte ihrer Nutzerinnen und Nutzer befreite (vgl. Reiberg 2017, 2018).

Ein diskursiver Kontext, der dieses politische Reformprogramm vielfach begründet und legitimiert hat, sind die Ziele, Ideen und Probleme, die mit dem Konzept einer »globalen Informationsgesellschaft« verbunden wurden (vgl. hierzu auch Keller 1998). Apologeten einer Liberalisierung des deutschen Telekommunikationsmarktes – wie etwa prominent Martin Bangemann, ehemaliger Bundeswirtschaftsminister und von 1989 bis 1993 EG-Kommissar für Industriepolitik, Information und Telekommunikation – mobilisierten Leitmotive einer Überwindung nationaler Grenzen und Zurückdrängung des Nationalstaates sowie eines neuen globalen Informationsaustausches. Verbunden mit diesen Leitmotiven waren Versprechen eines Wandels hin zu einer global vernetzten, partizipativen, freiheitlichen und egalitären Gesellschaft – als deren treibende Kräfte einerseits eine »*marked-led revolution*« und andererseits das Internet bzw. die digitale Informationstechnik selbst

6 Datenaufbereitung von Roser, Max/Ritchie, Hannah/Ortiz-Ospina, Esteban (2015): Internet. Online unter: https://ourworldindata.org/internet, abgerufen am 01.10.2021.

galten (zur Geschichte des technologischen Determinismus s. Chenou 2014).[7] Diese »diskursive Formation« (Foucault 1973) um eine »globale Informationsgesellschaft« führte daher wirtschaftsliberale Ideen eines schlanken Staates mit technikdeterministischen bzw. »technikutopistischen« Versprechen einer Emanzipation und Befreiung von staatlichen Herrschaftsverhältnissen zusammen (vgl. Dammann/Glasze 2022).

Staatliche Interventionen in die Gestaltung und Kontrolle von digitalen Kommunikationssystemen wurden im Kontext der diskursiven Formation einer »globalen Informationsgesellschaft« i.d.R. kritisch beurteilt. Diese galten etwa als gefährliche Hemmnisse für die sozialen und technischen Innovationskräfte des Internets und als Risiko für die internationale Wettbewerbsfähigkeit Deutschlands. Die im Jahr 1995 vom Deutschen Bundestag eingesetzte Enquete-Kommission zu »Deutschlands Weg in die Informationsgesellschaft« forderte beispielsweise mit Verweis auf einen »immer intensiveren Wettbewerb der Staaten um die Gunst von Unternehmen und Bürgern«, einen schlanken deutschen Staat, der sich »auf seine Kernaufgaben besinnt« (Deutscher Bundestag 1998). Gleichzeitig legitimierten Sorgen vor einem neuen deutschen Überwachungsstaat, dass Forderungen deutscher Sicherheitsbehörden nach mehr Kompetenzen zur Kontrolle digitaler Kommunikation vielfach zurückgewiesen wurden. Selbst progressiv-liberale Stimmen – wie beispielsweise der deutsche Chaos Computer Club – drängten in diesem Kontext wiederholt auf einen schlanken Staat, der sich auf die Sicherung der informationellen Selbstbestimmung und auf die Herstellung einer allgemeinen Kommunikationsfreiheit im Netz konzentrieren sollte (vgl. zur Geschichte des Diskurses zum »Überwachungsstaat« in Deutschland Hannah 2009; vgl. Dammann/Glasze 2022). Die Debatten um eine »globale Informationsgesellschaft« in Deutschland schlossen damit in gewisser Weise an vielfältige staatskritische Diskurse zum Internet an, die in den 1990er- und frühen 2000er-Jahren international zirkulierten (s. hierzu etwa bereits Barbrook/Cameron 1996 oder auch die in Deutschland vielfach rezipierte *Declaration of the Independence of Cyberspace* von John Perry Barlow 1996).

Die Forderungen nach einem schlanken Staat im Bereich der Telekommunikations- und Informationstechnik in Deutschland sind jedoch nicht ohne

7 Der in der EU einflussreiche Bangemann-Report (1994) spricht in diesem Kontext von einer »marked-led revolution« und fordert alle Mitgliedstaaten auf, »to put [their] faith in [the] market mechanism as the motive power to carry us into the Information Age« (Europäische Kommission 1994).

Widerspruch und Kritik geblieben: Bereits in den 1990er-Jahren fanden sich Stimmen, die vor einem drohenden Verlust staatlicher Handlungsfähigkeit und Souveränität durch die zunehmende Verbreitung des Internets warnten. Diese Warnungen wurden auch in apologetischen Texten *für* eine »globale Informationsgesellschaft« aufgegriffen und diskutiert – wie beispielsweise im Abschlussbericht der bereits erwähnten Enquete-Kommission (Deutscher Bundestag 1998). Die Kommission spricht 1998 von »neuen Herausforderungen für staatliche Souveränität«, die »in der Grenzenlosigkeit der neuen Kommunikationstechniken liegen«. Die globale Informationsgesellschaft führe »zu vermehrter Ausübung von politischer Macht durch Private« und »läßt die Staatsgewalt und damit die staatliche Souveränität in ihrer Wirkung mehr und mehr ins Leere laufen«. In diesem Kontext würde es für den Staat »immer schwieriger, seine Schutzfunktionen bei Straftaten und Rechtsbruch […] wahrzunehmen« (ebd.: 82f.). Diese Stellungnahme steht im Kontext einer Reihe von Problematisierungen fehlender staatlicher Souveränität über die digitale Kommunikation, die ausgehend von den späten 1990er-Jahren auch in öffentlich-politischen Mediendiskursen in Deutschland aufgegriffen und thematisiert wurden. Exemplarisch hierfür zeigen dies Dammann und Glasze (2022) anhand einer Analyse von Artikeln und Beiträgen im Nachrichtenmagazin *Der Spiegel* (1995–2016) sowie der Nachrichten-Websites *Netzpolitik.org* (2004–2019) und *Heise online* (1999–2019). Über die gesamten Untersuchungszeiträume steigen die relativen Anteile von Artikeln und Beiträgen, in denen der Begriff »Internet« zusammen mit Begriffen von »Staat bzw. Staatlichkeit« auftauchen. Damit deutet die Analyse auf einen längeren Trend der zunehmenden diskursiven Bearbeitung und Problematisierung des Themas »Internet« mit Begriffen und Konzepten von Staatlichkeit in deutschsprachigen Medien hin.

Abbildung 1: Häufigkeitsanalyse der Dokumente, in denen das Wort »Staat« zusammen mit dem Begriff »Internet« in Artikeln des* Spiegel, *auf* Heise online *und auf* Netzpolitik.org *vorkommt (aus Dammann/Glasze 2022)*

Inhaltlich beziehen sich diese Problematisierungen von Staatlichkeit vielfach auf Fragen der souveränen Rechtsdurchsetzung etwa im Hinblick auf Verletzungen des Urheberrechts und Verstöße gegen Datenschutzvorschriften oder auf Präventionen und Ahndungen von Cyberkriminalität. Am prominentesten finden sich Forderungen nach mehr Staatlichkeit seit den frühen 2000er-Jahren im Kontext von Debatten um Datenschutz. Zwischen 2000 und 2010 stieg der Anteil von Nutzerinnen und Nutzer des Internets in der deutschen Bevölkerung von 30 auf 82 Prozent[8], während gleichzeitig eine Vielzahl neuer Webdienste und sozialer Medienplattformen entstand (Stichwort: Web 2.0). Eingebettet war diese Entwicklung in eine Phase der Ökonomisierung von personenbezogenen bzw. verhaltensbezogenen Daten, die zu einer intensivierten Produktion, Speicherung und Distribution von digitalen (Meta-)Daten durch kommerzielle Anbieter führte. Die Ausmaße dieser neuen *Datenökonomien* – und die damit verbundenen Sicherheitsproblematiken – wurden durch eine Reihe von Datenskandalen in den 2000er-Jahren immer wieder in öffentlichen Mediendiskursen sichtbar gemacht und problematisiert: 2008 wurde etwa bekannt, dass aus den Rechenzentren von *T-Mobile,* einer Tochtergesellschaft der Deutschen Telekom, die Daten von rund 17 Millionen Kundinnen und Kunden entwendet worden waren.[9] Im Jahr 2009 wurden 1,6 Millionen Datensätze von Kindern und Jugendlichen aus dem sozialen Netzwerk schülerVZ öffentlich.[10] Im selben Jahr erklärte der damalige Bundesdatenschutzbeauftragte Peter Schaar, dass die staatlichen Aufsichtsbehörden mit den großen Mengen illegal zirkulierender Daten deutscher Bürger*innen auf dem digitalen Schwarzmarkt überfordert seien.[11] Darüber hinaus gab es viele ähnliche Skandale bei international operierenden Unternehmen wie AOL, Google, Microsoft und Facebook, die auch in den deutschen Medien aufgegriffen und diskutiert wurden.

Doch nicht nur im Hinblick auf privatwirtschaftliche Unternehmen wurden Problematiken des Datenschutzes in einer »globalen Informationsgesellschaft« sichtbar. Auch die Überwachung der digitalen Kommunikation

8 Datenaufbereitung von Roser, Max/Ritchie, Hannah/Ortiz-Ospina, Esteban (2015): Internet. Online unter: https://ourworldindata.org/internet, abgerufen am 01.10.2021.

9 Vgl. https://www.zeit.de/online/2008/41/telekom-datenklau; 15.10.2021.

10 Vgl. https ://netzpolitik.org/2009/datenleck-bei-schuelervz-war-groesser-als-bekannt; 15.10.2021.

11 Vgl. https ://rp-online.de/digitales/internet/chronik-der-datenskandale; 15.10.2021.

deutscher Bürger*innen durch ausländische – in der Regel US-amerikanische – Geheimdienste wurde zunehmend problematisiert. Ende der 2000er-Jahre konsolidierte sich im Kontext dieser Problematisierungen eine Perspektive, der zufolge staatliche Institutionen zum Schutz deutscher Bürger*innen vor ausländischen Staaten und vor (ausländischen) Unternehmen verstärkt in die digitale Kommunikation intervenieren müssten (vgl. Dammann/Glasze 2022). Diese Sichtweise findet sich auch bei den lange Zeit eher staatskritischen, liberal-progressiven Apologetinnen und Apologeten einer »globalen Informationsgesellschaft« wie etwa dem deutschen Chaos Computer Club (CCC). Der CCC schreibt in einer Stellungnahme 2009:

> »Die bilateralen Abkommen, die den USA und weiteren Staaten unkontrollierten Zugriff auf deutsche Datenbanken verschaffen, […] gehören eingeschränkt. Die deutsche Regierung muß sich auf europäischer Ebene dafür starkmachen, Drittstaaten nicht weiterhin Zugriff auf sensible Daten zu erlauben. Der Staat muß hier die Schutzfunktion für seine Bürger auch im digitalen Raum wahrnehmen.« (Chaos Computer Club 2009)

Darüber hinaus forderten die Mitglieder des CCC im Jahr 2010 stärkere strafrechtliche Maßnahmen gegen kommerzielle Anbieter von digitalen Diensten und Plattformen:

> »Die Datenskandale der letzten Jahre haben eines gezeigt: Die Industrie ist zum verantwortungsvollen Umgang mit sensiblen Daten von Verbrauchern nicht in der Lage. […] Die Strafen für Datenverbrechen müssen drastisch verschärft und eine persönliche Haftbarkeit von Geschäftsführern für Verstöße eingeführt werden.« (Chaos Computer Club 2010)

Die Fragen der souveränen Rechtsdurchsetzung durch staatliche Institutionen und der Übernahme weiterer Schutzfunktionen für die (Daten-)Sicherheit deutscher Bürger*innen waren daher bereits vielfach in den 1990er-Jahren – und dann verstärkt in den 2000er-Jahren – grundlegende Themen der politisch-öffentlichen Debatten in Deutschland zum Internet und zur »globalen Informationsgesellschaft«. Dennoch blieben Forderungen nach staatlicher Souveränität in und über digitale Kommunikationssysteme bis in die frühen 2010er-Jahre deutlich begrenzt. Neben den bereits genannten Warnungen vor der Entstehung eines deutschen Überwachungsstaates und Verweisen auf die Gefahren staatlicher Interventionen für die sozialen und technischen Innovationskräfte des Internets sowie für die internationale Wettbewerbsfähigkeit Deutschlands (vgl. Dammann/Glasze 2022) lässt sich ein weiteres Motiv

für diese Begrenzung erkennen: So dominierten im Diskurs um eine »globale Informationsgesellschaft« vielfach Ideen von zukünftig auf internationaler Maßstabsebene angesiedelten Regelungssystemen – in denen neben technischen Standards der digitalen Kommunikation auch die genannten Probleme des Datenschutzes, des Copyrights und der Cybersicherheit bearbeitet werden sollten (s. hierzu im Detail das folgende Kapitel; vgl. DeNardis 2014; Mueller 2017). Dieser Hoffnung auf internationale Regulierungsansätze der digitalen Kommunikation lag also die Vorstellung einer zumindest teilweisen Verlagerung von staatlichen Souveränitätsprinzipien auf internationale Organisationsstrukturen zugrunde. Als Lösung für die Probleme der »globalen Informationsgesellschaft« wurde in Deutschland daher vielfach eine verstärkte internationale Zusammenarbeit angemahnt und ein Beharren auf territoriale Souveränitätsprinzipien als kontraproduktiv bewertet.[12] Wie wir im nächsten Kapitel zeigen, ließ sich eine solche Organisation auf internationaler Maßstabsebene im Laufe der 2000er-Jahre aber nur sehr begrenzt verankern und durchsetzen – und die Versprechen einer globalen Informationsgesellschaft verloren nach und nach an Plausibilität.

3. Problematisierungen der »globalen Informationsgesellschaft« und Gegenentwürfe für eine »digitale Souveränität« im internationalen Vergleich

Die in Deutschland und vielen weiteren, i.d.R. westlichen Staaten im Laufe der 1990er-Jahre umgesetzten und international proklamierten Regierungsprogramme für eine »globale Informationsgesellschaft« konnten sich weltweit nicht durchsetzen. Gerade in Ländern mit einer deutlicher auf Zentralstaatlichkeit ausgerichteten Regierungspolitik und einer umfassenderen staatli-

12 Bereits die Enquete-Kommission zu »Deutschlands Weg in die Informationsgesellschaft« betonte 1998: »Der Nationalstaat löst sich keineswegs auf. Als einziger, die nationale Fläche beherrschender Hoheitsträger behält er seine wichtigste dauerhafte Funktion als Judikative in der Wahrnehmung und Durchsetzung der Rechtsordnung. Der Regulierungswettbewerb, in dem er sich mit anderen Staaten in der Informationsgesellschaft befinden wird, zwingt jedoch zu einer Beschränkung und Verschlankung staatlicher Aufgaben und Strukturen.« (Deutscher Bundestag 1998: 83) Die Lösung für diesen hier artikulierten Zwang hin zu einem schlanken Staat liegt der Kommission zufolge zum einen »in einer verstärkten internationalen Zusammenarbeit und zum anderen in der Besinnung auf klassische Staatsaufgaben« (ebd.).

chen Kontrolle bzw. Begrenzung von öffentlich-politischen Diskursen – wie etwa in Vietnam, China, Burma/Myanmar, dem Iran, Belarus, Russland, Pakistan, Saudi-Arabien, Thailand, Malaysia oder Indonesien – war die Geschichte des Internets von Beginn an vielfach eingebettet in restriktive staatlich-territoriale Interventionen in digitale Infrastrukturen und Datenzirkulationen (vgl. hierzu etwa Al-Tawil 2001; Warf 2011; Subramanian 2011). Die Überwachung, Filterung und Zensur der digitalen Kommunikation durch staatliche Institutionen stellt daher keinen historischen Bruch und keine Ausnahme in der globalen Geschichte des Internets dar, sondern war und ist vielmehr für den größten Teil der Personen, die weltweit das Internet nutzen, die Regel. In diesem Kontext muss der Idee einer »Wiederherstellung« von staatlicher Kontrolle über das Internet – und Vorstellungen einer »Fragmentierung des Internets« (vgl. Mueller 2017) – vielfach widersprochen werden: Die Infrastrukturen der digitalen Kommunikation wurden in vielen der genannten Länder von Anfang an nach Prinzipien zentralisierter staatlicher Kontrolle und territorialer Souveränität ausgearbeitet und implementiert. Hierzu gehört beispielsweise die planmäßige Installation von staatlich kontrollierten Internetknoten für das *Peering* (Zusammenschluss von Computernetzwerken zum Datenaustausch) bzw. den Transit des transnationalen Datenverkehrs, der Ausbau und die Gestaltung zentraler Netzwerkinfrastrukturen unter staatlicher Schirmherrschaft sowie die umfangreiche staatliche Kontrolle von (privatwirtschaftlichen) Internet-Serviceprovidern (vgl. Goldsmith/Wu 2006; Deibert et al. 2008; Warf 2011). Bereits in den späten 1990er-Jahren deutete sich damit an, dass die digitale Kommunikation in staatszentrierte Regierungsmodelle integriert werden kann. Die Technik des Internets determinierte also keinen »schlanken Staat«, so wie es vielfach von Apologetinnen und Apologeten einer »globalen Informationsgesellschaft« proklamiert wurde. In einer Studie zur globalen Internetzensur stellen Deibert et al. (2008) vielmehr fest: »A key aspect of control online […] is that states have, on an individual basis, defied the cyberlibertarians by asserting control over the online acts of their own citizens in their home states.«

Seit den frühen 2000er-Jahren wurden Ansätze einer staatszentrierten Einbettung der digitalen Kommunikation zunächst v.a. im Kontext der chinesischen Regierung weiter zu einem diskursiven Zusammenhang ausgearbeitet und als politische Forderung etabliert. Die chinesische Regierung hatte bereits Ende der 1990er-Jahre damit begonnen, im Zuge des Golden Shield Projects Techniken zu erwerben und zu entwickeln, die dazu dienen, Informationsflüsse über das Internet für Nutzer*innen im chinesischen Territorium zu

zensieren (vgl. Chandel et al. 2019). In den 2000er-Jahren wurden diese Praktiken der Informationskontrolle in zunehmender Weise öffentlich als Elemente einer staatlichen Souveränität Chinas legitimiert und mit Leitbildern von Autonomie und Nichteinmischung verknüpft, die die chinesische Regierung auch in anderen Politikfeldern propagiert. Gleichzeitig nutzt die chinesische Führung das Schlagwort einer »digitalen Souveränität« seit ca. 2005 und in zunehmender Weise auch als Leitbild einer staatsorientierten, internationalmultilateralen Regulierung des Internets und wendet sich damit gegen den Status quo der *multi-stakeholder governance* des Internets, der als US-dominiert kritisiert wird (vgl. Zeng/Stevens/Chen 2017; Creemers 2020; Thumfart 2021).

In verschiedenen geographischen Kontexten findet seit den späten 2000er-Jahren eine Konsolidierung von zentralstaatlichen und auf Kontrolle ausgerichteten Regierungsmodellen im Bereich der digitalen Kommunikation statt (vgl. Deibert 2015; Cattaruzza et al. 2016; Mueller 2017; Budnitsky/Jia 2018; Lambach 2019; Floridi 2020; Pohle/Thiel 2020; Liu 2021). International wird diese Einbettung der digitalen Kommunikation in staatliche Kontrollstrukturen nicht zuletzt von der chinesischen Administration unter dem Schlagwort »digitale Souveränität« als Gegenentwurf zum schlanken Staat in einer »globalen Informationsgesellschaft« postuliert. Dabei suchte die chinesische Führung den diplomatischen Schulterschluss mit weiteren Regierungen – nicht zuletzt mit der russischen Administration (vgl. McKune/Ahmed 2018; Creemers 2020). Die russische Regierung hat in den 2010er-Jahren – und damit einige Jahre später als China – begonnen, die digitale Kommunikation im eigenen Land zunehmend staatlich zu kontrollieren, nicht zuletzt ausgelöst durch die Beobachtung der vielfach digital organisierten Protestbewegungen in der Arabischen Welt zu Beginn der 2010er-Jahre. Dazu wurde in großer Geschwindigkeit eine Vielzahl rechtlicher und infrastrukturell-technischer Maßnahmen ergriffen, die letztlich auf ein »souveränes RuNet« zielen (vgl. Limonier 2018; Pétiniaud/Limonier/Bertrand 2022). Auch die russische Regierung legitimiert diese Politiken mit einem dezidiert staats- und territorialorientierten Konzept von Souveränität. Gleichzeitig macht sie »digitale Souveränität« zu einem Schlagwort russischer Außenpolitik (vgl. Nocetti 2015). So bringen insbesondere die Delegationen aus Russland und China in den 2000er- und 2010er-Jahren regelmäßig das Konzept einer »digitalen Souveränität« in internationale Debatten ein: z.B. 2003 und 2005 auf dem World Summit on the Information Society (WSIS) der UN-Organisation für Telekommunikation (der International Telecommunication Union, ITU) oder der Generalversammlung der UN 2011 und 2015 (vgl. Margolin 2016;

Creemers 2020). Dabei suchen China und Russland weitergehende internationale Unterstützung für diese Agenda – beispielsweise im Kontext regionaler Kooperation in der Shanghaier Organisation für Zusammenarbeit oder auf den von der chinesischen Führung seit 2014 jährlich organisierten Welt-Internetkonferenzen (vgl. Aronczyk/Budnitzky 2017; Zeng/Stevens/Chen 2017). Unterstützung finden Russland und China dabei einerseits von weiteren autoritär regierten Staaten wie den Regierungen im Iran, in Kasachstan, den Vereinigten Arabischen Emiraten oder Saudi-Arabien, die mit dem Schlagwort »digitale Souveränität« die Kontrolle der digitalen Kommunikation ihrer Bevölkerung legitimieren. Bezüglich der von China und Russland mit »digitaler Souveränität« verknüpften Vorstellung einer staatsorientierten, international-multilateralen Regulierung des Internets und der damit verbundenen Kritik an einer US-amerikanischen Hegemonie werden sie aber andererseits auch von weiteren »BRICS«-Staaten unterstützt (vgl. Thussu 2021) – wie z.B. Indien (vgl. Thomas 2019) oder Südafrika (vgl. Polantin-Reuben/Wright 2014).

Die Suche nach politischen Gegenentwürfen zur »globalen Informationsgesellschaft« und ein zumindest ansatzweiser Erfolg des vielfach durch die chinesische Administration propagierten Modells einer »digitalen Souveränität« zeigt sich international auch in einer Reihe von Ländern des »globalen Südens« wie beispielsweise in Kuba: Bereits in den frühen 2000er-Jahren finden sich in Kuba Forderungen unter dem Schlagwort »technologische Souveränität« im Bereich der digitalen Kommunikation – wobei diese vielfach gegen die USA gerichtet sind. Das Embargo der Vereinigten Staaten gegen Kuba umfasste bis 2009 auch Dienstleistungen und Infrastrukturen von US-amerikanischen Telekommunikationsunternehmen sowie Hard- und Softwareentwicklern – und sollte auch den Ausbau des kubanischen Intranets und dessen Anschluss an globale Internetinfrastrukturen erschweren (vgl. Boas 2000). Erst 2011/12 wurde der Inselstaat durch ein Unterseekabel (ALBA-1) von Venezuela aus an das weltweite Internet angeschlossen[13]. Zuvor hatten i.d.R. nur schwache Satellitenverbindungen zum kubanischen Intranet bestanden (vgl. Deibert et al. 2008). Die kubanische Administration beschloss daher bereits 2004 einen umfassenden Umzug der sporadisch bestehenden digitalen Infrastrukturen auf freie Software. Für Nutzerinnen und Nutzer von Endgeräten sowie für System- und Netzwerkadministratoren wurde hierfür an der 2002 gegründeten Universidad de las Ciencias Informáticas in Havanna unter anderem eine eigene kubanische Linux-Distribution (Nova Linux)

13 Vgl. https ://www.submarinecablemap.com/submarine-cable/alba-1 ; 19.05.2022.

entwickelt. Ziel dieser staatlich orchestrierten freien Softwareinitiative war und ist nach eigenen Angaben eine größere »technologische Souveränität«, nationale Sicherheit und Unabhängigkeit Kubas.[14] Neben diesem auf freier Software aufbauenden Modell einer »technologischen Souveränität« orientiert sich die kubanische Administration seit den 2010er-Jahren vielfach an dem chinesischen Modell einer zentralisierten digitalen Kontrolle und größtmöglichen Unabhängigkeit von US-amerikanischen Tech-Unternehmen. Der Regierungsansatz einer »digitalen Souveränität« in Kuba beinhaltet z.B. die Integration von Zensur- und Überwachungstechniken aus dem chinesischen Golden Shield Project (vgl. Warf 2013) und die Verwendung von Hard- und Software aus chinesischer Fertigung – allen voran von Huawei – für den Ausbau der digitalen Infrastrukturen (vgl. Henken/Garcia Santamaria 2021).

Unter Schlagwörtern einer »digitalen Souveränität« konsolidierten sich international daher im Laufe der 2010er- und frühen 2020er-Jahre eine Reihe von Regierungstechniken und Infrastrukturprojekten, die es zentralstaatlichen und autoritären Regierungssystemen ermöglichten, am ökonomischen Wettbewerb der digitalen Informations- und Kommunikationstechniken zu partizipieren – ohne hierfür die in den 1990er-Jahren postulierten Regierungsmodelle eines schlanken Staates in einer von US-amerikanischen Unternehmen dominierten »globalen Informationsgesellschaft« übernehmen zu müssen. Der Erfolg dieser Gegenentwürfe zur »globalen Informationsgesellschaft« zeigt sich nicht zuletzt auch darin, dass in einer wachsenden Zahl von Staaten mit Verweisen auf »digitale Souveränität« Gesetze zur Lokalisierung von (personenbezogenen) Daten und Infrastrukturprogramme zur Speicherung, Prozessierung und Zirkulation von Daten innerhalb nationaler Territorien (bspw. in Nigeria, China, Russland und im Senegal) begründet und legitimiert werden (vgl. Zeng/Stevens/Chen 2017; Parasol 2018; Liu 2020; Stadnik 2021; Vila Seoane 2021). Aber auch internationale Infrastrukturprojekte werden mit »digitaler Souveränität« verknüpft: China begründet etwa den Ausbau von Unterseekabeln in seiner Digital-Silk-Road-Initiative auch mit Verweisen auf »digitale Souveränität« (vgl. Shen 2018; Hemmings 2020). Gleiches gilt auch für Brasilien, das ausgehend von der NSA-Spionageaffäre 2013 die Verlegung eines Unterseekabels mit Direktverbindung in die EU nicht

14 Vgl. https://revista.jovenclub.cu/novamedia-nova-para-el-diseno-graficonovamedia-nova-for-graphic-design und https://www.nova.cu; 19.05.2022.

als ein technisch-ökonomisches, sondern als ein geopolitisches Projekt für mehr »digitale Souveränität« begreift.[15]

Wie wir im folgenden Kapitel zeigen, zirkulieren Ansätze einer »digitalen Souveränität« seit den 2010er-Jahren aber international nicht nur in den diskursiven Kontexten von Staaten, die den Ideen eines schlanken Staates in einer »globalen Informationsgesellschaft« bereits früh kritisch gegenüberstanden: Innerhalb der EU waren es zunächst Stimmen aus Frankreich, die das Schlagwort einer »digitalen Souveränität« 2006 aufgegriffen haben. In der breiteren öffentlichen Debatte in Frankreich wird »digitale Souveränität« allerdings erst seit Beginn der 2010er-Jahre diskutiert (vgl. Glasze et al. 2022b). In Deutschland werden Schlagwörter einer »digitalen Souveränität« ebenfalls zu Beginn der 2010er-Jahre rezipiert und markieren den Bruch mit der Diskursformation einer »globalen Informationsgesellschaft«.

4. Die Rezeption und Formung »digitaler Souveränität« in Deutschland: Forderungen nach territorialen Schließungen und technischen Kompetenzen im Nachgang zu den »Snowden-Enthüllungen« 2013

In Deutschland wurde das Schlagwort einer »digitalen Souveränität« im Kontext der Enthüllungen der digitalen Spionage durch v.a. US-amerikanische Geheimdienste 2013 aufgegriffen. Wie oben skizziert, wurden einige Konsequenzen der digitalen Vernetzung auch in Deutschland bereits in den 2000er-Jahren problematisiert. Prominent rückten diese Problematiken aber erst im Kontext der NSA-Spionageaffäre im Jahr 2013 in das Blickfeld der breiteren Öffentlichkeit (zur Resonanz der NSA-Spionageaffäre s. Müller 2017; Steiger/Schünemann/Dimmroth 2017). Vor dem Hintergrund der Offenlegung dieser automatisierten Massenüberwachung nahezu der gesamten digitalen Kommunikation durch eine Reihe von Programmen und Systemen US-amerikanischer und britischer Geheimdienste stellte sich nicht mehr nur die Frage, *wie* der deutsche Staat in die digitale Zirkulation eingreifen sollte, sondern in vielen Fällen auch, inwieweit der Staat überhaupt noch die Kompetenz, Fähigkeit und Möglichkeit hat, in die transnationale digitale Kommunikation

15 Vgl. https://aulablog.net/2014/04/28/brazilian-leadership-and-the-global-internet und https://www.spiegel.de/netzwelt/netzpolitik/internet-kabel-von-brasilien-nach-europa-geplant-a-955506.html; 06.09.2022.

einzugreifen. In diesem Zusammenhang bewerteten prominente Politikerinnen und Politiker – oft aus dem politisch konservativen Spektrum – die Spähaktivitäten der NSA als Angriff auf die territoriale Souveränität und Unabhängigkeit des deutschen Staates. Mit Schlagworten wie »digitale Souveränität« und »technologische Souveränität« wurde die Wiederherstellung der staatlichen Eingriffsbefugnisse in den digitalen Datenverkehr gefordert.

So sprach der CSU-Politiker Hans-Peter Uhl im Deutschen Bundestag von einem Verlust der »Regierungsfähigkeit« Deutschlands und bezeichnete die USA in diesem Zusammenhang als »digitale Besatzungsmacht«[16]. Darüber hinaus wurden in diesen Debatten auch Stimmen laut, die eine stärkere staatliche Kontrolle des digitalen Verkehrs forderten. So erklärte der damalige Bundesinnenminister Hans-Peter Friedrich (CSU): »Wir können die digitale Souveränität Europas nur bewahren, wenn es uns gelingt, in Zukunft die technologische Souveränität über die Netzinfrastruktur und die Netztechnologie zu erlangen und zu stärken.«[17] Argumentativ wurden in diesen Reaktionen 2013 vielfach Bilder einer territorialen Abschottung digitaler Datenströme mobilisiert und strategische Ansätze diskutiert, die das Routing von Datenpaketen innerhalb des nationalen Territoriums der Bundesrepublik Deutschland ermöglichen sollten. Dieser Ansatz einer technischen Regulierung der digitalen Kommunikation, bekannt als »Deutschland-Routing« – und manchmal ironisch als »Schlandnet« bezeichnet, – wurde beispielsweise prominent von der Deutschen Telekom aufgegriffen und gefördert. Laut Thomas Kremer, damals Vorstand für Datenschutz, Recht und Compliance bei der Deutschen Telekom, ging es dem größten deutschen Netzbetreiber um »mehr Sicherheit für die Internetnutzer. Dafür muss gewährleistet sein, dass Daten auf möglichst kurzen Strecken vom Sender zum Empfänger gelangen«.[18] Diese Idee eines »Netzes der kurzen Wege«, in dem Datenströme »ohne Umwege durch andere Rechtsräume vom Sender zum Empfänger« geleitet werden, ist allerdings auch auf breite Kritik gestoßen.[19] Dennoch

16 Hans-Peter Uhl, zitiert nach Amman et al. (2014).

17 Hans-Peter Friedrich in: Deutscher Bundestag (Hg.) (2013): Deutscher Bundestag. Plenarprotokoll 18 (2).

18 https://www.telekom.com/de/verantwortung/datenschutz-und-datensicherheit/archiv-datenschutznews/news/sicherheit-telekom-verstaerkt-praesenz-am-internetknoten-de-cix-349806; 15.10.2021.

19 https://www.telekom.com/de/verantwortung/datenschutz-und-datensicherheit/archiv-datenschutznews/news/sicherheit-telekom-verstaerkt-praesenz-am-internetknoten-de-cix-349806; 15.10.2021: Einerseits wurde befürchtet, dass die Deutsche

markierte diese Debatte eine Zäsur gegenüber der Diskursformation einer »globalen Informationsgesellschaft«. Diejenigen, die sich für einen stärker eingreifenden Staat einsetzen, konnten eine gemeinsame Formel für das Problem der digitalen Überwachung und der IT-Sicherheit finden: Staatliche und privatwirtschaftliche Überwachungspraktiken resultieren auch aus einem Mangel an Kompetenzen und Fähigkeiten des deutschen Staates. Nötig sind daher mehr »digitale Souveränität« für Deutschland und ein stärkeres Eingreifen des Staates in die digitale Kommunikation (zur Konjunktur des Begriffes »Souveränität« in deutschsprachigen Mediendiskursen zum Thema Internet s. Abbildung 2).

Abbildung 2: Häufigkeitsanalyse der Dokumente, in denen das Wort »Souveränität« zusammen mit dem Begriff »Internet« in Artikeln des Spiegel, *auf* Heise online *und auf* Netzpolitik.org *vorkommt*

Eigene Analyse und Darstellung; Datenquellen: Spiegel online, Heise online, Netzpolitik.org

Telekom ihr privates Monopol im deutschen Internet ausbauen könnte. Andererseits stellte sich die grundsätzliche Frage, inwieweit eine solche innerdeutsche Weiterleitung von Daten technisch möglich ist. Und nicht zuletzt wurde die Frage aufgeworfen, inwieweit das nationale Routing zu mehr Datenschutz und Sicherheit im Netz führen würde. Die Überwachung von Datenströmen durch Nachrichtendienste finde nicht nur dann statt, wenn sich die Datenpakete physisch außerhalb des deutschen Hoheitsgebiets befinden. So gilt es z.B. als wahrscheinlich, dass US-Geheimdienste über US-Netzbetreiber, die an dem Internetknoten in Frankfurt beteiligt sind, auf Datenströme innerhalb Deutschlands zugreifen können. Progressiv-liberale Akteure forderten daher eine verpflichtende Vollverschlüsselung digitaler Datenströme, um deutsche Bürgerinnen und Bürger vor der Überwachung durch Staaten und Nachrichtendienste zu schützen, anstelle einer staatlich erzwungenen Weiterleitung von Daten innerhalb territorialer Grenzen.

Diese Abkehr von Leitbildern und politischen Programmen eines schlanken Staates, wie sie seit den 1990er-Jahren unter dem Schlagwort der »globalen Informationsgesellschaft« gefordert wurden, hin zu einem stärker eingreifenden und kompetenten (d.h. »souveränen«) Staat wurde nach der NSA-Spähaffäre auch zunehmend in wirtschaftspolitischen Diskursen thematisiert. Die größten Branchenverbände der deutschen IKT-Branche, wie der Bitkom und der ZVEI, problematisierten dabei die gegenwärtige Gestaltung des internationalen Marktes. Einige wenige US-amerikanische und asiatische Unternehmen würden nahezu alle Bereiche und Technologien der digitalen Kommunikation dominieren und damit Unternehmen und öffentliche Verwaltung in Deutschland in eine schwierige Position bringen. In einem Positionspapier schreibt der ZVEI (2015):

> »In einer global vernetzten Welt bestimmen Funktionsfähigkeit und Vertrauenswürdigkeit der genutzten IT-Infrastruktur ganz wesentlich den Fortbestand von Unternehmen, Verwaltung und kritischen Infrastrukturen. Funktionsfähigkeit und Vertrauenswürdigkeit beruhen wiederum auf durchgängigen Kontrollmöglichkeiten aller sicherheitsrelevanten Systemkomponenten und Prozesse. Diese durchgängige Qualitätssicherung ist in Europa derzeit nur bedingt gegeben. Wichtige Schlüsselkomponenten wie z.B. Betriebssysteme, Rechner und Steuerungsanlagen, Router und Firewalls kommen marktbeherrschend aus außereuropäischer Fertigung.«

In diesem Zusammenhang zeichnete der Bitkom ein Leitbild von Deutschland und Europa als »souveräne Systeme«. Diese müssten bei »digitalen Schlüsseltechnologien und -kompetenzen, entsprechenden Diensten und Plattformen über eigene Fähigkeiten auf internationalem Spitzenniveau« verfügen und dabei auch in der Lage sein, »ihr Funktionieren im Inneren zu sichern und ihre Integrität nach außen zu schützen« (Bitkom 2015). Das Ziel einer solchen wirtschaftspolitischen Einbettung der digitalen Kommunikation wurde auch von einer Reihe anderer Akteure im deutschen Wirtschaftsdiskurs aufgegriffen. So stellte das Bundesministerium für Wirtschaft und Energie (BMWi) fest, dass es für die »zukünftige wirtschaftliche Entwicklung Europas und Deutschlands« wichtig sei, »diejenigen Stellen zu identifizieren, die eine technische Kontrolle über die IKT-Gesamtsysteme ermöglichen« (BMWi 2015). Der Beirat Junge Digitale Wirtschaft (BJDW) beim BMWi bemängelte, dass der europäische digitale Binnenmarkt »sich in der Hand außereuropäischer Konzerne« befände, und forderte: »[D]ie digitale Souveränität kann und muss zurückgewon-

nen werden«.[20] Die damalige Bundeskanzlerin Angela Merkel äußerte sich auf dem Weltwirtschaftsgipfel in Davos 2018:

> »Es gibt große amerikanische Unternehmen, die Zugriff auf Daten haben – Daten sind der Rohstoff des 21. Jahrhunderts. Die Antwort auf die Frage ›Wem gehören diese Daten?‹ wird letztendlich darüber entscheiden, ob Demokratie, Partizipation, Souveränität im Digitalen und wirtschaftlicher Erfolg zusammengehen.«[21]

Entsprechende Problematisierungen kommen dabei nicht alleine von marktliberalen und konservativen Stimmen, sondern auch von der parlamentarischen Linken wie dem Abgeordneten der Linkspartei André Hahn: »US-Router haben eingebaute Sicherheitslücken, jene aus China vermutlich auch. Deshalb brauchen wir eine Rückgewinnung an technologischer Souveränität durch die Förderung der Entwicklung von eigener Hard- und Software.«[22]

In den 2010er-Jahren wurde auch in medialen Diskursen zur Internetpolitik in Deutschland die Rolle von Technologieunternehmen bei der Steuerung der digitalen Zirkulation zunehmend problematisiert. Wie schon in den 2000er-Jahren waren es häufig Datenskandale von Unternehmen, die Fragen nach Privatsphäre, informationeller Selbstbestimmung und IT-Sicherheit aufwarfen. Dabei zeigen die Mediendiskurse einerseits deutliche Kontinuitäten in der Problematisierung der Steuerung digitaler Zirkulation, andererseits aber auch Hinweise auf inhaltliche Brüche. Unternehmen werden deutlicher differenziert und dabei national und geographisch positioniert beschrieben: Facebook, Microsoft und Google – alles Unternehmen, die bereits seit mehreren Jahren die digitale Zirkulation in Deutschland prägen – werden nun explizit als *US-amerikanische* Unternehmen beschrieben, die die Privatsphäre und IT-Sicherheit der deutschen Bürgerinnen und Bürger bedrohen. Zugleich wird die deutsche Bundesregierung zum zentralen Adressaten dieser Problematisierungen. Die Gewährleistung der IT-Sicherheit und des Schutzes

20 BJDW (2015): BJDW-Stellungnahme zum Thema EU-Binnenmarkt. Online unter: https://www.bmwi.de/Navigation/DE/Ministerium/Beiraete/beiraete.html, abgerufen am 15.10.2021.

21 Merkel, Angela (2018): Speech at the Annual Meeting of the World Economic Forum in Davos. Online unter: https://www.bundeskanzlerin.de/bkin-de/aktuelles/rede-von-bundeskanzlerin-merkel-beim-jahrestreffen-des-world-economic-forum-am-24-januar-2018-in-davos-455460, abgerufen am 15.10.2021.

22 André Hahn in: Deutscher Bundestag (Hg.) (2018): Deutscher Bundestag. Plenarprotokoll 19 (26).

der Privatsphäre der Bürgerinnen und Bürger wird nun häufig als Pflicht des Staates gesehen. Während in den 2000er-Jahren noch die Begrenzung des Staates im Vordergrund stand, wurden in den 2010er-Jahren Stimmen lauter, die eine Begrenzung ausländischer Unternehmen und der mit ihnen verbundenen ausländischen Staaten durch staatliche Eingriffe forderten (vgl. Dammann/Glasze 2022).

Die wirtschafts- und sicherheitspolitischen Problematiken der digitalen Kommunikation wurden und werden in den politisch-öffentlichen Diskursen der 2010er-Jahre also zunehmend mit Forderungen nach *mehr* staatlichen Eingriffen und mehr Marktmacht für heimische Unternehmen beantwortet. Der heimische Markt wird dabei nicht nur als Quelle wirtschaftlicher Prosperität gefasst, sondern auch als Grundlage von Datenschutz, IT-Sicherheit und letztlich staatlicher Steuerungsfähigkeit. So kam es in den 2010er-Jahren zu einem weiteren Bruch gegenüber der Diskursformation einer »globalen Informationsgesellschaft«: Während im Diskurs einer »globalen Informationsgesellschaft« in den 1990er-Jahren die Integration Deutschlands in einen digital vernetzten internationalen Markt als Quelle für wirtschaftlichen Wohlstand und sozialen Fortschritt galt, tauchen nun Ansätze in den Problematisierungen einer »digitalen Souveränität« auf, in denen diese Ziele durch die Regulierung und den Schutz des Binnenmarktes erreicht werden sollen.

Der Begriff der »digitalen Souveränität« wird dabei nicht ausschließlich auf den Staat bezogen, sondern in zunehmender Weise auch für Organisationen und Individuen eingefordert. So sprechen Wirtschaftsverbände[23] und das Bundesministerium für Wirtschaft (BMWi 2021) von »digital souveränen Unternehmen«, viele Kommunen und Bundesländer erklären »digitale Souveränität« zu einem politischen Ziel[24] und zahlreiche Organisationen der Zivilgesellschaft fordern eine »digital souveräne Gesellschaft«[25]. Dabei wird

23 Bspw. 2020 der Fachverband Software und Digitalisierung innerhalb des Verbandes Deutscher Maschinen- und Anlagenbauer (https://www.vdma.org/software-digitalisierung; 07.01.2022).

24 So haben sich bspw. die Koalitionspartner in Hamburg 2020 darauf verständigt, dass Hamburg »digital souverän« werden soll, und der 2021 etablierte Senat von Berlin will eine »digital souveräne Stadt« schaffen (https://spd.berlin/media/2021/11/Koalitionsvertrag-Zukunftshauptstadt-Berlin.pdf; 10.01.2021). Der Deutsche Städtetag legt 2020 ein Positionspapier vor, mit dem er die »Digitale Souveränität von Kommunen stärken« will (https://www.staedtetag.de/positionen/positionspapiere/diskussionspapier-digitale-souveraenitaet-kommunen-staerken).

25 Siehe bspw. die Initiative: https://digitalezivilgesellschaft.org/; 10.01.2022.

vielfach explizit die Figur eines »digital souveränen Individuums« entworfen (s. hierzu Winkler/Dammann 2022). Die Figur des »digital souveränen Individuums« knüpft dabei erstens an medienpädagogische Debatten zur individuellen Kompetenz von Mediennutzenden an (s. Beitrag Müller/Kammerl 2022 in diesem Band). Gleichzeitig wird sie zweitens vor dem Hintergrund der Debatten um Wahlbeeinflussungen in digitalen Medien und »*alternative facts*« mit Forderungen nach politisch aufgeklärten und mündigen Bürgerinnen und Bürgern verknüpft (s. Beitrag Odzuck 2022 in diesem Band). Und drittens schließt sie an geoökonomische und geopolitische Debatten an: Das digital souveräne Individuum ist dabei einerseits ein digital kompetentes Subjekt, das den ökonomischen Erfolg Deutschlands (bzw. Europas) in der Digitalisierung sicherstellen soll. Andererseits verkörpert diese Figur – vorgestellt als ein eigenständig, aufgeklärt und souverän handelndes Subjekt – gewissermaßen die spezifisch werteorientierten Leitbilder deutscher Digitalpolitik gegenüber einem als US-amerikanisch beschriebenen digitalen Kapitalismus und einem vielfach als chinesisch dominiert angesehenen digitalen Autoritarismus (vgl. Winkler/Dammann 2022).

5. Fazit und Ausblick: Öffnung und Europäisierung »digitaler Souveränität«

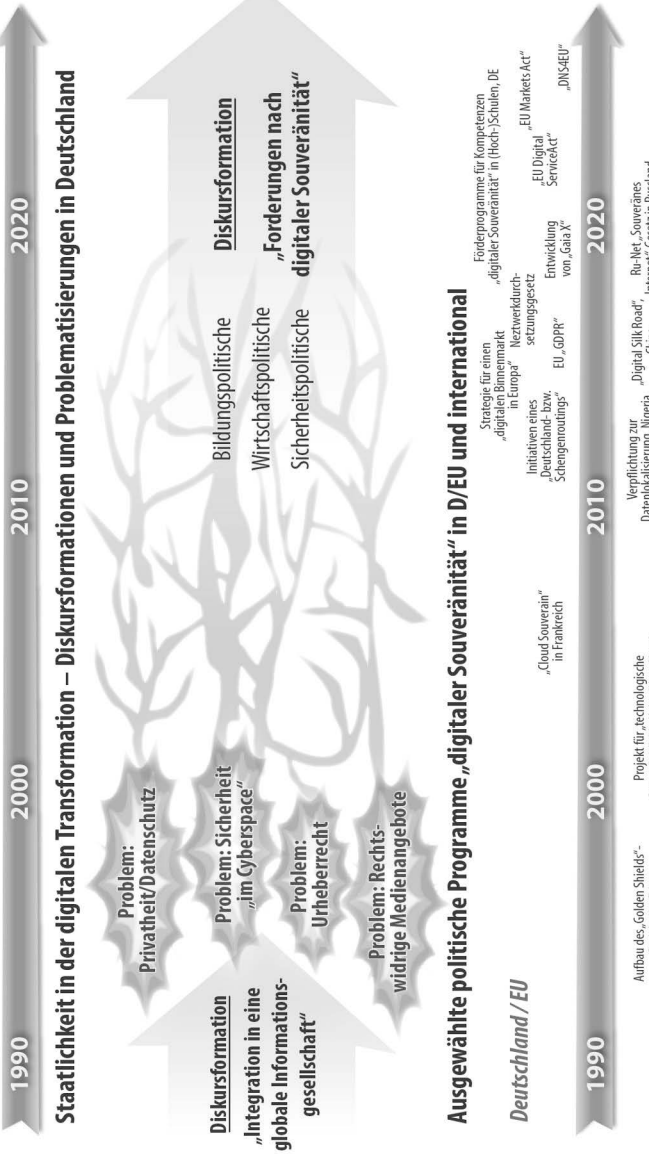
Wie die historische Rekonstruktion öffentlich-politischer Diskurse in Deutschland zeigt, wurden digitale Kommunikationssysteme in den 1990er-Jahren auch in Deutschland in erster Linie als Treiber einer Vernetzung und Überwindung von Grenzen diskutiert. Das Leitbild der »Integration in eine globale Informationsgesellschaft« prägte die Telekommunikationspolitiken. Der Staat sollte als Infrastrukturanbieter und Regulierer zurückgedrängt und begrenzt werden. Allerdings wurden dabei zumindest vereinzelt ab den 2000er-Jahren auch erste kritische Stimmen laut, die eher nach *mehr* staatlichem Einfluss im Digitalen rufen – beispielsweise bei Fragen von Datenschutz und Urheberrecht.

Das Schlagwort einer »digitalen Souveränität«, wie es zu Beginn der 2010er-Jahre v.a. in diskursiven Kontexten der autoritären Regierungen in China und Russland ausgearbeitet worden war und hier in erster Linie orientiert an Vorstellungen staatlich-territorialer Souveränität, wurde in den öffentlich-politischen Debatten in Deutschland erst 2013 aufgegriffen. Im Nachgang der Enthüllungen von Edward Snowden beklagten dabei zahlreiche

Politikerinnen und Politiker einen staatlichen Kontrollverlust und skizzierten Forderungen nach einer staatlich-territorialen Abschließung von Datenströmen. Auch wenn sich diese Forderungen nicht in konkrete Politiken übersetzt haben, so markiert das Schlagwort dennoch eine markante Diskursverschiebung in der deutschen Digitalpolitik: Forderungen nach »mehr Staat« werden in den 2010er-Jahren zunehmend hegemonial und bilden gewissermaßen einen neuen Konsens in der Digitalpolitik – »digitale Souveränität« ist damit das Schlagwort einer neuen diskursiven Formation.

Dabei wird »digitale Souveränität« in den öffentlich-politischen Debatten in Deutschland rasch nicht nur an Vorstellungen staatlich-territorialer Souveränität orientiert, sondern mit einer Vielzahl weiterer gesellschaftlicher Forderungen verbunden: Fragen nach der Handlungsfähigkeit, den Kompetenzen und der Selbstbestimmung von Organisationen (bspw. Wirtschaftsunternehmen und Kommunen) sowie Individuen (»der/die digital souveräne Bürger/Bürgerin«) werden ebenfalls mit dem Schlagwort der »digitalen Souveränität« verknüpft. Der enorme Erfolg, den »digitale Souveränität« Ende der 2010er- und Anfang der 2020er-Jahre im öffentlich-politischen Diskurs in Deutschland hat, lässt sich also nicht zuletzt damit erklären, dass unterschiedliche politische Forderungen sich in diesem Schlagwort treffen können: (a) sicherheitspolitische Positionen, die im Sinne staatlich-territorialer Souveränität eine Stärkung Deutschlands bzw. der EU fordern, (b) wirtschaftspolitische Positionen, die eine Förderung »heimischer« Unternehmen und mehr Unabhängigkeit von ausländischen Monopolen erreichen möchten, (c) Stimmen aus dem Kontext der Open-Source-/Open-Software-Bewegung, die eine Begrenzung der Marktmacht der internationalen Tech-Unternehmen anstreben, (d) progressive netzpolitische Stimmen, die vom Staat sowohl Sicherheit der Bürger*innen gegenüber Überwachung und Kriminalität als auch mehr bürgerliche Teilhabe am Netz fordern, sowie nicht zuletzt (e) bildungspolitische Stimmen, die sich humanistischen Idealen selbstbestimmter Individuen verpflichtet sehen – und Individuen zu eigenständigen Entscheidungen und souveränen Handlungskompetenzen in der digitalen Welt verhelfen möchten. Die Zusammenführung dieser Forderungen unter dem Schlagwort »digitale Souveränität« ermöglicht die Legitimierung und Umsetzung neuer digitalpolitischer Programme in verschiedenen Feldern der formalen Politik.

Abbildung 3: Diskurse und Programme einer »digitalen Souveränität« in Deutschland und international



Seit Ende der 2010er- und insbesondere seit Beginn der 2020er-Jahre wird das Schlagwort der »digitalen Souveränität« zudem intensiv von den Institutionen der Europäischen Union aufgegriffen – in hohem Maße vorangetrieben von Apologetinnen und Apologeten aus Deutschland und Frankreich. Die EU entwickelt eine digitale Agenda, die sich nicht mehr nur auf den Binnenmarkt und die Einbindung in globale Zusammenhänge konzentriert, sondern auf die Schaffung europäischer Standards mit globaler Wirkung abzielt. Sie engagiert sich zunehmend für eine europäische digitale Industriepolitik sowie die Entwicklung digitaler Infrastrukturen und diskutiert strategische Fragen der Cybersicherheit. Mit digitalen Datenschutzstandards wie der Datenschutz-Grundverordnung oder dem Cloud-Projekt Gaia-X versucht die EU, die Größe ihres eigenen Binnenmarktes und ihre Regulierungskapazität zu nutzen, um ihre digitalen Standards zu globalisieren (vgl. Glasze et al. 2022b). Die Europäische Kommission definiert dabei »digitale« bzw. »technologische Souveränität« als Verteidigung europäischer Werte und positioniert sich gleichzeitig als Verfechterin eines offenen, dezentralisierten, ungeteilten Internets der freien Märkte (vgl. Europäische Kommission 2021). Mit dieser Kombination aus faktischer Regulierungsmacht und werteorientierter Legitimation baut die EU ein alternatives Modell der digitalen Transformation auf als dritte Option neben den Vereinigten Staaten und China in den aktuellen globalen geopolitischen und geoökonomischen Kämpfen um die Gewinne der digitalen Transformation (s. auch Hobbs 2020 und Christakis 2020). »Digitale Souveränität« wird damit zu einem Baustein der Entwicklung einer geopolitischen Agenda der EU.

Interessanterweise werden in der deutschen Debatte (zumindest bis zur Fertigstellung dieses Beitrages im Frühjahr 2022) die Spannungsfelder und Widersprüche zwischen den unterschiedlichen Forderungen, die mit »digitaler Souveränität« verknüpft werden, kaum problematisiert – beispielsweise Widersprüche zwischen Vorstellungen von Souveränität als (individuelle bzw. kollektiv-demokratische) Selbstbestimmung und Souveränität als zentralisierte staatliche Herrschaft (eine Ausnahme sind die Beiträge von Thiel 2019, 2021; s. dazu auch die Einleitung von Glasze/Odzuck/Staples 2022 sowie den Beitrag von Odzuck 2022 in diesem Band). Die historische Rekonstruktion und internationale Kontextualisierung in diesem Beitrag mag daher auch zu einer Sensibilisierung der weiteren Debatte beitragen.

Literaturverzeichnis

Al-Tawil, Khalid M. (2001): »The internet in Saudi Arabia«, in: Telecommunications Policy 25 (8–9), S. 625–632, https://doi.org/10.1016/S0308-5961(01)00036-2.

Amman, Thomas/Banse, Dirk/Bewarder, Manuel/Flade, Florian/Malzahn, Claus C./Müller, Uwe (2014): »Digitale Besatzungsmacht«, in: Die Welt vom 06.07.2014.

Aronczyk, Melissa/Budnitzky, Stanislav (2017): »Nation branding and internet governance: Framing debates over freedom and sovereignty«, in: Uta Kohl (Hg.), The net and the nation sate. Multidisciplinary perspectives on the internet governance, Cambridge: Cambridge University Press, S. 48–65.

August, Vincent (2021): Technologisches Regieren, Bielefeld: transcript.

Auswärtiges Amt (2020): Gemeinsam. Europa wieder stark machen. Programm der deutschen Ratspräsidentschaft. Online unter: https://www.eu2020.de, abgerufen am 15.06.2022.

Barbrook, Richard/Cameron, Andy (1996): »The Californian ideology«, in: Science as Culture 6 (1), S. 44–72, doi.org/10.1080/09505439609526455.

Bitkom (2015): Digitale Souveränität. Positionsbestimmung und erste Handlungsempfehlungen für Deutschland und Europa. Online unter: https://www.bitkom.org/Bitkom/Publikationen/Digitale-Souveraenitaet-Positionsbestimmung-und-erste-Handlungsempfehlungen-fuer-Deutschland-und-Europa.html, abgerufen am 15.10.2021.

BMWi – Bundesministerium für Wirtschaft (2015): Industrie 4.0 und Digitale Wirtschaft. Impulse für Wachstum, Beschäftigung und Innovation. Online unter: https://www.bmwk.de/Redaktion/DE/Publikationen/Industrie/industrie-4-0-und-digitale-wirtschaft.pdf%3F__blob%3DpublicationFile%26v%3D3, abgerufen am 19.05.2022.

BMWi – Bundesministerium für Wirtschaft und Energie (2021): Schwerpunktstudie Digitale Souveränität. Bestandsaufnahme und Handlungsfelder. Online unter: https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/schwerpunktstudie-digitale-souveranitaet.pdf?__blob=publicationFile&v=6, angerufen am 19.05.2022.

Boas, Taylor C. (2000): »The dictator's dilemma? The internet and U.S. policy toward Cuba«, in: The Washington Quarterly 23 (3), S. 57–67, https://doi.org/10.1162/016366000561178.

Budnitsky, Stanislav/Jia, Lianrui (2018): »Branding internet sovereignty: Digital media and the Chinese–Russian cyberalliance«, in: European Journal of Cultural Studies 21 (5), S. 594–613, https://doi.org/10.1177/1367549417751151

Castells, Manuel (1994): »Space of flows – Raum der Ströme. Eine Theorie des Raums in der Informationsgesellschaft«, in: Peter Noller/Walter Prigge/Klaus Ronneberger (Hg.), Stadt-Welt. Über die Globalisierung städtischer Milieus, Frankfurt a.M.: Campus, S. 120–134.

Castells, Manuel (2000): The rise of the network society, Malden/Oxford: Wiley-Blackwell.

Cattaruzza, Amaël/Danet, Didier/Taillat, Stéphane/Laudrain, Arthur (2016): »Sovereignty in cyberspace: Balkanization or democratization«, in: International Conference on Cyber Conflict (CyCon U.S.), S. 1–9, https://doi.org/10.1109/CYCONUS. 2016.7836628.

Chandel, Sonali/Jingji, Zang/Yunnan, Yu/Jingyao, Sun/Zhipeng, Zhang (2019): »The golden shield project of China: A decade later—an in-depth study of the great firewall«, in: 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), IEEE, S. 111–119, https://doi.org/10.1109/CyberC.2019.00027.

Chaos Computer Club (2009): Chaos Computer Club verschenkt Spickzettel digitaler Bürgerrechte für die weiteren Koalitionsverhandlungen. Online unter: https://www.ccc.de/de/updates/2009/pm-spickzettel, abgerufen am 15.10.2021.

Chaos Computer Club (2010): Forderungen für ein lebenswertes Netz. Online unter: https://www.ccc.de/de/updates/2010/forderungen-lebenswertes-netz, abgerufen am 15.10.2021.

Chenou, Jean-Marie (2014): »From cyber-libertarianism to neoliberalism: Internet exceptionalism, multi-stakeholderism, and the institutionalisation of internet governance in the 1990«, in: Globalizations 11 (2), S. 205–223.

Christakis, Theodore (2020): »›European digital sovereignty‹: Successfully navigating between the ›Brussels effect‹ and Europe's quest for strategic autonomy«, in: SSRN Journal 7, https://doi.org/10.2139/ssrn.3748098.

Couture, Stephane/Toupin, Sophie (2019): »What does the notion of ›sovereignty‹ mean when referring to the digital?« in: New Media & Society 21 (10), S. 2305–2322.

Creemers, Rogier (2020): »China's conception of cyber sovereignty«, in: Dennis Broeders/Bibi van den Berg (Hg.), Governing cyberspace. Behavior, power, and diplomacy (= Digital technologies and global politics), Lanham: Rowman & Littlefield, S. 107–144.

Dammann, Finn/Glasze, Georg (2022, im Druck): »Governing Digital Circulation: the Quest for Data Control and Sovereignty in Germany«, in: Territory, Politics, Governance.

Deibert, Ronald (2015): »The geopolitics of cyberspace after Snowden«, in: Current History 114 (768), S. 9–14.

Deibert, Ronald/Palfrey, John/Rohozinski, Rafal/Zittrain, Jonathan (Hg.) (2008): Access denied: The practice and policy of global internet filtering, Cambridge/London: MIT Press.

Deutscher Bundestag (1998): Schlussbericht der Enquete-Kommission Zukunft der Medien in Wirtschaft und Gesellschaft – Deutschlands Weg in die Informationsgesellschaft. Drucksache 13/11004. Online unter: http://dip21.bundestag.de/dip21/btd/13/110/1311004.pdf, abgerufen am 01.10.2021.

Ermoshina, Ksenia/Musiani, Francesca (2017): »Migrating servers, elusive users: Reconfigurations of the Russian internet in the post-snowden era«, in: Media and Communication 5 (1), S. 42–53, https://doi.org/10.17645/mac.v5i1.816.

Europäische Kommission (1994): Report on Europe and the global information society. Bulletin of the European Union, Supplement 2/94. Online unter: http://aei.pitt.edu/1199/1/info_society_bangeman_report.pdf, abgerufen am 14.02.2022.

Europäische Kommission (2021): 2030 digital compass: The European way for the digital decade. Online unter: https://data.europa.eu/doi/10.2759/425691, abgerufen am 19.05.2022.

Floridi, Luciano (2020): »The fight for digital sovereignty: What it is, and why it matters, especially for the EU«, in: Philosophy and Technology 33 (3), S. 369–378, https://doi.org/10.1007/s13347-020-00423-6.

Foucault, Michel (1973): Archäologie des Wissens, Frankfurt a.M.: Suhrkamp.

Friedman, Thomas L. (2007): The world is flat: A brief history of the twenty-first century, New York: Farrar Straus & Giroux.

Glasze, Georg/Cattaruzza, Amaël/Douzet, Frédérick/Dammann, Finn/Bertran, Marie-Gabrielle/Bômont, Clotilde/Braun, Matthias/Danet, Didier/Desforges, Alix/Géry, Aude/Grumbach, Stéphane/Hummel, Patrik/Limonier, Kevin/Münßinger, Max/Nicolai, Florian/Pétiniaud, Louis/Winkler, Jan/Zanin, Caroline (2022a): »Contested spatialities of digital sovereignty«, in: Geopolitics vom 05.04.2022, https://doi.org/10.1080/14650045.2022.2050070.

Glasze, Georg/Dammann, Finn (2021): »Von der globalen Informationsgesellschaft zum Schengenraum für Daten – Raumkonzepte in der Regie-

rung der digitalen Transformation in Deutschland«, in: Thomas Döbler/Christian Pentzold/Christian Katzenbach (Hg.), Räume digitaler Kommunikation. Lokalität – Imagination – Virtualisierung, Köln: Herbert von Halem Verlag, S. 159–182.

Glasze, Georg/Dammann, Finn/Münßinger, Max/Bômont, Clotilde/Danet, Didier/Desforges, Alix (2022b): »Reception and elaboration of ›digital sovereignty‹ in three European discourse arenas: France, Germany, and the EU«, in: Geopolitics, Forum Contested Spatialities of Digital Sovereignty, https://doi.org/10.1080/14650045.2022.2050070.

Glasze, Georg/Odzuck, Eva/Staples, Ronald (2022): »Einleitung: Digitalisierung als Herausforderung – ›Souveränität‹ als Antwort? Konzeptionelle Hintergründe der Forderungen nach ›digitaler Souveränität‹«, in: Georg Glasze/Eva Odzuck/Ronald Staples (Hg.), Was heißt digitale Souveränität? Diskurse, Praktiken und Voraussetzungen »individueller« und »staatlicher Souveränität« im digitalen Zeitalter, Bielefeld: transcript, S. 7–28.

Goldsmith, Jack L./Wu, Tim (2006): Who controls the internet? Illusions of a borderless world, Oxford: Oxford University Press.

Hannah, Matthew G. (2009): »Calculable territory and the West German census boycott movements of the 1980s«, in: Political Geography 28 (1), S. 66–75, https://doi.org/10.1016/j.polgeo.2008.12.001.

Hemmings, John (2020): »Reconstructing order: The geopolitical risks in China's digital silk road«, in: Asia Policy 27 (1), S. 5–21, https://doi.org/10.1353/asp.2020.0002.

Henken, Ted/Garcia Santamaria, Sara (Hg.) (2021): Cuba's digital revolution: Citizen innovation and state policy, Gainesville: University of Florida Press.

Hobbs, Carla (Hg.) (2020): Europe's digital sovereignty: From rulemaker to superpower in the age of US-China rivalry, London: European Council on Foreign Relations. Online unter https://ecfr.eu/publication/europe_digital_sovereignty_rulemaker_superpower_age_us_china_rivalry, abgerufen am 19.05.2022.

Hong, Yu/Goodnight, Gerald Thomas (2020): »How to think about cyber sovereignty: the case of China«, in: Chinese Journal of Communication 13 (1), S. 8–26.

Hummel, Patrik/Braun, Matthias/Tretter, Max/Dabrock, Peter (2021): »Data sovereignty: A review«, in: Big Data & Society 8 (1), https://doi.org/10.1177/2053951720982012.

Keller, Christel (1998): Der Begriff »Globale Informationsgesellschaft«: Wissenschaftliche Theorie – Politisches Programm – Globalisierte Geschäftssphä-

re. Zur politischen Steuerung der Entwicklung und nationalökonomischen Nutzung der Informationstechnik, Tübingen: Wilhelm-Schickard-Institut für Informatik.

Lambach, Daniel (2019): »The territorialization of cyberspace«, in: International Studies Review 22 (3), S. 482–506, https://doi.org/10.1093/isr/viz022.

Limonier, Kevin (2018) : Ru.net. Géopolitique du cyberespace russophone (= Les Carnets de l'Observatoire), Paris/Moskau : L'Inventaire.

Liu, Jinhe (2020): »China's data localization«, in: Chinese Journal of Communication 13 (1), S. 84–103, https://doi.org/10.1080/17544750.2019.1649289.

Liu, Lizhi (2021): »The rise of data politics: Digital China and the world«, in: Studies in Comparative International Development 56 (1), S. 45–67, https://doi.org/10.1007/s12116-021-09319-8.

Margolin, Jack (2016): »Russia, China and the push for ›digital sovereignty‹«, in: Global Observatory vom 02.12.2016. Online unter: theglobalobservatory.org/2016/12/russia-china-digital-sovereignty-shanghai-cooperation-organization, abgerufen am 19.05.2022.

Maull, Hans W. (2007): »Deutschland als Zivilmacht«, in: Siegmar Schmidt (Hg.), Handbuch zur deutschen Außenpolitik. Wiesbaden: VS Verlag für Sozialwissenschaften, S. 73–84.

McKune, Sarah/Ahmed, Shazeda (2018): »The contestation and shaping of cyber norms through China's internet sovereignty agenda«, in: International Journal of Communication 12, S. 3835–3855.

Mueller, Milton (2017): Will the internet fragment? Sovereignty, globalization and cyberspace (= Digital Future Series), Cambridge/Malden: Polity Press.

Müller, Jane/Kammerl, Rudilf (2022): »›Digitale Souveränität‹: Zielperspektive einer Bildung in Zeiten tiefgreifender Mediatisierung?«, in: Georg Glasze/Eva Odzuck/Ronald Staples (Hg.), Was heißt digitale Souveränität? Diskurse, Praktiken und Voraussetzungen »individueller« und »staatlicher Souveränität« im digitalen Zeitalter, Bielefeld: transcript, S. 201–228.

Nocetti, Julien (2015): »Contest and conquest: Russia and global internet governance«, in: International Affairs 91 (1), S. 111–130, https://doi.org/10.1111/1468-2346.12189.

Odzuck, Eva (2022): »›*Demokratische* digitale Souveränität‹. Plädoyer für einen normativen Begriff am Beispiel des digitalen Wahlkampfs«, in: Georg Glasze/Eva Odzuck/Ronald Staples (Hg.), Was heißt digitale Souveränität? Diskurse, Praktiken und Voraussetzungen »individueller« und »staatlicher Souveränität« im digitalen Zeitalter, Bielefeld: transcript, S. 127–158.

Open Source Business Alliance – Bundesverband für digitale Souveränität e.V. (Hg.) (2021): Manifest für digitale Souveränität. Online unter: https://osb-alliance.de/publikationen/veroeffentlichungen/manifest-fuer-digitale-souveraenitaet, abgerufen am 19.05.2022.

Parasol, Max (2018): »The impact of China's 2016 cyber security law on foreign technology firms, and on China's big data and smart city dreams«, in: Computer Law and Security Review 34 (1), S. 175–179, https://doi.org/10.1016/j.clsr.2017.05.022.

Perritt, Henry H. Jr. (1998): »The internet as a threat to sovereignty? Thoughts on the internet's role in strengthening national and global governance«, in: Indiana Journal of Global Legal Studies 5 (2), Article 4.

Pétiniaud, Louis/Limonier, Kevin/Bertrand, Marie-Gabrielle (2022): »Russia's pursuit of digital sovereignty: Political, industrial and foreign policy implications and limits«, in: Geopolitics, Forum Contested Spatialities of Digital Sovereignty, https://doi.org/10.1080/14650045.2022.2050070.

Pohle, Julia/Thiel, Thorsten (2020): »Digital sovereignty«, in: Internet Policy Review 9 (4), https://doi.org/10.14763/2020.4.1532.

Polatin-Reuben, Dana/Wright, Joss (2014): An internet with BRICS characteristics: Data sovereignty and the Balkanisation of the internet, Usenix. Online unter: https://www.usenix.org/system/files/conference/foci14/foci14-polatin-reuben.pdf, abgerufen am 19.05.2022.

Reiberg, Abel (2017): »The construction of a new policy domain in debates on German internet policy«, in: European Policy Analysis 3 (1), S. 146–167, https://doi.org/10.1002/epa2.1001.

Reiberg, Abel (2018): Netzpolitik: Genese eines Politikfeldes, Berlin: Nomos.

Sassen, Saskia (1996): Losing control? Sovereignty in an age of globalization. New York: Columbia University Press.

Seibel, Benjamin (2016): Cybernetic government. Informationstechnologie und Regierungsrationalität von 1943–1970, Wiesbaden: Springer VS.

Shen, Hong (2018): »Building a digital silk road? Situating the internet in China's belt and road initiative«, in: International Journal of Communication, 12. Online unter: https://ijoc.org/index.php/ijoc/article/view/8405 abgerufen am 19.05.2022.

Stadnik, Ilona (2021): »Control by infrastructure: Political ambitions meet technical implementations in RuNet«, in: First Monday 26 (3–5), https://doi.org/10.5210/fm.v26i5.11693.

Steiger, Stefan/Schünemann, Wolf J./Dimmroth, Katharina (2017): »Outrage without consequences? Post-Snowden discourses and governmental practice in Germany«, in: MaC 5 (1), S. 7, doi.org/10.17645/mac.v5i1.814.

Thiel, Thorsten (2019): »Souveränität: Dynamisierung und Kontestation in der digitalen Konstellation«, in: Jeanette Hofmann/Norbert Kersting/Claudia Ritzi/Wolf J. Schünemann (Hg.), Politik in der digitalen Gesellschaft. Zentrale Problemfelder und Forschungsperspektiven, Bielefeld: transcript, S. 47–60.

Thiel, Thorsten (2021): »Das Problem mit der digitalen Souveränität«, in: Frankfurter Allgemeine. Online unter: https://www.faz.net/aktuell/wirtschaft/digitec/europa-will-in-der-informationstechnologie-unabhaengiger-werden-17162968.html, abgerufen am 19.05.2022.

Thomas, Pradip Ninan (2019): The politics of digital India. Between local compulsion and transnational pressures, Oxford: Oxford University Press.

Thumfart, Johannes (2021): »The norm development of digital sovereignty between China, Russia, the EU and the US: From the late 1990s to the COVID crisis 2020/21 as catalytic event«, in: Dara Hallinan/Ronald Leenes/Paul de Hert (Hg.), Data protection and privacy. Enforcing rights in a changing world (= Computers, privacy and data protection, Band 14), S. 1–44.

Thussu, Daya Kishan (2021): »BRICS de-Americanizing the internet?«, in: Daya Kishan Thussu/Kaarle Nordenstreng (Hg.), BRICS media. Reshaping the global communication order? (= Internationalizing media studies), Abingdon/Oxon/New York: Routledge, S. 280–301.

Toal, Gerard (1999): »Borderless worlds? Problematising discourses of deterritorialisation«, in: Geopolitics 4 (2), S. 139–154.

Vila Seoane, Maximiliano Facundo (2021): »Data securitisation: The challenges of data sovereignty in India«, in: Third World Quarterly 42 (8), S. 1733–1750, https://doi.org/10.1080/01436597.2021.1915122.

Warf, Barney (2011): »Geographies of global internet censorship«, in: GeoJournal 76 (1), S. 1–23, https://doi.org/10.1007/s10708-010-9393-3.

Warf, Barney (2013): Global geographies of the internet (= SpringerBriefs of Geography, Band 1), Dordrecht u.a.: Springer, https://doi.org/10.1007/978-94-007-1245-4.

Winkler, Jan/Dammann, Finn (2022): »Digitally Competent – Digitally Sovereign – Digitally Civic: Geopolitics of Subject Formation in the German Context«, in: Geopolitics, Forum Contested Spatialities of Digital Sovereignty, S. 1–40, https://doi.org/10.1080/14650045.2022.2050070.

Zeng, Jinghan/Stevens, Tim/Chen, Yaru (2017): »China's solution to global cyber governance: Unpacking the domestic discourse of ›internet sovereignty‹«, in: Politics & Policy 45 (3), S. 432–464, https://doi.org/10.1111/polp.12202.

ZVEI (2015): Positionspapier. Stärkung vertrauenswürdiger IT-Infrastrukturen in Deutschland und Europa. Online unter: https://www.teletrust.de/fileadmin/docs/publikationen/broschueren/Digitale_Souver%C3%A4nit%C3%A4t/ZVEI_TeleTrusT_Diskussionspapier_Digitale_Souver%C3%A4nit%C3%A4t.pdf, abgerufen am 15.10.2021.

Soziotechnische Einflussfaktoren auf die »digitale Souveränität« des Individuums

Zinaida Benenson, Felix Freiling, Klaus Meyer-Wegener

Abstract *Dieses Kapitel nimmt eine eher technische Perspektive auf das Problem der »digitalen Souveränität« des Subjekts ein. Wir betrachten drei verschiedene soziotechnische Entwicklungen, die die Möglichkeit beeinflussen, in einer digitalisierten Welt ein selbstbestimmtes und autonomes Leben zu führen. Die erste Entwicklung betrifft die zunehmende Abhängigkeit von wenigen großen Diensteanbietern, die zwar für die Sicherheit der Nutzenden sorgen, aber gleichzeitig auch über die uneingeschränkte Macht über Daten und Geräte verfügen. Die zweite Entwicklung betrifft den Mangel an menschenzentrierter Gestaltung von Schutzmechanismen, der die realistische Wahrnehmung möglicher Bedrohungen erschwert. Die dritte und letzte Entwicklung bezieht sich auf unklare Vorstellungen über die Genauigkeit und die Nützlichkeit von gesammelten Daten. In der Gesamttendenz führen diese Entwicklungen zu starken Einschränkungen – sowohl im Hinblick auf die faktische als auch auf die selbst wahrgenommene Souveränität.*

1. Einleitung

Mehr als die Hälfte der Weltbevölkerung nutzt heute das Internet. Vielen ist dabei nicht bewusst, dass sie ein Netzwerk von verbundenen Computern nutzen, und viele weitere wissen nicht, dass Regierungen und internationale Konzerne bei der Benutzung des Internets ihre persönlichen Daten für eine Vielzahl von Zwecken sammeln und verarbeiten. Die digitale Transformation führt zunehmend zu einer Gesellschaft, in der eine aktive Teilhabe ohne Computer- und Internetnutzung kaum noch möglich ist. In diesem Kapitel legen wir den Fokus auf die »digitale Souveränität« des Subjekts, also die Möglichkeit, unter den oben beschriebenen Umständen ein selbstbestimmtes und autonomes Leben zu führen – sowohl im Hinblick auf die faktische als auch auf die selbst

wahrgenommene Souveränität des Individuums. Aus einer soziotechnischen Perspektive stellen wir allgemeine Beobachtungen zu drei relevanten Phänomenen an, die die »digitale Souveränität« stark beeinflussen und die mit den technischen Entwicklungen der Digitalisierung zusammenfallen.

Die erste Entwicklung wird durch den von Bruce Schneier (2012) geprägten Begriff der »feudalen Sicherheit« charakterisiert, der besagt, dass die Nutzenden heute vollständig von einem einzigen großen Diensteanbieter (oder einigen wenigen Diensteanbietern) abhängig sind. Diese Anbieter sorgen zwar für die Sicherheit der Personen, die die Dienste nutzen, haben aber auch uneingeschränkte Macht sowohl über ihre Daten als auch über die Funktionalität ihrer Geräte.

Die zweite Entwicklung betrifft die Probleme der Nutzenden, mögliche Bedrohungen für die Sicherheit und den Schutz der Privatsphäre realistisch wahrzunehmen, Risiken richtig einzuschätzen und angemessene Schutzmechanismen anzuwenden. Sicherheitsfachleute fordern häufig, dass das Verhalten der Nutzenden kontrolliert und eingeschränkt werden sollte und dass Verhaltensänderungen erzwungen werden müssen, um Sicherheitsprobleme einzudämmen. Diese Versuche, die Nutzenden zu »reparieren«, stehen jedoch in krassem Gegensatz zu Erkenntnissen aus der Forschung zur menschenzentrierten Sicherheit, die auf einen Mangel an menschenzentrierter Gestaltung von Schutzmechanismen hinweisen.

Die dritte und letzte Entwicklung bezieht sich auf eigentümliche Vorstellungen vom Wert personenbezogener Daten, dem »Öl des 21. Jahrhunderts« (vgl. Spitz 2017). Zweifellos können personenbezogene Daten verwendet werden, um Personen hinsichtlich ihrer politischen Orientierung, ihrer Persönlichkeitsmerkmale oder anderer gewünschter Eigenschaften zu klassifizieren. Geschäftsmodelle, die auf derartigen Klassifikationen basieren, sind breit etabliert. Die Genauigkeit und die Nützlichkeit dieser Klassifizierungen hängen jedoch vom angewandten Algorithmus und der Qualität der zugrunde liegenden Daten ab. Beide Aspekte führen zu Unsicherheiten, die schwer zu quantifizieren sind und weder durch die derzeitige Tendenz, alle Nutzungsdaten zu speichern, noch durch den Grundsatz der Zweckbindung bei der Nutzung personenbezogener Daten gemildert werden.

Die eher technisch gelagerte und demnach etwas eingeschränkte Perspektive dieses Kapitels hat ihren Ursprung in der wissenschaftlichen Sozialisation der Autorin und der Autoren, die aus der Informatik stammen – einer Disziplin, die noch vergleichsweise jung ist. Dies mag auch eine Erklärung dafür sein, dass der historische Betrachtungshorizont recht eng ist und vor allem

den Status quo betrachtet, also im Wesentlichen ausschließlich die Zeit der Expansion des kommerziellen Internets in den vergangenen 30 Jahren. Wir blicken auch nicht in die Zukunft, sondern beschränken uns auf die Nennung von Problembereichen, die maßgeblich durch »Errungenschaften« der Informatik entstanden sind. Gleichzeitig glauben wir, dass die Problembereiche nicht ohne eine kundige Kommentierung aus der Informatik voll verstanden werden können. Denn wie zu zeigen sein wird, beeinflussen die drei im Verlauf dieses Kapitels skizzierten Phänomene die »digitale Souveränität« weder vollständig positiv noch ausnahmslos negativ. Kühne Lösungsvorschläge sind demnach anderen Kapiteln dieses Bandes vorenthalten. Zur Einordnung existierender Phänomene sind die folgenden Betrachtungen möglicherweise trotzdem hilfreich.

Was sind Digitalisierung und Datafizierung?

Der Übergang von mechanischen und analogen elektronischen Systemen zur digitalen Elektronik begann in der zweiten Hälfte des 20. Jahrhunderts und hatte weltweit tiefgreifende wirtschaftliche, ökologische und gesellschaftliche Auswirkungen. Die zentrale Beobachtung, die u.a. von Shannon (1938) und Turing (1937) gemacht wurde, ist, dass Informationen in eine Folge von binären Ziffern (Bits) kodiert werden können, die ohne Qualitätsverlust dauerhaft gespeichert und auf denen allgemeine Berechnungen mithilfe digitaler Schaltkreise durchgeführt werden können. Eine solche digitale Informationsverarbeitung ist in gewissem Sinne universell: Jede Information kann in binären Ziffern kodiert werden, und binäre Ziffern können von universell programmierbaren digitalen Computern verarbeitet werden, die nur durch die Gesetze der Berechenbarkeit eingeschränkt sind (Hopcroft/Ullman/Motwani 2006). Während z.B. früher verschiedene Technologien verwendet wurden, um Text, Audio und Video zu speichern, zu übertragen und mit ihnen zu interagieren, wird heute alles auf kleinen universellen Computergeräten (Smartphones) erledigt, die anerkannten Regeln der Informationskodierung folgen (wie etwa mp3).

Der Begriff der *Digitalisierung* bezieht sich traditionell auf die Umwandlung von Informationen in eine digitale Form unter Verwendung bestimmter Kodierungsregeln. Heute wird der Begriff oft allgemeiner verwendet und verweist auf die zunehmende Nutzung digitaler Kommunikations- und Datenverarbeitungsgeräte in der Gesellschaft sowie auf die Übertragung einer wachsenden Zahl von Aufgaben an digitale Computer. Vor allem seit dem Aufkommen der nahtlosen globalen Vernetzung (»Internet«) zum Ende des

20. Jahrhunderts sind die Auswirkungen insbesondere auf die Unternehmen beträchtlich, zwingen diese zu einer »digitalen Transformation« (Matt/Hess/Benlian 2015) und haben einen ganz neuen Zweig datenorientierter Dienstleistungsunternehmen (wie Google und Facebook) hervorgebracht. Die Entwicklung wird durch die zunehmende Verfügbarkeit billiger Sensoren wie Kameras sowie lokaler und ferngesteuerter Erfassungsinfrastrukturen vorangetrieben, aber auch durch die allgegenwärtige Verbreitung persönlicher und verhaltensbezogener Daten, die von Einzelpersonen mithilfe digitaler Geräte erzeugt werden. Die Ära der digitalen Datenverarbeitung hat die Produktion digitaler Daten katalysiert und die anfänglichen Schwierigkeiten der Digitalisierung überwunden. Heute werden viele Daten »digital geboren« oder bei ihrer Entstehung nahtlos digitalisiert.

Die Datenproduktion bezieht sich nicht nur auf »Primärdaten«, die von Menschen erzeugt werden oder Sensormessungen widerspiegeln; auch digitale Berechnungen selbst erzeugen Daten, entweder als Ergebnisse der Berechnung von (primären) Eingabedaten oder als Daten, die den Berechnungsprozess aufzeichnen oder anderweitig beschreiben. Solche Daten werden gewöhnlich als »Sekundärdaten« oder »Metadaten« bezeichnet. Zu den Metadaten einer Berechnung gehören beispielsweise die Uhrzeit und das Datum der Berechnung, ein Verweis auf die Quelle der verarbeiteten Daten oder der Name der nutzenden Person, die für die Berechnung verantwortlich ist. Wenn einige Daten zur Beantwortung einer bestimmten Frage benötigt werden (in einem Produktionssystem oder in Bezug auf vergangenes persönliches Verhalten), ist es in der Regel kein Problem, das System so anzupassen, dass diese Daten für künftige Entscheidungen auch noch mitgespeichert werden. Die zunehmenden Rechengeschwindigkeiten, Bandbreiten der Kommunikationsnetze und Speicherkapazitäten haben zu dem Glauben an die allgegenwärtige Verfügbarkeit nützlicher und präziser Daten geführt, auf denen »gute Vorhersagen« basieren können (Dhar 2013). Folglich bezieht sich der Begriff der *Datafizierung* auf das Unterfangen, jede Frage in eine Frage nach Daten zu verwandeln.

Einerseits scheint die allgegenwärtige Verfügbarkeit von scheinbar fundierten Informationen auf Knopfdruck das Versprechen zu erfüllen, dass die Welt transparenter wird. Darüber hinaus können die vermeintliche Objektivität von Daten und ihre allgemeine Verfügbarkeit zu der Überzeugung führen, dass ihre Nutzung zu einer Verbesserung der Entscheidungsfindung von Organisationen und Einzelpersonen führen wird. Andererseits beruhen Informationen immer auf der Interpretation von Daten (bis hin zu den Kodierungsregeln der Datenspeicherung), und viele Antworten werden durch die Auswahl

der bereitgestellten Daten (und damit der gestellten Fragen) bestimmt. Überdies schafft die breite Verfügbarkeit und die gefühlte Transparenz personenbezogener Daten ein umgekehrtes Problem: Ein Mehr an Daten führt zu einem potenziellen Weniger an Privatsphäre.

Datafizierung, das Sammeln von persönlichen Daten und detaillierten Personenprofilen

In der Standardterminologie der Computersicherheit (vgl. Gollmann 2011) bedeutet das Sicherheitsziel der *Vertraulichkeit*, dass bestimmte Informationen nur befugten Personen zugänglich sind. Der Begriff der *Privatsphäre* bezieht sich in der Regel auf den Schutz der Vertraulichkeit von persönlichen Daten (im Gegensatz zu Daten, die einer Organisation gehören). Während der Begriff der Privatsphäre auch schon vor dem Aufkommen von Computern eine Bedeutung hatte, haben die mit der Digitalisierung einhergehenden Umstände der Datenproduktion und -verarbeitung zu einer komplexen Diskussion geführt, die über den technischen Bereich hinausgeht. Ein Grundstein für unser modernes Verständnis von Privatsphäre ist ein Urteil des Bundesverfassungsgerichts aus dem Jahr 1983. Darin wurde das Grundrecht auf informationelle Selbstbestimmung als die grundsätzliche Befugnis der einzelnen Person definiert, selbst zu entscheiden, welche Aspekte des eigenen Privatlebens anderen mitgeteilt werden sollen (vgl. BVerfG 1983). Dieses Urteil hat die von Westin (1970) entwickelten Ideen rechtlich kodifiziert und bildet heute die Grundlage des modernen europäischen Datenschutzrechts, einschließlich der Datenschutz-Grundverordnung (DSGVO bzw. General Data Protection Regulation, GDPR; vgl. European Parliament/Council of the European Union 2016).

Beim Schutz der Privatsphäre spielen personenbezogene Daten eine zentrale Rolle. Gemäß Artikel 4 der Datenschutz-Grundverordnung sind personenbezogene Daten definiert als »alle Informationen über eine bestimmte oder bestimmbare natürliche Person«. Die Definition ist recht weit gefasst und bezieht sich auf alle Daten, durch die eine natürliche Person (direkt oder indirekt) identifiziert werden kann. Dies umfasst offensichtliche »langfristige« Daten (wie Name, Geschlecht, Fingerabdruck, Sozialversicherungsnummer), mittelfristige Daten (Körpergröße, Handynummer) und auch kurzfristige Daten (aktueller Standort, persönliche Stimmung). Auch wenn einige dieser Daten subjektiv datenschutzrelevanter sind als andere, ist es durch die universelle Erfassung solcher Daten möglich, sich der persönlichen Identität einer Person anzunähern. Im Zusammenhang mit der Digitali-

sierung ist dies besonders relevant, da personenbezogene Daten häufig zur Identifizierung von Personen im Internet verwendet werden, was die Gefahr des Identitätsdiebstahls birgt (vgl. Hoofnagle 2007).

Angetrieben durch den Drang zur Datafizierung, ist der Trend zur Datenproduktion in vielerlei Hinsicht auch ein Trend zur Produktion von personenbezogenen Daten (vgl. Wylie 2019). Während bis etwa zum Jahr 2000 Computer oft von mehreren Personen gemeinsam genutzt wurden, sind Computer heute in den meisten Fällen persönliche Geräte, die nur von einer Person verwendet werden. Daher werden allein durch persönliche Interaktionen mit Computern bereits personenbezogene Daten erzeugt. Diese Daten lassen sich heute auch viel leichter einer Person zuordnen als in früheren Jahren, was die Erhebung personenbezogener Daten in einem Maße vereinfacht, dass Unternehmen vollständig individualisierte Dienste anbieten können. Dienste also, die eine einzigartige, auf bestimmte Personen zugeschnittene Zusammensetzung aufweisen, einschließlich ihrer thematischen und emotionalen Vorlieben bis hin zu aktuellen Meinungen und Stimmungen. Datenökosysteme, wie sie um soziale Netzwerke herum entstanden sind, zielen darauf ab, möglichst viele persönliche Daten zu sammeln, um detaillierte persönliche Profile zusammenzustellen, die manchmal sogar detaillierter erscheinen als die eigene persönliche Erinnerung (vgl. ebd.), aber dennoch nicht immer korrekt sein müssen (vgl. Garfinkel 2001).

Die Kluft zwischen faktischer und erlebter Souveränität eines Subjekts

Insgesamt ist die informationelle Selbstbestimmung also ein Grundrecht, das durch modernes Datenschutzrecht wie die DSGVO gestärkt wird. Aber die Digitalisierung und individualisierte Dienste stellen die Wahrnehmung und Gewährleistung dieses Rechts vor Herausforderungen, entweder durch die richtige Konfiguration von Datenschutzeinstellungen und Technologien zum Schutz der Privatsphäre oder durch die Rechenschaftspflicht von Diensteanbietern gegenüber Datenschutzbehörden (vgl. Kranig/Sachs/Gierschmann 2019). Wenn Daten bekannt werden, können sie außerdem nicht einfach vergessen werden. Die Kluft zwischen dem, was man können sollte, und dem, was man kann, wird immer größer, und es hat den Anschein, dass sich diese Kluft durch den zusätzlichen Einsatz von Informatikmethoden zur Datenanalyse vergrößert, der zu rasanten Fortschritten bei der Gesichts- und Spracherkennung, der Audio- und Videoproduktion sowie der Vorhersage von Aktivitäten, Meinungen und Stimmungen geführt hat.

2. Zunehmende Abhängigkeit von großen technischen Ökosystemen

Lock-in-Effekte, fehlende interoperable Standards und »feudale Sicherheit«

Die Digitalisierung hat ein wirtschaftliches Phänomen ermöglicht, das Forschende heute als Plattformökonomie bezeichnen. Vereinfacht gesagt, ist eine Plattform eine Umgebung, in der zwei Marktteilnehmende (Kaufende und Verkaufende) zusammenkommen, um kommerziell zu interagieren (vgl. Rochet/Tirole 2003). Während die Plattform-Metapher für klassische Plattformen (wie Einkaufszentren oder Kredit- und Debitkarten) eher unverständlich und konstruiert erscheint, hat die Digitalisierung (und insbesondere das Internet) die Rolle von Plattformen verstärkt, zunächst in Form von Internet-Medienportalen, wo kostenlose Inhalte Zuschauende anziehen, die wiederum Werbetreibende anziehen, und in letzter Zeit als digitale Ökosysteme, die oft um ein Betriebssystem (wie Microsoft Windows oder Apple iOS) oder um vernetzte Online-Umgebungen wie einen Marktplatz (Amazon), eine Suchmaschine (Google) oder ein soziales Netzwerk (Facebook) herum aufgebaut sind. Auch wenn noch viele Fragen rund um die Entstehung digitaler Plattformen, ihre *Governance*, Geschäftsmodelle und Auswirkungen auf Märkte und Gesellschaft unerforscht sind (vgl. Gawer 2010), spielen sie heute zweifellos eine beherrschende Rolle und sind bei der Teilnahme an vielen gesellschaftlichen Aktivitäten kaum zu vermeiden.

Eines der ältesten und am besten dokumentierten Geschäftsmodelle digitaler Plattformen, das auf den frühen Versuchen beruht, Nutzende für Medien- und Informationsportale wie Yahoo! zu gewinnen, ist Werbung. Erfolgreiche Plattformen ziehen die »Augäpfel« (engl. *eyeballs*) der Nutzenden an (Rochet/Tirole 2003) und verkaufen diese Ansichten (engl. *views*) an Werbekundschaft. Die Werbetreibenden entlohnen die Plattformen für den nachgewiesenen Konsum von Werbung, etwa auf Grundlage der Anzahl der Aufrufe oder Klicks. Moderne Internetwerbung erfolgt sogar auf individueller Basis (vgl. Anderson/Moore 2006): Auf der Grundlage dessen, was die Plattform über die oder den Nutzenden weiß, führt sie in Echtzeit eine Auktion für jede einzelne Ansicht durch. Bei dieser Auktion können Werbetreibende Gebote abgeben, und die höchstbietende Partei erhält den Zuschlag für ihre Anzeige. Dieser Ansatz ermöglicht es, Werbung mit fast beliebig kleinen Budgets zu schalten, was ihn für kleine Unternehmen und Privatpersonen attraktiv macht. Es wird je-

doch auch allgemein angenommen, dass die Konversionsrate von der Betrachtung bis zum Kauf bei individualisierter Werbung viel höher ist, da speziell zugeschnittene Anzeigen eine höhere Chance haben, das Interesse der Betrachtenden zu wecken. Untersuchungen deuten zwar darauf hin, dass dies zutreffen könnte (vgl. ebd.), aber es fehlen verlässliche Zahlen, wie viel effektiver dieser Mechanismus wirklich ist.

Insgesamt hängt das Versprechen personalisierter Werbung mit der Menge an Wissen zusammen, die eine Plattform über eine bestimmte Person, die sie nutzt, zur Verfügung hat. Um Werbeeinnahmen zu generieren, haben Plattformen ein weit verbreitetes und zunehmend aggressives Nutzendentracking betrieben, das auf Cookies oder anderen Browserfunktionen (vgl. Nikiforakis et al. 2013; Pugliese et al. 2020) bis hin zu personalisierten Gerätekennungen oder Geräte-Fingerabdrücken (vgl. Kurtz et al. 2016) basiert. Auch über Methoden der geräteübergreifenden Verfolgung und Verknüpfung von Informationsquellen wurde berichtet (vgl. Arp et al. 2017). Aufgrund ihrer Verwendung sind die meisten der erhobenen Daten eindeutig als personenbezogene Daten zu qualifizieren.

Natürlich steht es den Nutzenden frei, mehrere Plattformen sowohl als kaufende als auch verkaufende Person zu nutzen. In der Wirtschaftsliteratur wird dieses Phänomen als *Multihoming* bezeichnet. Multihoming auf einer Seite des Marktes führt in der Regel zu einer Verschärfung des Wettbewerbs auf der anderen Seite. In solchen Situationen versuchen die Plattformen, Anreize zu schaffen, damit die Nutzenden eine »exklusivere Beziehung« (Rochet/Tirole 2003: 993) zur Plattform eingehen. Dieses Verhalten lässt sich heute bei digitalen Plattformen beobachten. Einzelpersonen sind an personalisierte Konten gebunden, an die viele Annehmlichkeiten wie Cloud-Speicher, Backup, E-Mail und automatische Gerätekonfiguration geknüpft sind. Darüber hinaus werden der nahtlose Austausch von Dokumenten, die Nachrichtenübermittlung und die Verwaltung persönlicher Kontakte und Einstellungen nur innerhalb der Plattform ermöglicht. Plattformen fungieren als digitale Ökosysteme, in denen persönliche Daten in Silos mit proprietärer Software, Kommunikationsprotokollen und Datenformaten gesammelt werden. Dies steht in krassem Gegensatz zur offenen und interoperablen Natur der frühen Internetprotokolle (wie E-Mail und Internet Relay Chat) und führt dazu, dass die Nutzenden – langfristig gesehen – eine Plattform wählen müssen, die sie hauptsächlich nutzen wollen. Die Folge ist eine technologisch erzwungene Bindung an eine einzige Plattform. Trotz der Versuche, Datenportabilität in der Datenschutz-Grundverordnung zu regeln, ist es heute immer noch

schwierig, zwischen digitalen Ökosystemen zu migrieren, und das wird sicherlich auch noch einige Zeit so bleiben (vgl. Syrmoudis et al. 2021).

Obwohl es kontraintuitiv erscheinen mag, ist eine besondere Annehmlichkeit der digitalen Ökosysteme die Datensicherheit. Dies ist eine direkte Folge von zwei Entwicklungen. Die erste Entwicklung bezieht sich auf das Ausmaß der Kontrolle, die die Nutzenden über ihre eigenen Geräte haben. Bei klassischen PCs war es üblich, dass die Nutzenden ihre Sicherheit selbst verwalteten (und dafür verantwortlich waren): Sie konnten ein bestimmtes Betriebssystem wählen und ihr System fast ohne Einschränkungen installieren und konfigurieren. Den Anbietern moderner Smartphones und Tablets ist es gelungen, Hardware und Software so zu integrieren, dass es für die Nutzenden immer schwieriger wird, die volle Kontrolle über ihre eigenen Geräte zu erlangen. Die Kontrolle verbleibt bei den Herstellenden des Geräts, die Sicherheitsrichtlinien wie »installiere nur Software, die in Apples App Store erhältlich ist« durchsetzen können. Die zweite Entwicklung fällt mit dem allgemeinen Trend zusammen, Daten »in der Cloud« zu speichern, d.h. auf Servern, die von Unternehmen wie Dropbox kontrolliert werden, die diesen Dienst anbieten. Bei diesen meist von digitalen Plattformen angebotenen Diensten werden die Daten heute auf Internetservern und nicht mehr auf dem Gerät selbst gespeichert. Die Folge dieser beiden Entwicklungen ist, dass digitale Plattformen die volle Kontrolle über diese Daten haben, was einerseits gut ist, da z.B. Datensicherung und Zugriffskontrolle viel professioneller gehandhabt werden, als dies eine durchschnittliche Person, die sie nutzt, tun könnte. Andererseits müssen die Nutzenden diesen digitalen Plattformen volles Vertrauen entgegenbringen, sowohl was den rechtmäßigen Zugriff von Strafverfolgungsbehörden auf diese Daten angeht als auch die kontinuierliche Verfügbarkeit von Diensten mit fairen Preismodellen. Vor allem bei digitalen Plattformen, wo Nutzende durch die Bereitstellung von Daten bezahlen (wie Google und Facebook), befinden sich diese durch die Nutzungsbedingungen in einer sehr schwachen Position, da es kaum Beschränkungen dafür gibt, was die Plattformen mit ihren persönlichen Daten tun können. Dies schafft eine Situation, die als »feudale Sicherheit« (Schneier 2012) bezeichnet wurde, eine Situation, in der wir die Kontrolle über unsere Daten aufgeben, aber im Gegenzug darauf vertrauen, dass »unsere [Feudal-]Herren uns gut behandeln und vor Schaden bewahren werden«.

Glaube an technologieorientierte Lösungen (Privacy Enhancing Technologies)

Feudale Sicherheit ist ein eher einseitiges Vertrauensverhältnis, da digitale Plattformen kaum formale Garantien für ihre Dienste geben. Während viele Dienste behaupten, den Zugriff auf personenbezogene Daten durch Unbefugte zu verhindern, können die Diensteanbieter selbst die Daten in der Regel für jeden beliebigen Zweck nutzen (vgl. Stylianou/Venturini/Zingales 2015). Das übliche technische Modell des Datenschutzes basierte jedoch auf der Fähigkeit der oder des Einzelnen, die Offenlegung ihrer bzw. seiner persönlichen Daten zu steuern (vgl. Solove 2006). In digitalen Ökosystemen ist diese Fähigkeit (kodiert in den »Privatsphäre-Einstellungen« eines Kontos) jedoch darauf beschränkt, welche anderen *Nutzenden* (innerhalb desselben Ökosystems) auf die eigenen Daten zugreifen können. Der Zugriff durch die Plattform selbst kann nicht verhindert werden. Es gibt jedoch gut entwickelte technische Konzepte, mit denen Datenlecks und das Schutzniveau von persönlichen Daten zwischen beliebigen Parteien beschrieben werden können (vgl. Wagner/Eckhoff 2018). So besagt beispielsweise das Konzept der k-Anonymität (vgl. Sweeney 2002), dass innerhalb eines Datensatzes jede Person nicht von mindestens $k-1$ anderen Individuen des Datensatzes unterschieden werden kann. Es ist also möglich, präzise technische Garantien dafür zu formulieren, in welchem Umfang Informationen bei der Nutzung eines Dienstes geschützt sind.

Ähnlich wie bei der Entwicklung präziser Begriffe zur Beschreibung von Datenlecks hat die moderne Kryptografie ein Universum von Werkzeugen entwickelt, mit denen nahezu beliebige Berechnungen durchgeführt werden können, ohne dass Informationen an eine unbefugte Partei weitergegeben werden, die diese Informationen vorher nicht kannte. Zero-Knowledge-Protokolle ermöglichen es beispielsweise, eine Partei von einer Tatsache zu überzeugen, ohne diese Tatsache preiszugeben. Heutzutage ist es möglich, Algorithmen zu entwickeln, die es erlauben, die Weitergabe von persönlichen Daten auf ein einziges Informationsbit zu beschränken. Ein gutes Beispiel dafür ist das Protokoll für dezentrales, datenschutzgerechtes Proximity Tracing (DP3T), auf dem die meisten europäischen Warn-Apps gegen die Verbreitung von COVID-19 basieren (vgl. Troncoso et al. 2020). Das Protokoll stellt lediglich fest, ob eine möglicherweise gefährliche Begegnung innerhalb eines bestimmten Zeitraums stattgefunden hat oder nicht. Es ist nicht bekannt, mit wem der Kontakt stattfand oder wo er stattfand.

Dennoch ist die Entwicklung von Protokollen wie DP3T alles andere als trivial, insbesondere wenn die Anforderungen, wer was erfahren darf, nur vage definiert sind. In der Praxis wird daher argumentiert, dass der Schutz der Privatsphäre eine fortwährende »Identitätsmanagement«-Aufgabe ist, bei der Interessengruppen wie die Endnutzerinnen und -nutzer die Verwendung ihrer persönlichen Daten ständig überwachen und mithilfe technischer und rechtlicher Instrumente beeinflussen können. Im Zusammenhang mit der Nutzung von Gesundheitsdaten wurde dies als eine Verschiebung von einer reinen »Input-Orientierung« hin zu einer stärkeren »Output-Orientierung« charakterisiert (vgl. Deutscher Ethikrat 2017). Noch ist unklar, wie dieser Ansatz umgesetzt werden kann. Im technischen Bereich wurde die Idee untersucht, Entscheidungen an automatisierte Datenschutzassistenzprogramme unter der Kontrolle der oder des Einzelnen zu delegieren (vgl. Das et al. 2018), aber der Funktionsumfang, die Benutzungsfreundlichkeit und die Effektivität solcher Programme sind noch sehr rudimentär. Im Allgemeinen kann Identitätsmanagement auch an Organisationen delegiert werden, die die Datentreuhandschaft übernehmen, aber es ist unklar, wie für beide Seiten verständliche (und umsetzbare) Datenschutzerwartungen formuliert werden können (vgl. Rao et al. 2016). Es ist daher fraglich, ob digitale Plattformen als Datentreuhänder betrachtet werden können oder sollten.

Insgesamt scheint es immer noch eine ineffektive Kontrolle der Datenproduktion zu geben. Wie bereits erwähnt, ist der Preis für die Datenproduktion und die Datenspeicherung fast gleich null. Moderne Datenverarbeitungssysteme sind komplex, intransparent und schwer zu analysieren. Der Nachweis von Datenlecks ist zudem eine der komplexesten Aufgaben der Systemanalyse, da Informationen auf subtile Weise durch Seitenkanäle abfließen können, die sich willkürlich verschleiern lassen (vgl. Lampson 1973). Spezifische Vorschriften wie die Vorratsdatenspeicherung oder der gesetzlich vorgeschriebene Zugang zu Finanztransaktionen sind demnach Kompromisse, die technische mit rechtlichen Mechanismen koppeln, um diesem Dilemma zu begegnen.

Die Nichtexistenz von nicht personenbezogenen Daten

Obwohl auf den ersten Blick klar, ist die einfache Definition des Begriffs »personenbezogene Daten« in der Datenschutz-Grundverordnung (»alle Informationen über eine bestimmte oder bestimmbare natürliche Person«, vgl. European Parliament/Council of Europe 2016) auf den zweiten Blick erstaunlich komplex. Die Komplexität ergibt sich aus dem Attribut »bestimmbar«, d.h.

Daten können auch dann personenbezogene Daten sein, wenn sie sich nicht unmittelbar auf eine natürliche Person beziehen, aber mit einigem zusätzlichen »angemessenen« Aufwand zur Identifizierung einer Person verwendet werden können. Eine der zentralen Streitfragen im Bereich des Datenschutzes ist die Frage, was unter »angemessenem Aufwand« zu verstehen ist.

Es liegt auf der Hand, dass manche Daten viel weniger geeignet sind, einer Person zugeordnet zu werden, als andere. Der Temperaturwert des Meeresspiegels, der von einer automatischen Sensorstation in der Antarktis am Weihnachtsabend des vergangenen Jahres erfasst wurde, ist ein gängiges Beispiel für ein nicht personenbezogenes Datum. Aus konzeptioneller Sicht ist es jedoch immer möglich, eine Verbindung zu einem Menschen herzustellen und den Datenwert dieser natürlichen Person zuzuordnen. So könnte beispielsweise die Temperatur für die Personen relevant sein, die in der nahe gelegenen Forschungsstation arbeiten, oder die Daten könnten der Person zugeordnet werden, die die Datenabfrage durchgeführt hat. Für jeden Datensatz D gibt es also einen Datensatz D', sodass die Vereinigung von D und D' sich auf eine identifizierbare natürliche Person bezieht. Diese Argumentation zeigt, dass es zumindest theoretisch keine »nicht personenbezogenen Daten« gibt. Zwar ist diese Feststellung aus praktischer Sicht nicht sehr hilfreich, trägt aber zur Klärung bei, was mit dem »angemessenen Aufwand« erfasst werden soll (das Finden des Datensatzes D').

Die Literatur ist voll von Beispielen, in denen öffentlich verfügbare (und scheinbar anonyme) Datensätze durch Korrelation mit zusätzlichen Daten de-anonymisiert wurden. Eines der bekanntesten Beispiele aus der technischen Literatur ist die Re-Identifizierung von Personen, die sich bestimmte Filme angesehen haben – anhand eines von Netflix veröffentlichten anonymisierten Datensatzes (vgl. Narayanan/Shmatikov 2008). In jüngerer Zeit haben Forschende gezeigt, dass 99,98 Prozent der US-Amerikanerinnen und US-Amerikaner in jedem Datensatz anhand von nur 15 demografischen Attributen korrekt re-identifiziert werden können (vgl. Rocher/Hendrickx/de Montjoye 2019). In Anbetracht der Tatsache, dass es sehr genaue Datensammlungen über Verbrauchende gibt (insbesondere in den USA), ist es fraglich, ob ein ausreichendes Maß an Anonymität in einem öffentlich verfügbaren Datensatz erreicht werden kann: Während das Entfernen von Merkmalen aus einem Datensatz die Größe der Anonymitätsmenge schnell erhöht, hat das Hinzufügen von Merkmalen auch das Potenzial, die De-Anonymisierung exponentiell zu beschleunigen. Zumindest zeigen die obigen Beispiele deutlich, dass die Tatsache, ein personenbezogenes Datum zu sein, kein statisches,

sondern ein dynamisches Attribut ist, d.h. Daten, die zu einem Zeitpunkt keinen identifizierbaren Bezug zu einer natürlichen Person haben, können zu einem späteren Zeitpunkt tatsächlich einen solchen aufweisen (vgl. Hornung/Wagner 2019) – eine Erkenntnis, die die Materie nicht vereinfacht.

3. Herausforderungen der Selbstbestimmung

Mangelhafte mentale Modelle der Technologie

Mentale Modelle sind Vorstellungen der Menschen davon, wie Prozesse und Systeme funktionieren (vgl. Volkamer/Renaud 2013). Sie sind für die Entscheidungsfindung notwendig und müssen nicht korrekt sein. Stattdessen sollten mentale Modelle adäquat sein, d.h. sie sollten zu Entscheidungen führen, deren Ergebnisse für die Nutzenden von Vorteil sind (vgl. Camp 2009). So verstehen die Nutzenden womöglich nicht, wie ein Computervirus funktioniert, aber die Überzeugung, dass Viren ernsthaften Schaden anrichten können, kann zur Installation von Antivirensoftware führen (vgl. Wash 2010; Wash/Rader 2015).

Obwohl digitale Geräte und Dienste tagtäglich für eine Vielzahl wichtiger Aufgaben verwendet werden, fehlt vielen Nutzenden ein grundlegendes Verständnis dieser modernen Technologien, sodass ihre mentalen Modelle mangelhaft sind. Eine Untersuchung der mentalen Modelle von Smartphone-Apps ergab beispielsweise, dass die Hälfte der 24 befragten Nutzerinnen und Nutzer Apps nicht als Softwareprogramme wahrnahm, die Zugriff auf ihre Daten haben, sondern sie für Verknüpfungen zu Webseiten oder »Icons« hielt, mit denen sie nützliche Dinge tun konnten (vgl. King 2012). Selbst Nutzende mit hohem Allgemeinbildungsniveau weisen in diesem Bereich oft ein unzureichendes Bewusstsein und Wissen auf. So stellte sich heraus, dass mehrere aktive und gut ausgebildete E-Mail-Nutzende das Client-Server-Paradigma des Versendens und Empfangens von E-Mails nicht kannten und daher keinen Bedarf an einer Ende-zu-Ende-Verschlüsselung von E-Mails sahen (vgl. Renaud/Volkamer/Renkema-Padmos 2014). Kang et al. (2015) zitieren eine Person, die an ihrer Studie teilgenommen hat und die Funktionsweise des Internets folgendermaßen beschreibt: »Meine Daten gehen einfach überall hin.« Sie stellen fest, dass die mentalen Modelle der teilnehmenden Person ohne Informatikhintergrund »die Internet-Ebenen, -Organisationen und -Einheiten auslie-

ßen« (ebd.), was zu vielen falschen Vorstellungen über Sicherheit und Datenschutz führe.

Das Fehlen geeigneter mentaler Modelle der Technologie macht es den Nutzenden unmöglich, Gefahren für ihre Sicherheit und Privatsphäre in der digitalen Welt realistisch wahrzunehmen, Risiken richtig einzuschätzen und angemessene Schutzmechanismen anzuwenden. Dies macht auch die Entwicklung von benutzungsfreundlichen Schutzmechanismen zu einer besonderen Herausforderung: Forschung im Bereich Human-Computer-Interaction (HCI) zur Entwicklung von Maßnahmen zum Schutz von Sicherheit und Privatsphäre hat gezeigt, dass Laien meist nicht in der Lage sind, diese Maßnahmen zu verstehen und anzuwenden (vgl. Herley 2013).

Digitale Selbstbestimmung versus »Sicherheitsmüdigkeit«

Abgesehen davon, dass sie schwer zu verstehen und richtig anzuwenden sind, wurde festgestellt, dass Schutzmaßnahmen einen zu hohen kognitiven und zeitlichen Aufwand erfordern (bis hin zur Undurchführbarkeit) oder nicht den Sicherheitsnutzen bieten, der den Aufwand rechtfertigen würde (vgl. Herley 2009; Reeder/Ion/Consolvo 2017). Es gibt sogar den Begriff der Sicherheitsmüdigkeit (engl. *security fatigue*), der die Resignation der Benutzenden angesichts der vielen Sicherheitsanforderungen beschreibt, die oft mit ihren Lebens- und Arbeitsrealitäten und manchmal sogar miteinander in Konflikt stehen (vgl. Stanton et al. 2016).

Ähnlich unbefriedigend ist die Situation beim Datenschutz. Viele Nutzende scheinen gegenüber dem Schutz ihrer persönlichen Daten zu resignieren und akzeptieren einfach, dass sie nichts dafür tun können (vgl. Turow/Hennessy/Draper 2015). Darüber hinaus gibt es starke Hinweise aus der Verhaltensökonomie, dass Menschen, selbst wenn sie ihre Privatsphäre schützen wollten, dazu nicht in der Lage wären. So haben mehrere experimentelle Studien gezeigt, dass Entscheidungen zum Schutz der Privatsphäre durch einfache experimentelle Bedingungen, wie beispielsweise eine 15-sekündige Ablenkung oder leicht unterschiedliche Formulierungen der Datenschutzfragen, in Richtung einer größeren Offenlegung von Daten manipuliert werden können (vgl. Acquisti/Brandimarte/Loewenstein 2015).

Diese Erkenntnisse sind wichtig für die Datenschutz-Grundverordnung und ähnliche Vorschriften: Einerseits brauchen wir diese Regelungen, weil die Forschung wiederholt gezeigt hat, dass Menschen nicht in der Lage sind, ihre Entscheidungen in Bezug auf Sicherheit und Datenschutz so zu treffen, dass

sie für sie vorteilhaft sind und ihren Wünschen und Präferenzen entsprechen. Andererseits könnten die Forderungen dieser Verordnungen, den Nutzenden mehr Transparenz und Kontrolle über ihre persönlichen Daten zu geben, gerade deshalb vergeblich sein, weil es den Nutzenden an Wissen, Fähigkeiten und Ressourcen fehlen könnte, um ihre gesetzlichen Rechte sinnvoll zu nutzen.

Von technologiezentrierter zu menschenzentrierter Gestaltung von Schutzmaßnahmen

Sicherheitsfachleute geben häufig den Benutzenden die Schuld für ihr mangelndes Sicherheitsbewusstsein, für die Nichtbefolgung von Sicherheitsratschlägen und für die Verursachung von Sicherheitsproblemen. Diese Denkweise ist als »Fix the User«-Paradigma bekannt (vgl. Schneier 2016): Das Verhalten der Nutzenden sollte kontrolliert und eingeschränkt werden, und es müssen Verhaltensänderungen erzwungen werden, um Sicherheitsprobleme einzudämmen. Die bahnbrechende Veröffentlichung *Users are not the enemy* von Adams und Sasse (1999) hat es geschafft, zumindest einen Teil dieser auf Schuldzuweisungen basierenden IT-Sicherheitskultur grundlegend in Richtung konstruktiverer Ansätze zu verändern. In einer Reihe von Interviews zeigten die Autorinnen, dass die Nutzenden nicht aus Unachtsamkeit oder bösem Willen heraus unsicher handeln, sondern weil die Sicherheitsmechanismen nicht nutzerzentriert entwickelt wurden und dadurch eine schlechte Gebrauchstauglichkeit aufweisen.

Menschenzentrierte IT-Sicherheit und Datenschutz setzen auf das Verständnis der Fähigkeiten der Menschen für Sicherheits- und Datenschutzaufgaben. Außerdem sollen Sicherheit und Datenschutz stets im Kontext betrachtet werden: Was sind die Lebens- und Arbeitsrealitäten der Nutzenden, was sind ihre primären Ziele und Aufgaben? Wie interagieren die Ziele von Sicherheit und Datenschutz mit diesem Kontext? Dieses Verständnis ist notwendig für die Entwicklung angemessener Sicherheits- und Datenschutzmaßnahmen, die von der Mehrheit der Nutzenden verwendet werden können und dann auch verwendet werden. Das heißt, anstatt die Nutzenden an die Technologie anzupassen (was sowieso nicht gelingt), sollte man die Technologie an die Bedürfnisse und Fähigkeiten der Nutzenden anpassen (vgl. Sasse 2015). Mit dieser Anpassung beschäftigt sich seit mehr als 20 Jahren Forschung und Entwicklung im interdisziplinären Bereich »Usable Security« (Cranor/Garfinkel 2005; Garfinkel/Richter Lipford 2014). Zu Erfolgen dieser Forschung gehören u.a. die Änderungen der international anerkannten

Richtlinien zur Passwortverwaltung (vgl. NIST 2017). Diese Richtlinien vereinfachen die Passworthandhabung für die Nutzenden (z.B. werden keine komplizierten, langen Passwörter mehr verlangt) und zeigen gleichzeitig auf, welche organisatorischen und technischen Maßnahmen die Anbieter zur sicheren Verwaltung von vereinfachten Passwörtern treffen müssen.

Es gibt sowohl konzeptionelle als auch ökonomische Gründe dafür, dass benutzbare Sicherheitsmaßnahmen immer noch selten sind. Konzeptionell stellen »Benutzbarkeit« und »Sicherheit« zwei Systemeigenschaften dar, die in einem Aspekt zueinander sehr ähnlich charakterisiert werden: Sie sind für die Funktionsweise der Systeme nicht zwingend notwendig. Deswegen werden sie bei der Entwicklung oft später hinzugefügt, nachdem funktionale Eigenschaften implementiert und getestet wurden, was zu gegenseitiger Abschwächung der beiden Eigenschaften führt (vgl. Yee 2004): Wenn Sicherheit nicht von Anfang an in der Systemarchitektur vorhanden ist, werden beim späteren Hinzufügen der Sicherheitsmaßnahmen oft Hürden für die Benutzung eingebaut – die Benutzbarkeit sinkt. Bei dem Versuch, die Benutzbarkeit zu erhöhen, werden Sicherheitseigenschaften, beispielsweise vorgegebene Sicherheitseinstellungen, wieder abgeschwächt. Es ist deswegen unabdingbar, sowohl Sicherheit als auch Benutzbarkeit von Anfang an in den Entwicklungsprozess einzubinden (vgl. Sasse/Flechais 2005).

Jedoch würden solche Entwicklungsprozesse zusätzliche zeitliche, personelle und finanzielle Ressourcen beanspruchen, was aus der ökonomischen Perspektive problematisch ist. Die Verbraucherinnen und Verbraucher können die erhöhte IT-Sicherheit nicht selbst beurteilen und sind deswegen nicht bereit, für erhöhte Sicherheit mehr zu bezahlen (vgl. Anderson/Moore 2006). Folglich fehlen den Produzierenden ökonomische Anreize zum Erhöhen der IT-Sicherheit, die ihre begrenzten Ressourcen lieber in die schnelle Entwicklung von innovativen Lösungen mit attraktiver Funktionalität investieren. Dieses Marktversagen führt zur Notwendigkeit, IT-Sicherheit und Datenschutz zu regulieren, wie es beispielsweise im IT-Sicherheitsgesetz 2.0 (2021) und in der DSGVO (2016) vorgesehen ist. Zum Beispiel könnte das Anbringen von einem IT-Sicherheitskennzeichen die IT-Sicherheitsmaßnahmen der Hersteller sichtbar machen (vgl. Deutscher Bundestag 2021: Art. 1 § 9c) und zur Präferenz von Produkten mit besseren Sicherheitseigenschaften führen (vgl. Morgner et al. 2020). Regulierung führt in der Praxis jedoch nicht immer zur Verbesserung der Sicherheit und der Benutzbarkeit, wie die sehr negativen Nutzungserfahrungen mit kaum handhabbaren Cookie-Hinweisen auf den Webseiten gezeigt haben (vgl. Utz et al. 2019). Auch die praktische Umsetzbarkeit des IT-Sicher-

heitsgesetzes 2.0 wurde von mehreren Seiten kritisiert (s. Kipker/Scholz 2021 für einen Überblick).

4. Das Daten-Dilemma: Datenschutz vs. Datennutz

Der aktuelle Trend, alles aufzuheben

Zur »digitalen Souveränität« gehört auch zu wissen, welche Daten über einen selbst erfasst und welche Schlussfolgerungen aus ihnen gezogen wurden. Durch die Informationen des Whistleblowers Edward Snowden wurde 2014 bekannt, dass die NSA die Aufzeichnung des kompletten Internetverkehrs plante (vgl. Greenwald 2014). Was damals technisch zumindest als herausfordernd erachtet wurde, scheint heute ein plausibler Teil der Geschäftsstrategie vieler Unternehmen zu sein. Zwar ist nicht vollständig bekannt, was die oben bereits genannten digitalen Plattformen – die man summarisch gern als GAFAM (Google [Alphabet], Amazon, Facebook, Apple, Microsoft) bezeichnet – mit den Daten tun, die auf ihren Plattformen anfallen, aber mit großer Wahrscheinlichkeit heben auch sie erst einmal alles auf, was sie bekommen können, und nutzen es für ihre Zwecke. Wie oben schon diskutiert, sind das erst einmal Wege zur personalisierten Werbung und in gewissem Umfang auch zu personalisierten Services – ob die Benutzenden das nun wollen oder nicht. Es ist dann nur noch ein kleiner Schritt hin zu Manipulation und zur Modifikation des Verhaltens (vgl. Zuboff 2019). Hier wird definitiv feudale Sicherheit geboten, aber es ist nicht sicher, ob sich die Benutzenden das auch so wünschen.

Speicherplatz ist heute vergleichsweise preiswert und deshalb ausreichend verfügbar. Weil die Entscheidung, welche Daten wichtig sind und welche nicht, manchmal schwierig zu treffen ist, gibt es die deutliche Tendenz, erst einmal alles zu speichern und dann erst später zu entscheiden, was mit den Daten gemacht wird. Diese Herangehensweise wird im Volksmund gern als »Datengier« bezeichnet. Das bedeutet, es werden mehr Daten erfasst, als derzeit gebraucht werden, nur weil sie später vielleicht einmal nützlich sein könnten. Die nachträgliche Erweiterung eines Datenbestands ist immer mühsam und teuer, weshalb Entwickelnde dies zu vermeiden versuchen. Beides zusammen führt dann zu sogenannten »Daten-Friedhöfen«, also großen Datenmengen, die zwar gespeichert sind, aber nie gelesen werden.

Die Versprechen des Data Mining und der öffentlichen Daten, das Problem der Datenqualität und die Nachvollziehbarkeit von maschinellem Lernen

Viele Daten werden heute also ohne bestimmten Zweck und auf Vorrat gespeichert. Wenn sie nicht dauerhaft auf Daten-Friedhöfen landen, werden solche Datenbestände manchmal wiederentdeckt in der Hoffnung, sie doch noch nutzen zu können. Man vermutet darin etwa wichtige Informationen über das Verhalten von Kundinnen und Kunden oder über die Verbreitung von Infektionen. Was dann allerdings vorliegt, sind zumeist nur sogenannte »Rohdaten«, was bedeutet, dass sie meist nicht unmittelbar für eine Analyse geeignet sind. Es gibt eigentlich immer die wohlbekannten Probleme mit der Datenqualität: Unvollständigkeit (fehlende Werte), Ungenauigkeit, schlichte Fehler und Veralterung, um nur einige zu nennen.

Viele Algorithmen wurden schon vorgeschlagen, um diese Probleme zu beheben (vgl. Müller/Freytag 2003) (soweit das überhaupt möglich ist). Alle diese Verfahren der Datenbereinigung (*data cleaning* oder *data cleansing* genannt) nutzen aber Extrapolationen oder Schätzungen, führen also unter Umständen selbst auch wieder Ungenauigkeiten ein. Die tatsächlichen Werte zu finden, erfordert oft manuellen Eingriff und ist deshalb viel zu teuer. Es ist also notwendig, genau zu dokumentieren, welche Daten tatsächlich erhoben und welche nachträglich auf die eine oder andere Art rekonstruiert wurden. Bei dieser Dokumentation handelt es sich um Metadaten, die für die Nutzung der Daten von eminenter Bedeutung sind.

Eine zweite, ebenfalls sehr wichtige Aufgabe für die Sammelnden und Besitzenden ist in der Vorbereitung von Daten für die Analyse die Integration von Datenbeständen aus verschiedenen Quellen. Auch das verändert die Daten: Werte werden in ein gemeinsames Format umgewandelt, Dubletten identifiziert und gelöscht. Eventuell gelingt das nicht perfekt und verzerrt die Daten dadurch ein kleines bisschen, auch bei allem Bemühen, das zu vermeiden. Die Bestände sind aber oft einfach zu groß, um jedes Detail noch einmal zu prüfen. Es ist für die Betroffenen wichtig, diese Vorverarbeitung bei Bedarf nachvollziehen zu können und vor allem zu prüfen, ob damit (womöglich sogar ohne Absicht) falsche Eindrücke entstehen könnten.

Nach der Erfassung von Metadaten und der Datenintegration kann dann die Analyse beginnen. Es werden Schlüsse aus den Daten gezogen, die gravierende Konsequenzen haben können. Neue Daten werden aus den Beständen abgeleitet, zumeist in sehr viel kompakterer Form (»aggregiert«), sodass inter-

essante Dinge wie z.B. Trends, Gruppierungen und Verhaltensmuster besser erkannt werden können. Die abgeleiteten Daten beziehen sich auf eine große Gruppe von Elementen, die dann statistisch ausgewertet wird, oder auch auf ein einzelnes Individuum, das klassifiziert oder in einer größeren Menge lokalisiert wird.

Die Methoden der Datenanalyse können wie folgt gruppiert werden (vgl. Han/Kamber/Pei 2011):

a) Vorhersage: Was wird eine Person als nächstes tun (z.B. kaufen)? Wohin wird eine Person gehen?
b) Klassifikation: Was für eine Person ist es? Gut oder böse? Reich oder arm? Gesund oder krank?
c) Gruppierung (Clusterbildung): Welche Personen bilden eine Gruppe mit ähnlichen Eigenschaften?
d) Ausreißer: Was macht eine Person besonders, anders als die anderen?
e) Assoziationen: Was kommt oft zusammen vor?

All diese Methoden brauchen große Datenbestände (»Big Data«). Wichtiger noch, sie brauchen alle auch menschliche Eingriffe. So müssen Schwellenwerte festgelegt und Hyperparameter gesetzt werden. Auch was Ähnlichkeit ist, muss für die Methoden erst festgelegt werden. Dadurch kann das Ergebnis aber auch manipuliert werden. Es ist heute durchaus üblich, diese Systeme schrittweise zu verbessern, indem die Einstellungen einfach ausprobiert werden. Passen die Ergebnisse nicht, werden die Einstellungen etwas abgeändert und die Daten erneut analysiert. Auch hier sind Transparenz und Nachvollziehbarkeit für die Betroffenen ein Desiderat.

Verzerrungen zwischen gespeicherten Daten und der Realität: Kann ein perfekter Zwilling erzeugt werden?

Das Konzept des »digitalen Zwillings« ist heutzutage sehr populär. Mit diesem Begriff ist eine digitale Repräsentation eines echten Objekts gemeint, die in möglichst vielen Aspekten diesem Objekt ähnelt. Genutzt werden digitale Zwillinge bei Gegenständen und Produkten, die überwacht und gewartet werden müssen. Das Konzept kann aber auch auf Menschen angewendet werden. Der Glaube daran, einen perfekten digitalen Zwilling erschaffen zu können, führt dazu, dass der Zwilling in manchen Situationen das reale Objekt ersetzt und allein die digitale Repräsentation die Basis für Entscheidungen liefert, die

das reale Objekt betreffen. Handelt es sich dabei um eine Person, kann deren Souveränität dadurch beeinträchtigt werden, denn man »fragt« nicht mehr sie, sondern den Zwilling.

Allerdings ist bereits aus den frühen Tagen des Datenbankeinsatzes bekannt, dass Daten nur ein Modell der Realität sind und dieses niemals ein vollständiges Bild ergeben kann (vgl. Kent 2012 [1978]). Deshalb ist der digitale Zwilling eigentlich eine Fiktion: Er suggeriert Vollständigkeit, die nie erreicht werden kann. (Vielleicht ist deshalb inzwischen auch die Bezeichnung »digitaler Schatten« auf dem Vormarsch.) Daher ist es sehr viel sinnvoller, einen bestimmten Zweck für das Sammeln und die Analyse der Daten zu definieren. In der Entwicklung von Datenbanken wurde gern der Begriff »Miniwelt« verwendet, um deutlich zu machen, dass nur ein kleiner Ausschnitt der Realität durch die Daten beschrieben wird. Trotzdem waren und sind die mit dieser Einschränkung entwickelten Datenbanken durchaus nützlich, und zwar sowohl für die Betreibenden als auch für deren Kundschaft, weil Vorgänge effizienter abgewickelt werden können. Entscheidend ist, dass die Daten trotz ihrer Unvollständigkeit nicht einfach pragmatisch als digitaler Zwilling genutzt werden dürfen. Diese Gefahr besteht, wenn keine anderen Daten vorliegen. Hier sollte die »digitale Souveränität« der Betroffenen erlauben, den »Zwilling« zu überprüfen und auf dessen Unvollständigkeit hinzuweisen – ohne gleich gezwungen zu werden, dann doch bitte für Vollständigkeit zu sorgen.

Die Schwierigkeiten der Datensparsamkeit, Kontrolle über die Daten und das Prinzip der Zweckbindung

Leider kann der Zweck des Datensammelns oft nur unpräzise definiert werden, außerdem ändert er sich mit der Zeit. Trotzdem ist es sehr sinnvoll, zumindest den Versuch zu machen, diesen Zweck zu identifizieren. Er sollte dokumentiert und, wo möglich, auch publiziert werden. Das hilft, die oben beschriebenen Tendenzen zu vermeiden, und es kann in erheblichem Umfang Ressourcen einsparen – vom Energieverbrauch bis zur Arbeitszeit der Angestellten. Datensparsamkeit, also die Beschränkung auf die Daten, die tatsächlich gebraucht werden, ist also nicht nur eine Frage des Datenschutzes, sondern entfaltet auch ökonomische und ökologische Wirkungen. Eine Konsequenz daraus ist auch das Löschen der Daten, die nicht mehr gebraucht werden.

5. Herausforderungen für die Forschung

Wie steht es nun um die »digitale Souveränität« des Individuums in der digitalisierten Welt? Unter welchen Umständen kann man heute und in Zukunft ein selbstbestimmtes und autonomes Leben führen? Die Betrachtung aus technischer und soziotechnischer Perspektive wirft mehr Fragen auf, als sie Antworten gibt, denn die großen Diensteanbieter entziehen Individuen eher Kontrolle über ihre Geräte und Daten, was faktisch und gefühlt zu einem Weniger an Selbstbestimmung führt. Dies schafft Abhängigkeiten, die auch Auswirkungen auf die Möglichkeit von Nutzenden haben, etwaige Bedrohungen für die Sicherheit und den Schutz der Privatsphäre realistisch wahrzunehmen. Noch ist in höchstem Maße unklar, unter welchen Umständen Nutzende überhaupt selbstbestimmte Entscheidungen über ihre eigene Sicherheit und Privatsphäre in einer digitalisierten Welt treffen können. Sicherlich gehört die menschzentrierte Gestaltung von Schutzmechanismen dazu, welche aber auch immer durch den Grad des Verständnisses für die technischen und soziotechnischen Zusammenhänge bedingt sind. Was muss man wissen und verstehen, um in einer digitalisierten Welt selbstbestimmt zu leben? Um die Risiken für die eigene Sicherheit und Privatsphäre richtig einzuschätzen sowie angemessene Schutzmechanismen anzuwenden? Was ist überhaupt ein akzeptables individuelles Schutzniveau? Wo liegen die Grenzen von Schutzmaßnahmen, und unter welchen Umständen ist es demnach sinnvoller Risiken einzugehen? Wie können Schutzmaßnahmen aussehen, die Nutzende dabei unterstützen, die vorhandenen Zielkonflikte besser abzuwägen? Wie verändern sich diese Umstände über die Zeit?

Über allem steht der oft suggerierte »hohe Wert« von (personenbezogenen) Daten, der immer wieder durch einen Blick auf den spekulativen Börsenwert der Internetkonzerne eher anekdotisch bestätigt wird. Wie sich dieser Wert jenseits von der Hoffnung auf zukünftige Unternehmensgewinne ausdrückt und unter welchen Umständen er entsteht, ist weiterhin hochgradig unklar – denn zu wenig ist bekannt über die Genauigkeit und die Nützlichkeit dieser Daten sowie über die Wirksamkeit der Algorithmen, mit denen sie verarbeitet werden. Eine differenzierte Betrachtung dieses Phänomens tut Not, denn ein gefühlter Verlust an individueller Souveränität ist langfristig genauso wirksam wie ein real existierender.

Literaturverzeichnis

Acquisti, Alessandro/Brandimarte, Laura/Loewenstein, George (2015): »Privacy and human behavior in the age of information«, in: Science 347 (6221), S. 509–514.

Adams, Anne/Sasse, M. Angela (1999): »Users are not the enemy«, in: Communications of the ACM 42 (12), S. 41–46.

Anderson, Ross/Moore, Tyler (2006): »The economics of information security«, in: Science 314 (5799), S. 610–613.

Arp, Daniel/Quiring, Erwin/Wressnegger, Christian/Rieck, Konrad (2017): »Privacy threats through ultrasonic side channels on mobile devices«, in: 2017 *IEEE European Symposium on Security and Privacy (EuroS&P)*, S. 35–47, https://doi.org/10.1109/EuroSP.2017.33.

Aziz, Arslan/Telang, Rahul (2015): What is a cookie worth? 14th *Annual Workshop on the Economics of Information Security (WEIS)*. Preliminary Draft, Heinz College, Carnegie Mellon University, Pittsburgh. Online unter: www.econ-infosec.org/archive/weis2015/papers/WEIS_2015_aziz.pdf, abgerufen am 24.02.2022.

BVerfG – Bundesverfassungsgericht (1983): Urteil des Ersten Senats vom 15. Dezember 1983 – 1 BvR 209/83 –, Rn. 1–215.

Camp, L. Jean (2009): »Mental models of privacy and security«, in: IEEE Technology and Society Magazine 28 (3), S. 37–46.

Cranor, Lorrie Faith/Garfinkel, Simson (2005): Security and usability: Designing secure systems that people can use, Beijing u.a.: O'Reilly.

Das, Anupam/Degeling, Martin/Smullen, Daniel/Sadeh, Norman (2018): »Personalized privacy assistants for the internet of things: Providing users with notice and choice«, in: IEEE Pervasive Computing 17 (3), S. 35–46, https://doi.org/10.1109/MPRV.2018.03367733.

Deutscher Bundestag (2021): Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0), Bundesgesetzblatt Teil I Nr. 25, Bonn: Bundesanzeiger Verlag.

Deutscher Ethikrat (2017): Big Data und Gesundheit – Datensouveränität als informationelle Freiheitsgestaltung. Stellungnahme, 30.11.2017. Online unter: https://www.ethikrat.org/fileadmin/Publikationen/Stellungnahmen/deutsch/stellungnahme-big-data-und-gesundheit.pdf, abgerufen am 20.08.2021.

Dhar, Vasant (2013): »Data science and prediction«, in: Communications of the ACM 56 (12), S. 64–73, https://doi.org/10.1145/2500499.

European Parliament/Council of the European Union (2016): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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 (General Data Protection Regulation). Online unter: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679, abgerufen am 20.08.2021.

Garfinkel, Simson (2001): Database nation, Beijing u.a.: O'Reilly.

Garfinkel, Simson/Richter Lipford, Heather (2014): »Usable security: History, themes, and challenges«, in: Synthesis Lectures on Information Security, Privacy, and Trust 5 (2), S. 1–124.

Gawer, Annabelle (Hg.) (2010): Platforms, markets and innovation, Cheltenham/Northampton: Edward Elgar Publishing.

Gollmann, Dieter (2011): Computer security, Chichester: Wiley.

Grassi, Paul A./Fenton, James L./Newton, Elaine M./Perlner, Ray A./Regenscheid, Andrew R./Burr, William E./Richter, Justin P./Lefkovitz, Naomi B./Danker, Jamie M./Choong, Yee-Yin/Greene, Kristen K./Theofanos, Mary F. (2017): Digital identity guidelines. Authentication and lifecycle management (NIST Special Publication 800–63B), https://doi.org/10.6028/NIST.SP.800-63b.

Greenwald, Glenn (2014): No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state, New York: Picador Metropolitan Books, Henry Holt.

Han, Jiawei/Kamber, Micheline/Pei, Jian (2011): Data mining: Concepts and techniques (= The Morgan Kaufmann Series in Data Management Systems), Burlington: Morgan Kaufmann.

Herley, Cormac (2009): »So long, and no thanks for the externalities: The rational rejection of security advice by users«, in: New security paradigms workshop (NSPW'09), Association for Computing Machinery (ACM), S. 133–144, https://doi.org/10.1145/1719030.1719050.

Herley, Cormac (2013): »More is not the answer«, in: IEEE Security & Privacy 12 (1), S. 14–19.

Hoofnagle, Chris Jay (2007): »Identity theft: Making the known unknowns known«, in: Harvard Journal of Law and Technology 21 (1).

Hopcroft, John E./Ullman, Jeffrey D./Motwani, Rajeev (2006): Introduction to automata theory, languages, and computation, Upper Saddle River: Prentice Hall.

Hornung, Gerrit/Wagner, Bernd (2019): »Der schleichende Personenbezug«, in: Computer und Recht 35 (9), S. 565–574.

Kang, Ruogu/Dabbish, Laura/Fruchter, Nathaniel/Kiesler, Sara (2015): »My data just goes everywhere: User mental models of the internet and implications for privacy and security«, in: Eleventh Symposium on Usable Privacy and Security (SOUPS), USENIX Association, S. 39–52.

Kent, William (2012 [1978]): Data and reality: A timeless perspective on perceiving and managing information in our imprecise world. Westfield: Technics Publications.

King, Jennifer (2012): How come I'm allowing strangers to go through my phone? Smartphones and privacy expectations, SSRN vom 15.03.2012, ht tp://dx.doi.org/10.2139/ssrn.2493412.

Kipker, Dennis-Kenji/Scholz, Dario E. (2021): »Das IT-Sicherheitsgesetz 2.0«, in: Datenschutz und Datensicherheit – DuD 45.1, S. 40–45.

Kranig, Thomas/Sachs, Andreas/Gierschmann, Markus (2019): Datenschutz-Compliance nach der DS-GVO. Köln: Reguvis Fachmedien.

Kurtz, Andreas/Gascon, Hugo/Becker, Tobias/Rieck, Konrad/Freiling, Felix C. (2016): »Fingerprinting mobile devices using personalized configurations«, in: Proceedings on Privacy Enhancing Technologies (1), S. 4–19.

Lampson, Butler W. (1973): »A note on the confinement problem«, in: Communications of the ACM 16 (10), S. 613–615.

Matt, Christian/Hess, Thomas/Benlian, Alexander (2015): »Digital transformation strategies«, in: Business & Information Systems Engineering 57 (5), S. 339–343, https://doi.org/10.1007/s12599-015-0401-5.

Morgner, Philipp/Mai, Christoph/Koschate-Fischer, Nicole/Freiling, Felix/Benenson, Zinaida (2020): »Security update labels: establishing economic incentives for security patching of IoT consumer products«, in: 2020 IEEE Symposium on Security and Privacy (S&P), S. 429–446, https://doi.org/10.1109/SP40000.2020.00021.

Müller, Heiko/Freytag, Johann-Christoph (2003): Problems, methods, and challenges in comprehensive data cleansing. Technical report, Humboldt-Universität zu Berlin. Online unter: http://dc-pubs.dbs.uni-leipzig.de/files/Mller2003ProblemsMethodsand.pdf, abgerufen am 20.06.2022.

Narayanan, Arvind/Shmatikov, Vitaly (2008): »Robust de-anonymization of large sparse datasets«, in: 2008 IEEE Symposium on Security and Privacy (S&P), S. 111–125, https://doi.org/10.1109/SP.2008.33.

Nikiforakis, Nick/Kapravelos, Alexandros/Joosen, Wouter/Kruegel, Christopher/Piessens, Frank/Vigna, Giovanni (2013): »Cookieless monster: Exploring the ecosystem of web-based device fingerprinting«, in: 2013 IEEE Symposium on Security and Privacy (S&P), S. 541–555.

Pugliese, Gaston/Riess, Christian/Gassmann, Freya/Benenson, Zinaida (2020): »Long-term observation on browser fingerprinting: Users' trackability and perspective«, in: Proceedings on Privacy Enhancing Technologies (2), S. 558–577, https://doi.org/10.2478/popets-2020-0041.

Rao, Ashwini/Schaub, Florian/Sadeh, Norman M./Acquisti, Alessandro/Kang, Ruogu (2016): »Expecting the unexpected: Understanding mismatched privacy expectations online«, in: Twelth Symposium on Usable Privacy and Security (SOUPS), S. 77–96.

Reeder, Robert W./Ion, Iulia/Consolvo, Sunny (2017): »152 simple steps to stay safe online: Security advice for non-tech-savvy users«, in: IEEE Security & Privacy 15 (5), S. 55–64.

Renaud, Karen/Volkamer, Melanie/Renkema-Padmos, Arne (2014): »Why doesn't Jane protect her privacy?«, in: Emiliano Cristofaro/Steven J. Murdoch (Hg.), Privacy Enhancing Technologies. 14th International Symposium PETS 2014, Amsterdam, The Netherlands, July 16–18, 2014, Proceedings, Cham: Springer, S. 244–262.

Rocher, Luc/Hendrickx, Julien M./Montjoye, Yves-Alexandre de (2019): »Estimating the success of re-identifications in incomplete datasets using generative models«, in: Nature Communications 10, Artikel Nr. 3069, https://doi.org/10.1038/s41467-019-10933-3.

Rochet, Jean-Charles/Tirole, Jean (2003): »Platform competition in two-sided markets«, in: Journal of the European Economic Association 1 (4), S. 990–1029, https://doi.org/10.1162/154247603322493212.

Sasse, M. Angela (2015): »Scaring and bullying people into security won't work«, in: IEEE Security & Privacy 13 (3), S. 80–83.

Sasse, M. Angela/Flechais, Ivan (2005): »Usable security: Why do we need it? How do we get it?«, in: Lorrie Faith Cranor/Simson Grafinkel (Hg.), Security and usability: Designing secure systems that people can use, Beijing u.a.: O'Reilly, S. 13–30.

Schneier, Bruce (2012): »When it comes to security, we're back to feudalism«, in: Wired 11. Online unter: https://www.wired.com/2012/11/feudal-security/, abgerufen am 01.06.2021.

Schneier, Bruce (2016): »Stop trying to fix the user«, in: IEEE Security & Privacy 14 (5), S. 96.

Shannon, Claude E. (1938): »A symbolic analysis of relay and switching circuits«, in: Transactions of the American Institute of Electrical Engineers 57 (12), S. 713–723, https://doi.org/10.1109/T-AIEE.1938.5057767.

Solove, Daniel J. (2006): »A taxonomy of privacy«, in: University of Pennsylvania Law Review 154, S. 477.

Spitz, Malte (2017): Daten – das Öl des 21. Jahrhunderts? Nachhaltigkeit im digitalen Zeitalter, Hamburg: Hoffmann und Campe.

Stanton, Brian/Theofanos, Mary F./Spickard Prettyman, Sandra/Furman, Susanne (2016): »Security fatigue«, in: IT Professional 18 (5), S. 26–32.

Stylianou, Konstantinos/Venturini, Jamila/Zingales, Nicolo (2015): »Protecting user privacy in the cloud: An analysis of terms of service«, in: European Journal of Law and Technology 6 (3). Online unter: https://ssrn.com/abstract=2707852, abgerufen am 01.07.2022.

Sweeney, Latanya (2002): »k-Anonymity: A model for protecting privacy«, in: International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems 10 (5), S. 557–570.

Syrmoudis, Emmanuel/Mager, Stefan/Kuebler-Wachendorff, Sophie/Pizzinini, Paul/Grossklags, Jens/Kranz, Johann (2021): »Data portability between online services: An empirical analysis on the effectiveness of GDPR Art. 20«, in: Proceedings on Privacy Enhancing Technologies 2021 (3), S. 351–372, https://doi.org/10.2478/popets-2021-0051.

Troncoso, Carmela/Payer, Matthias/Hubaux, Jean-Pierre/Salathe, Marcel/Larus, James/Bugnion, Edouard/Lueks, Wouter/Stadler, Theresa/Pyrgelis, Apostolos/Antonioli, Daniele/Barman, Ludovic/Chatel, Sylvain/Paterson, Kenneth/Capkun, Srdjan/Basin, David/Beutel, Jan/Jackson, Dennis/Roeschlin, Marc/Leu, Patrick/Preneel, Bart/Smart, Nigel/Abidin, Aysajan/Gürses, Seda/Veale, Michael/Cremers, Cas/Backes, Michael/Tippenhauer, Nils Ole/Binns, Reuben/Cattuto, Ciro/Barrat, Alain/Fiore, Dari/Barbosa, Manuel/Oliveira, Rui/Pereira, Jose (2020): Decentralized privacy-preserving proximity tracing. White Paper, Version vom 25.05.2020. Online unter: https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf, abgerufen am 25.08.2021.

Turing, Alan M. (1937): »On computable numbers, with an application to the Entscheidungsproblem«, in: Proceedings of the London Mathematical Society s2-42 (1), S. 230–265, https://doi.org/10.1112/plms/s2-42.1.230.

Turow, Joseph/Hennessy, Michael/Draper, Nora (2015): The tradeoff fallacy: How marketers are misrepresenting American consumers and opening them up to exploitation, SSRN vom 10.08.2016, http://dx.doi.org/10.2139/ssrn.2820060.

Utz, Christine/Koloßa, Stephan/Holz, Thorsten/Thielbörger, Pierre (2019): »Die DSGVO als internationales Vorbild? Erste Forschungsergebnisse zu

Grundprinzipien der DSGVO und Gedanken zu ihrer Umsetzbarkeit«, in: Datenschutz und Datensicherheit – DuD 43, S. 700–705.

Volkamer, Melanie/Renaud, Karen (2013): »Mental models – general introduction and review of their application to human-centred security«, in: Marc Fischlin/Stefan Katzenbeisser (Hg.), Number theory and cryptography. Papers in honor of Johannes Buchmann on the occasion of his 60th birthday, Berlin/Heidelberg: Springer, S. 255–280.

Wagner, Isabel/Eckhoff, David (2018): »Technical privacy metrics: A systematic survey«, in: ACM Computing Surveys 51 (3), Artikel Nr. 57, S. 1–38.

Wash, Rick (2010): »Folk models of home computer security«, in: Sixth Symposium on Usable Privacy and Security (SOUPS), Artikel Nr. 11, S. 1–16, https://doi.org/10.1145/1837110.1837125.

Wash, Rick/Rader, Emilee (2015): »Too much knowledge? Security beliefs and protective behaviors among United States internet users«, in: Eleventh Symposium on Usable Privacy and Security (SOUPS), USENIX Association, S. 309–325.

Westin, Alan F. (1970): Privacy and freedom, New York: Atheneum.

Wylie, Christopher (2019): Mindf*ck. Cambridge analytica and the plot to break America, New York: Random House.

Yee, Ka-Ping (2004): »Aligning security and usability«, in: IEEE Security & Privacy 2 (5), S. 48–55.

Zuboff, Shoshana (2019): The age of surveillance capitalism: The fight for a human future at the new frontier of power, New York: PublicAffairs.

»Digitale Souveränität« als Kontrolle
Ihre zentralen Formen und ihr Verhältnis zueinander

Max Tretter

Abstract *In Diskussionen zum Umgang mit und zur Regulierung des Digitalen kommt dem Begriff der »digitalen Souveränität« eine herausragende Rolle zu. Dabei wird sie häufig als eine Form der digitalen Kontrollausübung beschrieben – wobei der Rekurs auf den Kontrollbegriff dazu dienen soll, das Konzept »digitaler Souveränität« genauer zu bestimmen. Trotz derartiger Präzisierungsversuche bleiben beide Begriffe oftmals unklar und es wird nicht deutlich, wer seine »digitale Souveränität« artikuliert, indem er in welchen Kontexten »digitale Kontrolle« über wen ausübt. Mein Beitrag zielt darauf, diesen Unklarheiten entgegenzuwirken und mittels eines Reviews des akademischen Diskurses zu einem besseren Verständnis beider Begriffe und ihres Zusammenhangs beizutragen. Dazu zeige ich in einem quantitativ-orientierten Codierungs- und Auswertungsprozess zuerst auf, dass als Hauptakteur*innen Nationen genannt werden, die ihre »digitale Souveränität« primär in den Kontexten IT-Architektur, Gesetzgebung und Nationale Sicherheit verfolgen. Anschließend nutze ich semantische Analysen, um vier digitale Kontrollformen zu beschreiben, die in den Diskussionen um digitale Souveränitätsausübung zentral genannt werden: der Ausbau ihrer nationalen Digitalinfrastruktur, digitale Gesetzgebung, digitale Zensur sowie digitale Grenzkontrolle. Am Beispiel dieser vier digitalen Kontrollformen zeigt mein Beitrag auf, wie der Zusammenhang von »digitaler Kontrolle« und »digitaler Souveränität« konzipiert wird – und trägt so zu einem besseren Verständnis des digitalen Souveränitätskonzepts als einer Form »digitaler Kontrolle« bei.*

1. Einleitung

Angesichts der fortschreitenden Digitalisierung sämtlicher Lebensbereiche (vgl. Stalder 2015) und der stetig zunehmenden Verflechtung von On- und Offline zu einem »Onlife« (vgl. Floridi 2015), den sich daraus ergebenden Mög-

lichkeiten zur individuellen Selbstentfaltung (vgl. Reckwitz 2017: 225–370) und gesellschaftlichen Entwicklung (vgl. Ternès von Hattburg 2020) einerseits, der damit einhergehenden Risiken neuer Monopole (vgl. Galloway 2018), überwachungskapitalistischer Freiheitsberaubungen (vgl. Zuboff 2018) und Privatheitsverluste (vgl. Véliz 2020) andererseits, stellt sich mit zunehmender Dringlichkeit die Frage, wie mit dem Digitalen umzugehen sei (vgl. Klenk/Nullmeier/Wewer 2020).

Ein Konzept, das im Zusammenhang mit dieser Frage regelmäßig auftaucht und den Umgang mit dem Digitalen leiten soll, ist »digitale Souveränität«. Zuerst war in China und Russland von »digitaler Souveränität« die Rede. Dort bezeichnete sie autoritäre Bestrebungen, den *digitalen Raum* zu territorialisieren und abzuschließen, ihn unter staatliche Kontrolle zu bringen, zu regulieren und zu steuern (vgl. Dammann/Glasze 2021). In den 2010er-Jahren fand »digitale Souveränität« Einzug in die deutschen und europäischen Debatten zur Internet- und Digitalpolitik (vgl. Misterek 2017), wo sie das zuvor dominierende Paradigma der »globalen Informationsgesellschaft« ablöste (vgl. Glasze/Dammann 2021). Als das »digitalpolitische Buzzword der Stunde« (Pohle 2021: 6) wird »digitale Souveränität« seither von Nationen als Staatsziel (vgl. Klenk/Nullmeier/Wewer 2020; Pohle/Thiel 2021), von (Digital-)Unternehmen als Leitfaden (vgl. D'Elia 2016; Pohle/Thiel 2020) und von Privatpersonen (vgl. Cardullo/Kitchin 2018; Pohle 2020) oder Interessengruppen (vgl. Stewart 2017; Cooper 2019) als Direktive genannt. Seine häufige Verwendung in verschiedenen Formen, vielfältigen Konstellationen und diversen Kontexten macht das digitale Souveränitätskonzept jedoch äußerst diffus (vgl. Pohle 2021) und führt zu Uneinigkeiten hinsichtlich seiner Bedeutung (vgl. Couture/Toupin 2019). Um das Konzept mit Gehalt zu füllen, greifen viele Autor*innen auf den Kontrollbegriff zurück (vgl. Hummel et al. 2018) und beschreiben »digitale Souveränität« als eine Form von Kontrolle bzw. Kontrollausübung, die entweder *im* Digitalen oder *durch* das Digitale stattfindet (vgl. Adonis 2019; Couture/Toupin 2019; Fabiano 2020; Schneider 2020; Hummel et al. 2021). Dabei lässt sich Kontrolle nach Luciano Floridi (2020: 371) in offener Weise verstehen als »the ability to influence something (e.g., its occurrence, creation, or destruction) and its dynamics (e.g., its behaviour, development, operations, interactions), including the ability to check and correct for any deviation from such influence«.

»Digitale Kontrolle« bezeichnet demnach die Fähigkeit, entweder instrumentell auf das Digitale zurückzugreifen, um ein Gegenüber zu beeinflussen, oder das Gegenüber bei seinem Umgang mit dem Digitalen zu beeinflussen.

Entgegen der damit verbundenen Intention, trägt der Rekurs auf den Kontrollbegriff wenig dazu bei, das Konzept »digitaler Souveränität« zu präzisieren, denn es bleibt unklar, *welche Akteur*innen in welchen Kontexten, mit welchen Mitteln und auf welche Weise* »digitale Kontrolle« *über wen* ausüben.

Ein kurzer Blick in den digitalen Souveränitätsdiskurs demonstriert, dass manche Autor*innen Nationen als zentrale Souveräne erkennen, die »digitale Kontrolle« gegenüber anderen Nationen (vgl. Adonis 2019; Schneider 2020), über Unternehmen (vgl. Jacob/Lawarée 2020) oder ihre Bürger*innen (vgl. Keshet 2020) ausüben. Andere hingegen identifizieren große Digitalunternehmen als Souveräne, die Kontrolle gegen Staaten (vgl. Floridi 2020) oder über Nutzer*innen ihrer Dienste ausüben (vgl. Fabiano 2020). Wiederum andere Autor*innen erfassen Individuen (vgl. Cardullo/Kitchin 2018; Pohle 2020) oder bestimmte Interessengruppen (vgl. Stewart 2017; Cooper 2019) als *digitale Souveräne*. Indem Individuen Besitzansprüche auf ihre persönlichen Daten erheben (vgl. Hummel/Braun/Dabrock 2020) oder entscheiden, wer sie zu welchem Zweck verwenden darf (vgl. Hummel et al. 2018), üben sie »digitale Kontrolle« aus (vgl. Hummel/Braun/Dabrock 2019). Manche Autor*innen verorten »digitale Kontrolle« in militärischen Verteidigungs- (vgl. Adonis 2019) oder Offensivkontexten (vgl. Kukkola 2018b). Andere ordnen »digitale Kontrolle« primär gesellschaftlichen Diskursen (vgl. Floridi 2020) und Aushandlungen individueller Privatheit (vgl. Celeste/Fabbrini 2021), gesellschaftlicher Repräsentation und Partizipation (vgl. Stewart 2017; Hummel/Braun/Dabrock 2019; Pierri/Herlo 2021) oder gemeinwohlorientierter Datenverwendung (vgl. Hummel et al. 2018; Hummel/Braun 2020) zu. Wiederum andere Autor*innen erkennen gesetzgeberische Akte (vgl. Floridi 2020), den Ausbau digitaler Infrastrukturen (vgl. Floridi 2020; Schneider 2020), digitalökonomischen Wettbewerb (vgl. Fabiano 2020) oder sogar die gezielte Datenspende (vgl. Hummel et al. 2018; Hummel/Braun/Dabrock 2019) als Formen digitaler Kontrollausübung.

Diese Vielzahl der genannten Akteur*innen und Kontexte illustriert in anschaulicher Weise, wie unterschiedlich »digitale Kontrolle« verstanden werden kann – und dass sie dem Konzept »digitaler Souveränität« hinsichtlich ihrer Vielfalt und Diffusität in nichts nachsteht. Der Rekurs auf »digitale Kontrolle« kann dennoch zu einem besseren Verständnis des digitalen Souveränitätskonzepts beitragen – besonders dann, wenn man sich auf die zentral genannten digitalen Kontrollformen fokussiert und herausarbeitet, wie sie beschrieben werden, d.h. *welchen Akteur*innen* häufig zugeschrieben wird, *in welchen Kontexten* »digitale Kontrolle« *wie* gegen *wen* auszuüben. Diesen Weg gehe ich in

meinem Beitrag und frage: Welche Formen »digitaler Kontrolle« werden häufig genannt? Wie werden sie beschrieben? Und wie können diese Beschreibungen uns dabei helfen, das Konzept »digitaler Souveränität« besser zu verstehen?

Um beide Fragen zu beantworten und die Zentralformen »digitaler Kontrolle« zu skizzieren, führe ich ein Review durch und untersuche den englischsprachigen, akademischen Diskurs um »digitale Souveränität«. Als Ergebnis dieser Untersuchung kann ich als Erstes aufweisen, dass digitale Kontrollansprüche im von mir analysierten Sample besonders häufig *Nationen* zugeschrieben werden und deren Ausübung überwiegend in den Kontexten *IT-Infrastruktur*, *Gesetzgebung* und *Nationale Sicherheit* verortet wird. Als Nächstes fokussiere ich mich auf vier zentrale Formen digitaler Kontrollausübung – den Ausbau digitaler Infrastruktur, das Erlassen von Digitalgesetzen, digitale Zensur und digitale Grenzkontrollen –, um zu zeigen, wie das Ausüben »digitaler Kontrolle« von Nationen in den drei meistgenannten Kontexten beschrieben wird. In einer anschließenden Diskussion stelle ich dar, wie man den Zusammenhang der beschriebenen Formen »digitaler Kontrolle« als Netzwerk wechselseitiger Ermöglichungs- und Förderungsbeziehungen verstehen kann, und gehe der Möglichkeit alternativer Formen digitaler Kontrollausübung nach, die weniger restriktiv vorgehen und die aus ethischer Perspektive zu bevorzugen wären. Abschließend fasse ich die Ergebnisse in einem Fazit zusammen und zeige, was die Darstellung zentraler Formen »digitaler Kontrolle« zum Verständnis »digitaler Souveränität« beitragen kann.

2. Methoden

Die verschiedenen Zentralformen »digitaler Kontrolle« werden in mehreren Schritten in einem multimethodischen Review untersucht. Das Review fokussiert auf Formen »digitaler Kontrolle«, die sich im akademischen Diskurs *um* »digitale Souveränität«, nicht in den digitalen *Souveränitätspolicies* selbst als zentral erwiesen haben.

Der entscheidende Schritt des Reviews besteht darin, innerhalb des akademischen Diskurses zentrale Formen »digitaler Kontrolle« ausfindig zu machen und anhand relevanter Textausschnitte semantisch zu analysieren. Dabei werden wichtige Passagen mittels Unterstreichung hervorgehoben, anschließend wird kontextualisierend und kommentierend erläutert, wie sie »digitale Kon-

trolle« präsentieren. Um die relevanten Textausschnitte ausfindig zu machen, wurde der qualitativen Analyse ein umfangreicher Such- und Sampling- sowie ein quantitativ orientierter Auswertungs- und Selektionsprozess vorgeschaltet (vgl. Moher et al. 2009; Jesson/Matheson/Lacey 2011; Strech/Sofaer 2012).

Ausgerichtet auf methodische Überlegungen zur Durchführung eines Reviews (vgl. Moher et al. 2009; Jesson/Matheson/Lacey 2011; Strech/Sofaer 2012), durchsuchte ich die Datenbanken Web of Science, Scopus, Pubmed und GIFT mit dem Suchbegriff »*digital sovereignty*« oder einer AND-Kombination der Begriffe »*digital*« und »*sovereignty*«. Ich entschied mich für diese Suchstrategie, da die Wortkombination »*digital*« und »*control*« zu viele Ergebnisse lieferte, von denen ein Großteil nicht in Verbindung mit »digitaler Souveränität« stand, die Kombination der Begriffe »*digital*« und »*sovereignty*« mit »*digital*« und »*control*« hingegen zu spezifisch war und zu wenige Ergebnisse lieferte. Um den Suchbereich so weit wie möglich zu stecken, durchsuchte ich Überschriften, Abstracts und Volltexte oder führte eine Themensuche durch und formulierte die Suchstrategie auf Englisch.

Die Suchstrategie lieferte insgesamt 125 akademische Publikationen. In einem ersten Schritt entfernte ich Duplikate (13) sowie die Publikationen, deren Volltext nicht zugänglich war (5). Aus den verbleibenden 107 Publikationen sortierte ich diejenigen aus, die »digitale Souveränität« *nicht* als Form »digitaler Kontrolle« verstanden (22). Ich behielt die Publikationen im Sample, die erstens den Begriff »Souveränität« in Verbindung mit dem Begriff »digital« erwähnen, z.B. »digitale Souveränität« oder »Souveränität des Digitalen«, *und* diesen zweitens mit einer Form von Kontrolle, wie sie oben definiert wurde, in Verbindung brachten. Zudem schloss ich Publikationen aus, in denen der Begriff »Souveränität« nicht erwähnt wurde, ausschließlich nicht digitale Souveränitätsformen erwähnt wurden (z.B. »staatliche Souveränität«, »Ernährungssouveränität«) (19) *oder* »digitale Souveränität« nicht mit einer Form von Kontrolle in Verbindung gebracht wurde (3). 22 Papers erfüllten diese inhaltlichen Inklusionskriterien nicht, sodass das finale Sample 85 Publikationen enthielt.

Das finale Sample analysierte ich anschließend mit Fokus auf die Passagen, die »digitale Souveränität« thematisieren. Mithilfe des Programms *Atlas.Ti* codierte ich, welche Akteur*innen dort als Träger »digitaler Souveränität« aufgeführt werden und in welchen Kontexten »digitale Souveränität« genannt wird. Die Codes der beiden Kategorien – d.h. der Akteur*innen und der Kontexte – entnahm ich induktiv den Textpassagen (vgl. Burnard 1991) und überprüfte deren Validität anschließend an weiteren Passagen. Ich behielt einen Code, wenn er in mehreren Passagen vorkam, und verwarf

oder modifizierte ihn, wenn er in sämtlichen Textpassagen des Samples nur einmal vorkam. In mehreren Iterationen und kontinuierlichen Erhebungen, Verwerfungen und Korrekturen wurden so 319 Textpassagen in 85 Publikationen entlang von 20 Codes in zwei Kategorien (10 Akteur*innen, 10 Kontexte) codiert. Ziel dieser Codierungen war es, herauszuarbeiten, welche Akteur*innen und welche Kontexte zentral für »digitale Kontrolle« sind – und die anschließende qualitative Analyse auf diese Akteur*in-Kontext-Konstellationen fokussieren zu können.

Um zu überprüfen, ob die meistgenannten Souveränitätsakteur*innen ihre »digitale Kontrolle« auch in den am häufigsten genannten Kontexten ausüben, führte ich anschließend eine *Kookkurrenzanalyse* durch – d.h. ich errechnete die Zahl der Passagen, in denen zwei Codes aus verschiedenen Kategorien gemeinsam auftreten.

3. Ergebnisse

In diesem Abschnitt präsentiere ich zuerst die Ergebnisse der quantitativ orientierten Analyse, um so die relevanten Akteur*in-Kontext-Konstellationen »digitaler Souveränität« im Sample herauszuarbeiten. Diese Konstellationen nehme ich zum Ausgangspunkt, um anschließend die zentral vorkommenden Formen »digitaler Kontrolle« zu präsentieren. Dazu entnehme ich diesen Konstellationen paradigmatische Textpassagen und kontextualisiere sowie kommentiere sie anschließend.

3.1 Zentrale Akteur*innen und Kontexte »digitaler Souveränität«

Die quantitativ orientierte Analyse der Textpassagen hat ergeben, welche Akteur*innen als Träger »digitaler Souveränität« genannt werden und in welchen Kontexten »digitale Souveränität« vorkommt. Die Ergebnisse sind in unten stehender Tabelle absteigend nach Häufigkeit sortiert.[1]

1 Es ist zu beobachten, dass die als Code vorkommenden Akteur*innen und Kontexte den Akteur*innen und Kontexten des Datensouveränitätskonzepts stark ähneln (vgl. Hummel et al. 2021). Diese Ähnlichkeit ist wenig überraschend, da sich beide Konzepte sehr nahe stehen und häufig synonym verwendet werden (vgl. Adonis 2019; Hummel et al. 2021).

*Tabelle 1 Tabellarische Darstellung der Akteur*innen und Kontexte, die in den codierten Passagen mehr als einmal genannt wurden; absteigend nach Häufigkeit sortiert.*

Akteur*innen		Kontexte	
*Welche Entitäten werden als Träger*innen »digitaler Souveränität« genannt?*		*Was ist der umfassendere Bereich und/oder das Thema, das den Hintergrund für die Erwähnung der Souveränität bildet?*	
Nationen (191)	z.B. China, die Vereinigten Staaten, Mexiko (vgl. Schneider 2020), Russland (vgl. Kukkola 2018b), BRICS (vgl. Demidov 2014)	**IT-Architektur** (91)	Gestalten von Informations- und Kommunikationstechnologien und Pflegen digitaler Daten, Codes und Algorithmen
Privatrechtliche Unternehmen (42)	z.B. »Google, Facebook and Twitter« (Nocetti 2016: 1265), Youtube (vgl. Stewart 2017), »US-based companies« (D'Elia 2016: 6)	**Gesetzgebung** (72)	Ausarbeiten und/oder Anwenden eines Rechtskodex
Regierungsorganisationen (38)	z.B. nationale Rechtsprechung (vgl. Livshitz/Neklyudov/Lontsikh 2018), »Kremlin« (Budnitsky/Jia 2018: 14), »NSA« (Nocetti 2016: 1265)	**Nationale Sicherheit** (65)	Militärische Landesverteidigung (defensiv wie offensiv) und Sichern der Gesellschaft und öffentlichen Ordnung u.a. durch Überwachungs- und polizeiliche Maßnahmen
Bürger*innen (27)	Angehörige eines Staates oder einer Union, z.B. »Russian citizen« (Ermoshina/Musiani 2017: 46)	**Wirtschaft und Gewerbe** (40)	Erzielen, Erhalten und Verteilen des wirtschaftlichen Wohlstands

Konsument*innen (19)	Individuen, die digitale Anwendungen oder Dienstleistungen nutzen, z.B. Cloud Server (vgl. Markl 2019), Freeware (vgl. Couture/Toupin 2019)	**Gesellschaftlicher Diskurs und Interessenvertretung** (32)	Gestaltung des öffentlichen Diskurses, der Zivilgesellschaft und der kollektiven Willensbildung
Nicht-Regierungs-Organisationen (16)	Interessengruppen, Organisationen der Zivilgesellschaft, z.B. »Italian Privacy Data Protection Authority« (Fabiano 2020: 271)	**Internationale Beziehungen** (30)	Beziehungen zwischen Nationalstaaten und Regimen (vgl. Nicholson 1998)
Zwischenstaatliche Organisationen (16)	Globale oder multilaterale Programme, die von mehreren nationalen Regierungen eingerichtet und vorangetrieben werden	**Forschung** (14)	Generierung von Evidenz und Wissen, z.B. in der Biomedizin, den Sozialwissenschaften, der Wirtschaft
Gesellschaften (9)	Eine Gruppe von Personen, die sich anhand bestimmter Merkmale konstituiert und nach außen abgrenzt (vgl. Kosorukov 2017)	**Bildung und Kapazitätsaufbau** (11)	Fördern von Kenntnissen und Fähigkeiten im Umgang mit digitalen Infrastrukturen
Indigene Bevölkerungen (8)	z.B. Native Americans (vgl. Stewart 2017), First Nations (vgl. Couture/Toupin 2019)	**Öffentliche Verwaltung** (7)	Regierung und Erfüllen staatlicher Aufgaben (vgl. Henry 2017)
Expert*innen (8)	z.B. Ingenieur*innen (vgl. Arsène 2015: 25), Wissenschaftler*innen (vgl. Kukkola/Ristolainen 2018: 80)	**Soft Law** (5)	Nicht verbindliche Übereinkünfte, die bloßes Einhalten codifizierter Vorschriften übersteigen (vgl. Shaffer/Pollack 2010)

Betrachtet man die Häufigkeit, mit der die Codes in den Passagen vorkommen, zeigen sich deutliche Schwerpunkte. Von den insgesamt 374 codierten Akteur*innennennungen entfallen 191 – und damit mehr als die Hälfte (51,1 %) aller Nennungen – auf *Nationen*. Dies stimmt mit vorherigen Beobachtungen zum nationalen Profil des digitalen Souveränitätsbegriffs überein (vgl. Adonis 2019). Die meistgenannten Nationen sind, in absteigender Reihenfolge, Russland, China, die Europäische Union, die Vereinigten Staaten und die BRICS-Staaten. Von 358 codierten Kontextnennungen sticht kein Einzelkontext so deutlich hervor wie jener der Nationen bei den Akteur*innen. Die drei meistgenannten Kontexte *(IT-Architektur*, *Gesetzgebung* und *Nationale Sicherheit)* umfassen mit insgesamt 221 Nennungen jedoch deutlich mehr als die Hälfte aller Kontextnennungen (61,7 %). Diese Ergebnisse zeigen einen deutlichen Fokus digitaler Souveränitätsnennungen auf den*die Akteur*in *Nationen* sowie die Kontexte *IT-Architektur*, *Gesetzgebung* und *Nationale Sicherheit*.

Die Ergebnisse der *Kookkurrenzanalyse* legen nahe, dass die digitale Souveränitätsausübung von *Nationen* als meistgenannten Akteur*innen auch in den am häufigsten genannten Kontexten *(IT-Architektur*, *Gesetzgebung* und *Nationale Sicherheit)* verortet wird. Dies illustriert Tabelle 2, die die Zahl der Kookkurrenzen zwischen den Codes zweier Kategorien nennt. Zur besseren Übersichtlichkeit ist die Tabelle farbcodiert: Je höher die *Kookkurrenzwerte* zweier Codes, desto dunkler ist das Feld hinterlegt, je niedriger diese sind, desto heller das Feld.[2]

Zusammenfassend zeigen die Ergebnisse der quantitativ orientierten Analyse, dass »digitale Souveränität« in erster Linie als ein Bestreben von *Nationen* (51,6 %) in den Kontexten *IT-Architektur* (56), *Gesetzgebung* (51) und *Nationale Sicherheit* (59) beschrieben wird. Wenn ich im Folgenden näher untersuche, wie »digitale Souveränität« als Form »digitaler Kontrolle« ausgeübt wird, werde ich mich auf diese Akteur*in-Kontext-Konstellationen fokussieren.

2 Die Summe der in der Tabelle für jeden Code gelisteten Kookkurrenzen kann höher sein als die Zahl der in obiger Tabelle 2 festgehaltenen Gesamtnennungen eines Codes. Diese Abweichung kommt zustande, da ein Code in einer Textpassage mit mehreren anderen Codes *kookkurrieren* kann.

*Tabelle 2 Kookkurrenztabelle der Akteur*innen und der Kontexte. Angegeben werden die absoluten Zahlen der Kookkurrenzen. Die Farbcodierung der Darstellung folgt den absoluten Zahlen der Kookkurrenzen.*

	Nationen (191)	Privatrechtl. Unternehmen (42)	Regierungsorganisationen (38)	Bürger*innen (27)	Konsument*innen (19)	NGOs (16)	Zwischenstaatl. Organ. (16)	Gesellschaften (9)	Indigene Bevölkerungen (8)	Expert*innen (8)
IT-Architektur (91)	56	14	13	7	4	3	6	1	0	3
Gesetzgebung (72)	51	10	10	7	2	2	3	1	2	1
Nationale Sicherheit (65)	59	3	7	2	1	1	2	1	0	1
Wirtschaft und Gewerbe (40)	20	13	7	2	0	2	5	3	1	0
Gesellschaftlicher Diskurs und Interessenvertretung (32)	12	3	4	6	5	5	1	3	1	0
Internationale Beziehungen (30)	24	4	2	0	0	1	5	0	1	1
Forschung (14)	4	0	1	0	1	0	0	0	0	5
Bildung und Kapazitätsaufbau (11)	3	0	2	1	2	0	0	1	0	0
Öffentliche Administration (7)	2	0	2	4	1	0	0	0	0	0
Soft Law (5)	2	0	0	0	0	0	0	0	3	0

3.2 Formen der digitalen Kontrollausübung im Kontext »digitaler Souveränität«

Der Durchgang durch die Publikationen zeigt die Vielfalt digitaler Kontrollformen, mit der die Ausübung »digitaler Souveränität« durch *Nationen* in den Kontexten *IT-Architektur*, *Gesetzgebung* und *Nationale Sicherheit* beschrieben wird. Vier Formen »digitaler Kontrolle« werden dabei besonders häufig genannt: Ausbau der digitalen Infrastruktur, digitale Gesetzgebung, digitale Zensur und digitale Grenzziehung. Diese vier Formen »digitaler Kontrolle« skizziere ich nachfolgend.

Ausbau der digitalen Infrastruktur

Als erste Form »digitaler Kontrolle« wird der Ausbau nationaler Digitalinfrastukturen genannt. Dieser finde auf mehreren Ebenen statt (vgl. Kagermann/Streibich/Suder 2021), angefangen bei der Sicherung von Rohstoffen und Produktionskapazitäten über das Verlegen von Kabeln, den Bau von Servern und Knotenpunkten sowie das Inbetriebnehmen von Satelliten und die Vergabe von Domainnamen (vgl. Arsène 2015) bis hin zum Etablieren eigener bzw. die Zusammenarbeit mit bestehenden Digitalplattformen (vgl. Schneider 2020). Durch diesen umfassenden Ausbau ihrer digitalen Infrastrukturen sicherten Nationen auf der einen Seite ihre Unabhängigkeit gegenüber anderen Akteur*innen, auf deren Digitalinfrastrukturen sie fortan weniger oder gar nicht mehr angewiesen sind. Auf der anderen Seite schaffen Nationen so die Grundlagen für eine Kontrollausübung gegen andere Akteur*innen. Als exemplarisches und paradigmatisches Beispiel eines solchen Digitalinfrastrukturausbaus wird Russland mit seinen Bestrebungen, eine nationale Informationsumgebung mit dem Namen *RuNet* zu etablieren, angeführt. Anfangs als Projekt zum Erschaffen einer russischen Informationsumgebung initiiert – d.h. eines russischsprachigen Raums im Internet, der auf der russischen Kultur, Spiritualität und dem »Russian way of doing things« (Ristolainen 2017: 12) basiert –, sei RuNet nach und nach in staatliche Kontrolle überführt (vgl. Lonkila/Shpakovskaya/Torchinsky 2019) und in russische Programme zum Ausbau der nationalen »digitalen Souveränität« eingegliedert worden (vgl. Asmolov/Kolozaridi 2020).

> »The updated program would include plans to eliminate the dependence of RuNet from external networks and to ensure that RuNet would be fully controlled by the state. *Minkomsvyaz* [das Russische Kommunikationsminis-

> terium – MT] declared that by 2020, ninety-nine percent of Russian Internet traffic would be transmitted within the country and that a ›back-up copy‹ of ninety-nine percent of the ›critical infrastructure‹ within Russia would be created.« (Ristolainen 2017: 118, Herv. i.O.)

Das Ziel der staatlichen Übernahme des RuNet bestünde darin, wie Ristolainen (2017) herausarbeitet, dass der Großteil des russischen Datenaustauschs landesintern, d.h. im russischen Territorium und auf russischer Infrastruktur, stattfindet. Auch die kritische Infrastruktur Russlands und ihre Back-ups sollten mittel- bis langfristig ganz ins RuNet verlagert werden (vgl. Nikkarila/Ristolainen 2017; Stadnik 2019).

Das Etablieren einer solchen Informationsumgebung sei, wie Kukkola (2018a: 6, eigene Herv.) unterstreicht, eng mit digitalen Kontrollbestrebungen verbunden:

> »Additionally, technological and administrative solutions behind ›digital sovereignty‹ may provide Russia a unified, resilient and deeply protected national segment of Internet which can be disconnected from the global Internet at will. At the same time, Russia would be free to take advantage of the vulnerabilities of other nations. This would have far ranging strategic implications on the international level. It should shape our thinking on such issues as deterrence, resilience, and escalation control in cyberspace.«

Eine nationale Informationsumgebung, die sich im Zweifelsfall vom globalen Internet abtrennen ließe, als eigenständiges, nationales Netzwerk unabhängig vom globalen Internet fortexistieren und den nationalen Datenaustausch aufrechterhalten sowie die nationale kritische Infrastruktur beherbergen könnte (vgl. Kukkola 2018a; Nikkarila/Ristolainen 2017), verleihe Russland Unabhängigkeit gegenüber anderen Akteur*innen und deren digitaler Infrastruktur (vgl. Kukkola 2018a). Mit einem eigenständigen RuNet würde Russland nicht mehr darauf angewiesen sein, Kabel, Satelliten oder Server in US-amerikanischer, chinesischer oder privater Hand zu nutzen. Damit verlören staatsfremde Akteur*innen die Einfluss- und Kontrollmöglichkeiten, Druck gegen Russland auszuüben, indem sie den russischen Datenaustausch oder die kritische Infrastruktur behindern oder blockieren (vgl. Ristolainen 2017).

Damit schaffe Russland sich einen asymmetrischen Vorteil, der darin bestehe, dass andere Akteur*innen, v.a. Nationen, die nicht über eine vergleichbare nationale Informationsumgebung verfügen, noch immer abhängig

von den Digitalinfrastrukturen anderer Akteur*innen und dem transnationalen Datenaustausch sind. Diese Abhängigkeiten könne sich Russland einseitig zunutze machen. Wo andere Akteur*innen auf russische Digitalinfrastruktur angewiesen sind, könne es den Zugriff auf diese als Druckmittel zur Kontrollausübung einsetzen (vgl. Schneider 2020). Aber auch dort, wo Akteur*innen auf andere, nicht russische Digitalinfrastruktur angewiesen sind, könne es diese Abhängigkeit nutzen, den transnationalen Informationsfluss durch Cyberangriffe stören – und dadurch deren Datenaustausch und Teile der kritischen Infrastruktur anderer Akteur*innen kritisch behindern (vgl. Singer/Friedman 2014).

Wie einige Autor*innen am Beispiel RuNet zeigen, nutze Russland den Ausbau der eigenen Digitalinfrastruktur in doppeltem Sinne zur »digitalen Kontrolle«: Nach außen gewinne Russland durch RuNet Unabhängigkeit von anderen Akteur*innen und verhindere, dass diese »digitale Kontrolle« gegen Russland ausüben. Gleichzeitig räume diese Unabhängigkeit Russland einen asymmetrischen Vorteil ein, den der Staat nutzen könne, um Kontrolle gegen andere Akteure auszuüben (vgl. Nikkarila/Ristolainen 2017). Neben der Unabhängigkeit Russlands, die der Staat durch den Ausbau seiner Digitalinfrastruktur gewonnenen hat und als Form der offensiven Kontrollausübung gegen andere Akteur*innen wenden kann, erkennen einige Autor*innen weltweit auch andere Möglichkeiten, die durch digitale Infrastruktur gewonnene Unabhängigkeit zu nutzen. So visiere beispielsweise Europa mit Projekten wie seiner Dateninfrastruktur *Gaia-X* und dem Errichten eines *europäischen Datenraums* (IDSA) (vgl. Braud et al. 2021) oder Deutschland mit dem Entwickeln einer sogenannten »*Bundescloud*« (vgl. BMI et al. 2021) ebenfalls den Ausbau der eigenen Digitalinfrastruktur an (vgl. Möllers 2020) – bringe die dadurch gewonnene Unabhängigkeit jedoch nicht *gegen* andere Akteur*innen in Stellung, sondern nutze sie, um europäische Daten vor fremdem Zugriff und damit die Souveränität ihrer Bürger*innen vor fremder Kontrollausübung zu schützen (vgl. Schneider 2020).

»Digitale Kontrolle« durch Gesetzgebung

Als weitere, nach innen auf die eigenen Bürger*innen sowie die im eigenen Territorium agierenden Unternehmen gerichtete Form »digitaler Kontrolle« wird Gesetzgebung identifiziert (vgl. Klafki/Würkert/Winter 2017). Wie eine gesetzliche digitale Kontrollausübung aussehen kann, zeigt Ristolainen am Beispiel Russland:

> »Russia has intensively ratified new laws that meet the objectives of both the Information Security Doctrine and the Strategy on the Development of an Information Society. Between 2012 and 2014, the Russian government passed several laws that aimed at gaining a complete control over RuNet and, some of these laws were tightened in the period 2015–2017. These laws, for instance, allow the Federal Service for Supervision of Communications, Information Technology and Mass Media *(Roskomnadzor)* to block and to censor harmful information and websites deemed extremist or a threat to public order. They also demand that owners and operators of websites store all information about the arrival, transmission, delivery, and processing of voice data, written text, images, sounds, or other kinds of action and keep this content for six months. The laws limit anonymous money transfers and donations on the Internet and require all web-based writers (bloggers, social media accounts) with posts that exceed 3,000 page views to register with the government. They control the dissemination or re-dissemination (tweeting and retweeting) of ›extremist materials‹ […].In addition, the laws prohibit anonymous access to the Internet in public spaces.« (Ristolainen 2017: 119f., eigene Herv.)

Die von Ristolainen angeführten, im Kontext und zur Zielumsetzung der russischen *Information Security Doctrine* ratifizierten Gesetze zielen darauf, der russischen Regierung Kontrollmöglichkeiten im RuNet zu eröffnen (vgl. Kerr 2018). Indem diese Gesetze einen anonymen Zugang zum Internet an öffentlichen Orten verbieten, ebenso wie anonyme Geldtransfers und Spenden, indem sämtliche russische *Content Creators*, die eine Relevanzgrenze überschreiten, ihre Tätigkeit bei der Regierung registrieren müssen und indem Webseiten dazu verpflichtet werden, sämtliche Informationen über auf ihnen veröffentlichte und ausgetauschte Daten für mindestens sechs Monate zu speichern, führe die russische Regierung ein umfassendes Transparenz- und Nachverfolgbarkeitsdispositiv ein. Sämtliche im RuNet durchgeführten Aktionen ließen sich von den zuständigen Behörden nachvollziehen und Einzelpersonen zuordnen (vgl. Freedom House 2021c). Die damit praktizierte Überwachung sei selbst ein Moment der Kontrollausübung gegen alle im RuNet aktiven Akteur*innen (vgl. Domańska 2019; Vladimir/Vitaly 2019) und eröffne darüber hinaus die Möglichkeit weiterer, intensiverer Kontrollausübung gegen unliebsame Akteur*innen.

Diese Form der gesetzlichen Kontrollausübung sei jedoch nur möglich, solange die Daten in russischem Territorium bleiben – sie lasse sich jedoch nicht

mehr ausüben, sobald sich User*innen außerhalb des russischen Teils des Internets bewegen und ihre Daten in anderen Jurisdiktionsgebieten verarbeitet und gespeichert werden. Um dem entgegenzuwirken und zu verhindern, dass sich russische Bürger*innen so der Kontrollausübung entziehen, habe, so die These von Savelyev (2016), die russische Regierung Gesetze zur Datenlokalisierung erlassen.

> »The law #242-FZ was adopted on 1 September 2014. It obliges providers to ›store personal data of Russian citizens, used by internet services, on the territory of the Russian Federation‹. Providers must guarantee recording, systematization, accumulation, storage, updates, modifications and extraction of personal data using databases located on Russian territory. Non-compliance with this new law may result in total blockage of the service. […] Web services are also required to build backdoors for Russian secret services to access stored data.« (Ermoshina/Musiani 2017: 46, eigene Herv.)

Wie Ermoshina und Musiani darlegen, sind digitale Unternehmen gesetzlich dazu gezwungen, die von ihnen erhobenen und verarbeiteten Daten auf russischem Territorium zu speichern. Dies führe wiederum dazu, dass die Unternehmen die o.g. Vorschriften zur Transparenz und Nachvollziehbarkeit einhalten müssten. Somit seien auch nicht russische Digitalunternehmen, wollen sie ihre Dienste in Russland anbieten, verpflichtet, die Daten ihrer User*innen für sechs Monate zu speichern – und im Bedarfsfall den zuständigen Behörden zugänglich zu machen. Letzteres werde weiterhin dadurch vorangetrieben, dass sämtliche digitale Dienste per Gesetz eine *virtuelle Backdoor* besitzen müssten, d.h. die Möglichkeit, dass russische Behörden, teils unbemerkt von den Digitalprovidern selbst, auf deren Daten zugreifen können (vgl. Sargsyan 2016). Kämen die Unternehmen diesen Forderungen nicht nach, dürften sie ihre Dienste nicht auf russischem Territorium anbieten, und der Zugriff auf deren Onlinepräsenzen würde auf russischem Territorium geblockt (vgl. O'Driscoll 2020).

Einige Publikationen betonen, dass analoge gesetzliche Regulierungen zur Datenlokalisierung oder zur Transparentmachung und Nachvollziehbarkeit von Datenströmen auch in anderen Ländern erlassen wurden, beispielsweise in China (vgl. Cattaruzza et al. 2016), ebenso wie der Einbau von *Backdoors* in vergleichbarer Weise auch von der *NSA* gefordert wurde (vgl. Linder 2021). Solche Formen der Gesetzgebung erwiesen sich als digitale Kontrollausübung des Staates, die sich gegen Unternehmen sowie gegen die eigenen Staats-

bürger*innen richten. Im Gegensatz zu solchen, von vielen Autor*innen als autoritär eingestuften (vgl. Adonis 2019; Ristolainen 2017), gesetzlichen Kontrollausübungen gibt es andere Formen der Gesetzgebung, die als weniger autoritär wahrgenommen werden. Ein Beispiel hierfür stellt die europäische *General Data Protection Regulation* dar (vgl. Sharma 2020). Zwar reguliere auch diese den digitalen Datenaustausch, im Gegensatz zur russisch-chinesischen Gesetzgebung verpflichte sie jedoch in erster Linie Digitalunternehmen, die Daten ihrer User*innen vor zweckfremder Verwendung zu schützen, solange die User*innen einer solchen Verwendung nicht explizit zustimmen (vgl. ebd.). So ziele die europäische Digitalgesetzgebung nicht darauf ab, die eigenen Bürger*innen transparenter zu machen, sondern trage zu deren Anonymität, Selbstbestimmung und Souveränität bei (Fabiano 2020: 272) – und übe ihre eigene Kontrolle nicht gegen, sondern zum Wohl der eigenen Bürger*innen aus (vgl. Schneider 2020). Während beiderlei Formen der Gesetzgebung eine Form der digitalen Kontrollausübung darstellen, unterscheiden sie sich darin, gegen wen sie gerichtet sind und wer durch sie begünstigt bzw. wessen Macht durch sie gestärkt wird.

»Digitale Kontrolle« durch Zensur, Friction und Flooding

Gesetzgebung als eine Form digitaler Kontrollausübung auf struktureller Ebene wird, so halten einige Publikationen fest, auf inhaltlicher Ebene durch staatliche Zensur, d.h. das Zurückhalten von Informationen oder das Unterdrücken missfallender Meinungen, ergänzt. Digitale Zensur nutze unterschiedliche Algorithmen, *Spy-* und *Malwares*, um primär das Internet, gegebenenfalls aber auch Privatcomputer, nach missfallenden Meinungen und Informationen zu durchsuchen (vgl. Murdoch/Anderson 2008) und diese dann entweder automatisch oder nach manueller Überprüfung zu löschen oder den Zugriff auf diese zu verhindern (vgl. Leberknight et al. 2010). Häufig gehe dies – je nach gesetzlichem Hintergrund – einher mit einer anschließenden Überwachung der Personen, einer Einschränkung ihres Internetzugangs oder mit Geldstrafen (vgl. Ruan/Knockel/Crete-Nishihata 2020). Durch solch restriktive Maßnahmen können staatliche Regierungen kontrollieren, auf welche Informationen die Bevölkerung zugreifen darf – und damit nicht nur die freie Meinungs*äußerung*, sondern auch deren freie Meinungs*bildung* beschränken (vgl. Freedom House 2021b).

Wie in exemplarischer Weise der »*Freedom on the Net 2021*«-Report alljährlich berichtet, übten viele Nationen »digitale Kontrolle« mittels Zensur aus (vgl. ebd.). Dabei herrsche, wie der Report in seiner Ausgabe aus dem Jahr

2021 hervorhebt, in China »the worst environment for internet freedom for the seventh year in a row« (ebd.: 1) und habe weltweit eines der ausgefeiltesten Zensursysteme (vgl. Freedom House 2021a). Wie Nguyen-Thu (2018) herausarbeitet, übe China seine Zensur in zwei speziellen Formen aus: *Friction* und *Flooding*. *Friction* beschreibt den Einsatz eines umfassenden digitalen Sicherungssystems, das dazu beiträgt, sämtliche nicht chinesischen bzw. alle nicht von der chinesischen Regierung erlaubten Digitalplattformen zu blockieren. Diese sogenannte »Great Firewall« verhindere, dass chinesische Staatsbürger*innen ohne größeren Aufwand auf missliebige Plattformen zugreifen können (vgl. Griffiths 2021), zu denen u.a. Tech-Giganten wie Google, Facebook, Instagram und Twitter gehören (vgl. Perunicic 2021). Mit der Blockade dieser Plattformen hemme die chinesische Regierung freien Informationszugang und freie Meinungsäußerung (vgl. Griffiths 2021) – und schaffe eine »bereinigte« Form des Internets, in der nur das existiert, was von den chinesischen Zensurbehörden zugelassen wird (vgl. Lams 2018). Begleitet werde *Friction* durch *Flooding*, eine Strategie des gezielten Produzierens und Verbreitens riesiger Informationsmengen auf chinesischen wie globalen Digitalplattformen. Die dafür notwendigen Berge an Informationen werden von »armies of people or bots« (Farrell 2018) extra produziert, die einzig für diesen Zweck von der chinesischen Regierung angestellt bzw. programmiert wurden. Das Ziel des *Flooding* bestehe darin, unerwünschte Informationen in einer Menge irrelevanter oder falscher Informationen auf- und untergehen zu lassen, sodass diese kaum mehr zu finden und vom umgebenden Informationsüberschuss zu unterscheiden sind (vgl. Roberts 2018). Dies solle es Algorithmen und menschlichen Internetnutzer*innen möglichst schwer machen, an sie heranzukommen.

Benennt *Friction* demnach das gezielte Beschränken von Informationen für die eigene Bevölkerung, bezeichnet *Flooding* das planmäßige Produzieren von Informationsüberschüssen sowohl für die eigene Bevölkerung als auch für die Weltöffentlichkeit. Beide werden als einander ergänzende Ansätze zur Manipulation der Informationsbeschaffungs-, -auswertungs- und -produktionsmöglichkeiten im Interesse der chinesischen Regierung beschrieben. Durch das Etablieren eigener Alternativplattformen zu den westlichen Digitalplattformen (vgl. Rottwilm 2016) sowie die enge Zusammenarbeit mit diesen habe die chinesische Regierung diese Informationskontrolle noch weiter ausgebaut (vgl. Budnitsky/Jia 2018). Mittels digitaler Zensur und aktiver Informationsmanipulationen übe sie somit eine effektive Form »digitaler Kontrolle« aus (vgl. Roberts 2014).

Kontrolle durch digitale Grenzziehung

Als vierte Zentralform digitaler Kontrollausübung wird im digitalen Souveränitätsdiskurs digitale Grenzziehung genannt. Wird das Ziehen und Schützen territorialer Grenzen seit jeher als eine Form souveräner Kontrollausübung erachtet (vgl. Brown 2010), beobachten einige Autor*innen deren allmähliche Ausdehnung auf den digitalen Raum. Dies habe einerseits zur Folge, dass territoriale Grenzen fortan zunehmend digital kontrolliert werden und Algorithmen als »Sortiermaschinen« auftreten (vgl. Mau 2021), andererseits, dass digitale Territorien beansprucht, durch Grenzen eingezäunt und von anderen abgegrenzt werden. Ein Musterbeispiel solch digitaler Territorialitätsbestrebungen liefere Russland mit seinem Ziel, das eigene digitale Territorium durch einen »digitalen Eisernen Vorhang« (Nation World News Desk 2021) zu schützen. Enthielten bereits der russische Ausbau ihrer nationalen Digitalinfrastruktur, die sich notfalls auch vom globalen Internet abtrennen ließe, sowie die russische Datenlokalisierungsgesetze protektionistische Momente, würden diese im Fall Russlands digitaler Territorialitätsbestrebungen überdeutlich. Grundlage einer solchen digitalen Grenzziehung ist, wie Kukkola and Ristolainen (2018: 83f.; eigene Herv.) festhalten, eine Projektion der territorialen Grenzen in den digitalen Raum:

> »Territoriality is increasingly projected into cyberspace. The Russian Federation is constructing the infrastructural basis for national control of the Internet. This process is explicitly connected to the concept of digital sovereignty. […] Digital sovereignty requires digital borders to mark the limits of state jurisdiction and power. Therefore, to ensure Russian digital sovereignty, the digital borders of a national segment of the Internet need to be delineated and protected, and cross-border control needs to be organised.«

Eng mit den Bemühungen um eine nationale Datenumgebung zusammenhängend, sollen digitale Grenzen dazu beitragen, das nationale Segment des Internets abzustecken, vom globalen Internet abzugrenzen sowie notfalls abtrennen zu können und v.a. den Grenzverkehr zu regeln. Wie Kukkola and Ristolainen (2018: 86) weiter ausführen, gibt es mehrere technische, institutionelle oder vertragliche Möglichkeiten, dies zu bewerkstelligen:

> »To ensure digital sovereignty, these borders must be protected. In cyberspace, this could be done through various technological means, institutions, information sharing, and agreements. Protection is facilitated by control, which means actors with authority and means to monitor and, if

> necessary, to intervene and to investigate illegitimate cross-border and internal traffic. Only through protected and controlled borders in cyberspace, however defined or constructed, can digital sovereignty be established in the national segment of the Internet.«

Digitale Grenzziehungen und -kontrollen erlauben einen Überblick darüber, wer sich innerhalb des eigenen Digitalraums aufhält und wer die digitalen Grenzen wann zu welchem Zweck überquert. Dies mache eine umfassende Überwachung möglich, ebenso wie das Einschränken des Grenzverkehrs zu bestimmten Zeiten, zu bestimmten Zwecken oder für bestimmte Personen (vgl. Bangkok Post 2021). Auf diese Weise realisiere Russland sein Ziel eines »digitalen Eisernen Vorhangs« (Nation World News Desk 2021) immer weiter. Dieses Mehr an »digitaler Kontrolle« soll, wie Kukkola (2018a) festhält, zum Schutz der nationalen Interessen und des nationalen Territoriums, kurz: zur nationalen Sicherheit beitragen. Gleichzeitig liefere die digitale Grenzziehung neben den defensiven auch »offensive advantage[s] in cyberspace« (ebd.: 1), indem sie – wie bereits das Etablieren einer unabhängigen nationalen Informationsumgebung – asymmetrische Informations- und Machtvorteile schaffe und es erlaube, diese strategisch oder abschreckend gegen andere Nationen in Stellung zu bringen (vgl. ebd.).

So wird digitale Grenzkontrolle im digitalen Souveränitätsdiskurs als ein Moment der digitalen Kontrollausübung von nationalen Regierungen gegen Einzelpersonen oder Unternehmen präsentiert. Es wird betont, dass und wie digitale Grenzkontrollen Nationen einen Vorteil an Informationen und Macht verschaffen – sie wissen, wer sich zu welchem Zweck in ihrem digitalen Raum befindet, und können den Grenzverkehr bei Bedarf einschränken oder sperren –, den Nationen zu defensiven oder offensiven Zwecken nutzen können.

4. Diskussion

In den Ergebnissen habe ich vier Formen digitaler Kontrollausübung von *Nationen* in den Kontexten *IT-Architektur*, *Gesetzgebung* und *Nationale Sicherheit* skizziert – der Ausbau von digitaler Infrastruktur, digitale Gesetzgebung, digitale Zensur und digitale Grenzziehung –, die in den Diskussionen um »digitale Souveränität« als zentrale Kontrollformen verhandelt wurden. Diese Ergebnisskizzen werfen drei Fragen auf: (1) Wie kann man das Verhältnis der vier Zentralformen »digitaler Kontrolle« zueinander verstehen? (2) Ste-

cken diese das gesamte Spektrum digitaler Kontrollmöglichkeiten ab? (3) Wie sind die dargestellten Formen digitaler Kontrollausübung ethisch zu bewerten? Diese Fragen werde ich diskutieren, indem ich zuerst eine Möglichkeit skizziere, das Zusammenwirken der verschiedenen Formen digitaler Kontrollausübung zu verstehen, anschließend auf die Limitationen der Untersuchung eingehe und dann eine ethische Einschätzung der Ergebnisse vornehme.

4.1 Zusammenwirken der verschiedenen Formen digitaler Kontrollausübung

Dass die vier Zentralformen »digitaler Kontrolle« häufig gemeinsam genannt werden, zeigt auf eindrückliche Weise Ristolainen (2017). Am Beispiel Russlands bringt er die vier oben dargestellten Formen »digitaler Kontrolle« – Digitalinfrastruktur (»RuNet«), Gesetzgebung (»developing laws«), digitale Zensur (»Internet censorship«) und digitale Grenzziehung (»extension of the existing territory«, »digital Westphalia«, »challenge […] open global Internet«) – in einem Zitat zusammen (s.u.), kennzeichnet sie explizit als Formen von *Kontrolle* (»control«) und *Macht* (»power«) und präsentiert sie als Momente der russischen Idee »digitaler Souveränität«:

> »Russia has engaged with cyberspace by adapting the idea of ›digital sovereignty‹ through the development of Internet censorship and *control*. RuNet – the Russian segment of the Internet – is considered an extension of existing territory in the Russian ›information space‹ and a promoter of a ›digital Westphalia‹ or ›cyber Westphalia‹. Over the recent years, RuNet has become a platform for the Russian state to use its *power* by developing laws and technical solutions that challenge the global open Internet.« (Ristolainen 2017: 113, eigene Herv.)

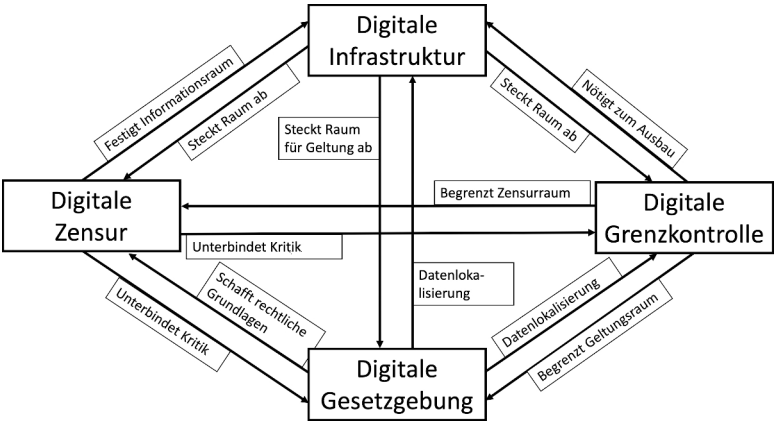
Gleichzeitig deutet Ristolainen (ebd.) an, dass die verschiedenen Formen »digitaler Kontrolle« zusammenwirken, wenn er aufzeigt, dass jede *Ausübung* »digitaler Kontrolle« in instrumenteller Weise (»through«, »by«) gleichsam andere Formen »digitaler Kontrolle« *ermöglichen* und *fördern* kann. Diesen Gedanken ausführend und die Darstellungen weiterer Autor*innen hinzuziehend, lässt sich zeigen, dass der Ausbau der digitalen Infrastruktur – indem er die Möglichkeiten fremder Kontrollausübung verringert und es den ausbauenden Akteur*innen ermöglicht, ihre gewonnene Unabhängigkeit in »digitale Kontrolle« zu überführen – vielfach als Voraussetzungen für anschließende Kontrollausübungen identifiziert wird. Wenn durch Gesetzgebung das Digitale re-

guliert wird, werde dadurch »digitale Kontrolle« ausgeübt und gleichzeitig die Möglichkeiten für weitere digitale Kontrollausübungen geschaffen, beispielsweise durch Gesetze zur Datenlokalisierung oder zum Datenschutz.

Diesen Gedankengang Ristolainens, dass sämtliche digitalen Kontrollformen miteinander wechselwirken und einander verstärken, werde ich nun am Beispiel Russlands explizieren und illustrieren, *wie* man die Wechselwirkungen zwischen den verschiedenen Formen »digitaler Kontrolle« – d.h. deren wechselseitiges Ermöglichen sowie Fördern und ihr Beitrag zur Steigerung des Gesamtmaßes an »digitaler Kontrolle« – verstehen kann. In der Zusammenschau verschiedener Diskussionsbeiträge lässt sich das Zusammenwirken verschiedener digitaler Kontrollformen in Russland so rekonstruieren: Der Ausbau der russischen Digitalinfrastruktur und das Etablieren einer nationalen Informationsumgebung ermögliche eine digitale Grenzziehung, während gleichzeitig die digitale Grenzziehung zur Abgrenzung des RuNet beitrage und damit die Herausbildung einer nationalen Digitalinfrastruktur befördere. Das Etablieren einer nationalen Digitalinfrastruktur stecke einen klaren Raum ab, in dem nationale Gesetze gelten und sich durchsetzen lassen. Umgekehrt trügen Gesetze zur Datenlokalisierung dazu bei, den Abfluss russischer Daten in fremde Nationen zu unterbinden, die digitalen Grenzen zu sichern und die nationale Informationsumgebung zu konsolidieren. Zuletzt sei es leichter, Zensur in einem begrenzten Digitalraum zu üben, während umgekehrt Zensur dazu beitrage, die nationale Digitalinfrastruktur als kohärente und umfassende Informationsumgebung ideologisch zu festigen. Digitale Gesetzgebung zur Löschung von Inhalten, die als extremistisch, terroristisch oder gefährlich für die öffentliche Ordnung eingestuft werden (vgl. Kravchenko 2019), trieben eine Zensur voran – ebenso wie digitale Grenzkontrollen, die verhindern, dass User*innen ihre verdächtigen Inhalte anderswo verbreiten oder in nichtregulierten Teilen des Internets Meinungen und Informationen finden, die in Russland zensiert werden. Umgekehrt verhindere die Zensur, dass Informationen oder Meinungen öffentlich verbreitet werden, die kritisch gegenüber einer restriktiven Gesetzgebung oder digitalen Grenzkontrollen eingestellt sind.

Diese Wechselbeziehungen zwischen verschiedenen Formen »digitaler Kontrolle«, die im Sample (oftmals implizit) identifiziert werden können, lassen sich schaubildhaft darstellen (s. Abb. 1).

Abbildung 1: Darstellung der Wechselbeziehungen zwischen verschiedenen Formen »digitaler Kontrolle«; konstruiert nach obigen Ausführungen zum Beispiel Russlands



Das Beispiel Russland zeigt eindrücklich, dass die verschiedenen Formen digitaler Kontrollausübung miteinander in Verbindung gebracht und wie deren wechselseitige Ermöglichungs- und Förderungsbeziehungen präsentiert werden. Gleichzeitig zeigen verschiedene Ausführungen zu den (oben angedeuteten) Wechselwirkungen zwischen *Friction* und *Flooding*, zu digitaler Gesetzgebung und dem Ausbau der digitalen Infrastruktur in China (vgl. Nguyen-Thu 2018), zur Digitalgesetzgebung in den Vereinigten Staaten – die sehr liberal ausfällt und es großen Plattformunternehmen erlaubt, ihre Dominanz auf dem globalen Digitalmarkt zu behaupten und auszubauen (vgl. Schneider 2020) – sowie zur Gesetzgebung der Europäischen Union, die auf einen Schutz europäischer Daten zielt und ihr Pendant in den Bemühungen zum Aufbau eines europäischen Datenraums finden (vgl. Braud et al. 2021), dass vergleichbare Wechselwirkungen auch zwischen den Formen digitaler Kontrollausübung anderer Länder identifiziert werden – und legen nahe, dass sich deren Gesamtzusammenhänge vermutlich in ähnlicher Weise rekonstruieren ließen.

4.2 Limitationen der Untersuchung

Die Darstellung der Zentralformen »digitaler Kontrolle« und ihrer Wechselbeziehungen wirft die Frage auf, ob damit *sämtliche* Formen »digitaler Kontrolle« erfasst sind oder ob obige Darstellungen sich um weitere digitale Kontrollfor-

men erweitern ließen. Diese Rückfrage lässt sich in Form von vier Limitationen darstellen – die ich abschließend um eine fünfte, fundamentalmethodologische Limitation ergänze.

Die erste Limitation betrifft die Beschaffenheit des analysierten Samples. In dieses wurden hauptsächlich Publikationen aus dem akademischen Diskurs *um* »digitale Souveränität« einbezogen, nicht jedoch die digitalen Souveränitätspolicies *selbst*, in denen das Konzept entworfen und eingesetzt wurde. Diese Fokussierung kann blinde Flecken oder Akzentverschiebungen zur Folge haben – beispielsweise bei bestimmten Formen digitaler Kontrollausübung, die in den *Policies* festgelegt wurden, im Diskurs aber zu wenig oder gar nicht beachtet oder umgekehrt übermäßig hervorgehoben wurden. Umgekehrt kann es sich als Vorteil erweisen, den Diskurs um »digitale Souveränität« und nicht digitale Souveränitätspolicies selbst zu analysieren. Denn wo Gesetzestexte gattungsmäßig sehr konzis sind und ihre Punkte so verdichtet wie möglich darlegen, bietet der Diskurs Platz für ausführliche Darstellungen, Systematisierungen und Kontextualisierungen. Folglich ist der Diskurs um digitale Souveränitätspolicies an vielen Stellen ausführlicher und mehrdimensionaler. Zudem hat in ihm bereits eine Sortierung stattgefunden, im Zuge derer die als zentral erachteten Aspekte mehr Aufmerksamkeit erfahren als die weniger zentralen.

Limitationen zwei und drei betreffen die Fokussierung, die während der Analyse des Samples vorgenommen wurde. So stammen, als zweite Limitation, alle präsentierten Formen »digitaler Kontrolle« aus den Konstellationen von Nationen und den drei meistgenannten Akteur*innen. Damit werden sämtliche Formen »digitaler Kontrolle«, die im Diskurs anderen Akteur*innen in anderen Souveränitätskontexten zugeschrieben werden, ausgeblendet – beispielsweise in ökonomischen (vgl. D'Elia 2016; Kukkola 2018a; Vladimir/Vitaly 2019), advokatorischen (vgl. Stewart 2017), *soft-law*- (vgl. ebd.), wissens- oder bildungsorientierten (vgl. Müller et al. 2020; Renz/Hilbig 2020) Kontexten. Als dritte Limitation fokussiert sich die Untersuchung in ihrem qualitativ orientierten Analyseteil auf nur vier zentrale Formen »digitaler Kontrolle« – obwohl insgesamt deutlich mehr Formen, wie Akteur*innen ihre Kontrolle in den drei betrachteten Kontexten ausüben, beschrieben werden. Neben infrastruktureller, gesetzgebender, informationsreglementierender und territorialer Kontrolle werden beispielsweise kulturelle oder narrative Kontrollformen genannt, die – darin der Zensur vergleichbar, aber mit anderen Mitteln vorgehend – auf eine Kontrolle der hermeneutischen Wahrnehmung zielen (vgl. Tretter 2021). Beiden Einwänden ist recht zu geben. Gleichzeitig

ist darauf hinzuweisen, dass es Ziel der Untersuchung war, *zentrale* Formen »digitaler Kontrolle« aus dem Diskurs zu analysieren, um mit deren Hilfe das Konzept »digitaler Souveränität« besser zu verstehen. Ein solches Vorgehen verlangt eine Selektion sowie das Setzen eines Fokus.

Die vierte Limitation betrifft die Voraussetzungen, die dieser Untersuchung zugrunde liegen. So folgt die Untersuchung, wie in der Einleitung dargelegt, einer großen Zahl von Autor*innen darin, dass sie zwischen »digitaler Souveränität« und »digitaler Kontrolle« einen engen Zusammenhang annimmt. Dieser enge Zusammenhang zwischen »digitaler Souveränität« und »digitaler Kontrolle« und der Beschreibung Ersterer als eine Form der Letzteren leuchtet einerseits ein. So kommt dem Moment der Kontrolle eine entscheidende und konstituierende Rolle in prominenten Souveränitätskonzeptionen zu (vgl. Philpott 2003). Umgekehrt stelle sich jedoch die Frage, ob wirklich *jede* Form »digitaler Souveränität« notwendig eine Form »digitaler Kontrolle« sein müsse oder ob es nicht auch andere mögliche Formen »digitaler Souveränität« gebe, die ohne Kontrolle auskommen oder nur ein geringes Maß dieser benötigen. Solche Formen kontrollloser oder -armer »digitaler Souveränität« sind aus der Untersuchung prämissenhaft ausgeschlossen.

Insgesamt weisen die Limitationen darauf hin, dass im Diskurs sowohl weitere Formen »digitaler Kontrolle« wie auch weitere Formen »digitaler Souveränität« beschrieben werden, die im Rahmen dieser Untersuchung nicht betrachtet wurden. Damit verweisen sie erneut auf die bereits zu Anfang diagnostizierte Vielgestaltigkeit des digitalen Souveränitätskonzepts und können als Warnung gelten, »digitale Souveränität« vorschnell auf ein Modell oder einige wenige Formen digitaler Kontrollausübung zu reduzieren.

Neben den vier inhaltlichen Limitationen muss auf eine fünfte methodologische Limitation hingewiesen werden. So wurde lediglich – quasi Beobachtungen beobachtend – untersucht, wie »digitale Souveränität« als »digitale Kontrolle« *beschrieben* wurde und wie die verschiedenen digitalen Kontrollformen im digitalen Souveränitätsdiskurs *präsentiert* wurden. Es wurde jedoch nicht untersucht, was »digitale Souveränität« »in Wirklichkeit«, d.h. abseits des Diskurses, ist und wie sie sich realweltlich darstellt. Ist diesem Einwand auf der einen Seite recht zu geben, ist ihm auf der anderen Seite zu entgegnen, dass enge Wechselbeziehungen zwischen der »wirklichen« Ausübung von »digitaler Souveränität« und »Kontrolle« und deren Beschreibung bestehen. Häufig ist die »Wirklichkeit« digitaler Souveränitäts- und -kontrollausübungen epistemisch kaum anders als durch Beschreibungen vermittelt wahrzunehmen sowie umgekehrt »wirkliche« Ausübungen »digitaler Souverä-

nität« und »digitaler Kontrolle« – frei nach dem Motto: das Leben imitiert die Kunst – nicht selten ein Reflex darauf sind, wie solche Ausübungen beschrieben werden. In diesem Sinne ist die Beobachtung zweiter Ordnung nicht per se als Defizit einzustufen, sondern kann im Gegensatz den Blick schärfen und sensibel machen für digitale Kontroll- und Souveränitätsausübungen »in der Wirklichkeit«.

4.3 Ethische Einschätzung

Neben den eher methodisch orientierten Rückfragen, die in den Limitationen benannt wurden, werfen die Ergebnisse auch ethische Fragen auf. Wie in der Einleitung bereits aufgezeigt, wurde das Konzept »digitaler Souveränität« ursprünglich in Russland und China entwickelt. Dort diente es als Leitkonzept für autoritäre Bestrebungen des Staates, den digitalen Raum zu territorialisieren, in staatliche Kontrolle zu überführen, zu regulieren und zu steuern (vgl. Dammann/Glasze 2021; Glasze/Dammann 2021). Dieses Ziel verfolgten beide Staaten, den Analysen des digitalen Souveränitätsdiskurses oben folgend, indem sie »restriktive« (vgl. Hummel et al. 2018; Schünemann/Kneuer 2021) Formen »digitaler Kontrolle« einsetzen. Die Restriktivität ihrer digital souveränen Kontrollausübung wird dort besonders deutlich, wo beschrieben wird, wie Russland oder China die eigene Digitalinfrastruktur ausbauen und staatliche Firewalls und digitale Grenzkontrollen etablieren, um dadurch ihren eigenen Digitalraum vom globalen Internet abzutrennen und fremde Akteur*innen aus diesem auszuschließen bzw. ihnen nur unter bestimmten Bedingungen Zugang zu ermöglichen. Richtet sich die Restriktivität mit diesen digitalen Kontrollausübungen protektionistisch nach außen, wendet sie sich in Formen der digitalen Zensur wie der Digitalgesetzgebung repressiv nach innen. So werden – den obigen Beschreibungen folgend – den eigenen Staatsbürger*innen Informationen vorenthalten bzw. nur die gewünschten Informationen zugänglich gemacht, sie werden auf bestimmte Transparenzvorschriften und Verhaltenskodizes festgeschrieben und ihre Verstöße wie Übertretungen geahndet. In seinen ursprünglichen Kontexten, so lässt sich mit Blick auf die Ausführungen zu Russland und China festhalten, wird »digitale Souveränität« mittels restriktiver Formen »digitaler Kontrolle« ausgeübt.[3] Dies wirft die Frage auf, ob das Konzept von diesen restriktiven Kontrollformen zu lösen ist, ob

3 Je systematischer die verschiedenen Formen restriktiver »digitaler Kontrolle« auftreten, sich – wie oben aufgezeigt – wechselseitig ermöglichen, fördern und stützen, des-

der »digitalen Souveränität« anhaltend ein restriktives Moment eingeschrieben ist oder ob sie sich, wenn in freiheitlich-demokratischen Kontexten adaptiert, weniger restriktiv gestalten lässt.

Betrachtet man exemplarisch das digitale Souveränitätskonzept der Europäischen Union, so wird dies als eines beschrieben, das freiheitlich-demokratisch darauf ziele, die Daten europäischer Staatsbürger*innen vor fremdem Zugriff sowie sie selbst vor ungewollter Beeinflussung und äußerer Kontrollausübung durch Dritte zu schützen – und so die digitalen Freiheitsräume der Bürger*innen zu erhalten oder zu erweitern (vgl. Fabiano 2020; Schneider 2020). Mit dieser freiheitsorientierten Zielsetzung wird ein deutlicher Unterschied zwischen dem europäischen Konzept »digitaler Souveränität« und den repressiven Formen digitaler Kontrollausübung in Russland oder China markiert. Allerdings lässt sich den Beschreibungen entnehmen, dass auch das digitale Souveränitätskonzept der Europäischen Union darauf zielt, einen *europäischen* Datenraum zu schaffen, in dem die Daten der EU-Bürger*innen zirkulieren können, ohne auf außereuropäische Digitalinfrastrukturen angewiesen zu sein (vgl. Braud et al. 2021). Zwar soll dieser europäische Datenraum dem Schutz der Freiheit europäischer Staatsbürger*innen dienen – doch zeigen sich in den geschilderten Anliegen, einen »eigenen« Datenraum zu schaffen und so weit wie möglich zu verhindern, dass die Daten von EU-Bürger*innen in »fremde« Datenräume abwandern, ebenso protektionistische Züge. Es ist demnach festzuhalten, dass auch das digitale Souveränitätskonzept der Europäischen Union nicht frei von restriktiven Momenten beschrieben wird – wenn diese auch deutlich mildere, d.h. weniger repressive, Formen annehmen als in China oder Russland. Ähnliche Ergebnisse würde vermutlich auch eine Untersuchung der Darstellungen des digitalen Souveränitätskonzepts der Vereinigten Staaten zutage fördern.

Aus der distanzierten Deskription heraustretend und die Rolle eines liberaldemokratisch sozialisierten Ethikers einnehmend, stellt sich die Frage, ob bzw. wie sich »digitale Souveränität« so gestalten ließe, dass sie möglichst wenig restriktiv ist – ohne dass das Konzept umgekehrt zu einem zahnlosen Tiger wird und die mit dem Konzept angestrebten Ziele, beispielsweise die digitalen Freiheitsräume der eigenen Bürger*innen zu erweitern oder zu erhalten, nicht mehr erreicht werden können. Hierzu bräuchte es Formen digitaler Kontrollausübung, die nicht primär restriktiv vorgehen. Wie solche wenig

to weniger Widerstand- und Subversionsmöglichkeiten bieten sie und desto kritischer werden sie.

oder nicht restriktiven Formen digitaler Kontrollausübung aussehen könnten und wie sich »digitale Kontrolle« auf eine wenig(-er) oder nicht restriktive Weise ausüben ließe, stellen z.B. Hummel, Braun und Dabrock (2019) am Beispiel individueller Datenspenden dar. Statt die eigenen Daten protektionistisch zu schützen, andere aus dem eigenen Einflussbereich auszuschließen und so eine restriktive Form »digitaler Kontrolle« auszuüben, könne sich »digitale Kontrolle« auch in nach außen gerichteten, interaktiven und partizipativen Prozessen zeigen. Indem Datenspender*innen ihre Daten bewusst für festgelegte Zwecke freigeben, könnten sie beeinflussen, wer welche Daten für welche Zwecke einsehen und nutzen darf. So könnten Datenspender*innen eine Form »digitaler Kontrolle« ausüben, die nicht restriktiv vorgeht, sondern durch Öffnung und partizipative Mitbestimmung lenkt – und damit sowohl sich selbst als auch anderen neue Freiheits- und solidarische Beziehungsräume eröffnen. Am Beispiel von KI-Anwendungen für den Public-Health-Bereich illustrieren Braun, Bleher und Hummel (2021), welche Schlüsselrolle dem Vertrauen beim Ausüben bedeutungsvoller »digitaler Kontrolle« zukommt und dass »digitale Kontrolle« dann an Bedeutung gewinne, wenn sie auf Vertrauen gründet. Und am Beispiel künstlich-intelligenter klinischer Entscheidungsunterstützungssysteme zeigen Bleher und Braun (2022), wie »digitale Kontrolle« und Verantwortung wechselseitig aufeinander angewiesen sind und dass es kontrolllose Verantwortung ebenso wenig geben solle wie verantwortungslose Kontrolle. Diese Beispiele zeigen auf, dass »digitale Kontrolle« nicht zwangsläufig auf eine primär restriktive Weise ausgeübt werden muss. Stattdessen lässt sich »digitale Kontrolle« auch auf Freigiebigkeit, Solidarität, Vertrauen oder Verantwortung gründen. Diese Darstellungen zeigen auf, dass und wie es prinzipiell möglich ist, »digitale Souveränität« auch von restriktionsfreien oder -armen Formen »digitaler Kontrolle« her neu zu denken – und dem Konzept dadurch eine Form zu geben, die aus ethischer Perspektive zu favorisieren ist, ohne ihm dadurch seine Zähne zu nehmen.[4]

4 Einschränkend sei an dieser Stelle erwähnt, dass die präsentierten Darstellungen restriktionsfreier oder -ärmerer »digitaler Kontrolle« in erster Linie auf individuelle oder institutionelle Akteur*innen fokussieren. Die Übertragung dieser digitalen Kontrollformen auf staatliche Ebene ist möglich, muss aber entsprechend reflektiert erfolgen.

5. Fazit

Die Ausgangsfrage meiner Überlegungen war, welche Formen »digitaler Kontrolle« im digitalen Souveränitätsdiskurs häufig genannt und wie sie beschrieben werden und wie sie zum Verständnis »digitaler Souveränität« beitragen können. Um diese Fragen zu beantworten, habe ich die Darstellung »digitaler Kontrolle« im digitalen Souveränitätsdiskurs untersucht. Eine erste, quantitativ orientierte Analyse des akademischen Diskurses hat ergeben, dass »digitale Souveränität« in erster Linie als ein Bestreben von *Nationen* in den Kontexten *IT-Architektur*, *Gesetzgebung* und *Nationale Sicherheit* beschrieben wird – zentrale Formen »digitaler Kontrolle« also primär in diesen Konstellationen zu suchen sind. In einer qualitativ orientierten Auseinandersetzung mit relevanten Textpassagen habe ich anschließend untersucht, wie vier Zentralformen »digitaler Kontrolle« – der Ausbau nationaler Digitalinfrastruktur, digitale Gesetzgebung, digitale Zensur sowie digitale Grenzkontrolle – präsentiert werden. In den Diskussionen habe ich schließlich aufgezeigt, wie das Zusammenwirken der verschiedenen digitalen Kontrollformen geschildert wird, und herausgearbeitet, dass sie in eine Wechseldynamik gegenseitigen Ermöglichens und Steigerns gestellt werden. Nach weiteren Hinweisen darauf, dass die dargestellten Formen nicht das gesamte Feld digitaler Kontrollausübungen umfassen, habe ich Vorschläge aufgezeigt, wie sich »digitale Kontrolle« auch weniger restriktiv, beispielsweise freigiebigkeits-, solidaritäts-, verantwortungs- oder vertrauensbasiert, denken ließe.

Diese Betrachtungen der Darstellungen zentraler digitaler Kontrollformen und ihres Zusammenwirkens können abschließend dazu beitragen, das Konzept »digitaler Souveränität« besser zu verstehen – indem sie in der Vielfalt seiner Konstellationen und Beschreibungen konkrete Einblicke ermöglichen, wie »digitale Kontrolle« wahrgenommen werden und welche zentralen Artikulationsformen »digitale Souveränität« annehmen kann. Dies kann dabei helfen, zukünftige akademische Diskussionen über »digitale Souveränität« und »digitale Kontrolle« zu orientieren und zum Verständnis in politischen Überlegungen beitragen.

Literaturverzeichnis

Adonis, Abid A. (2019): »Critical engagement on digital sovereignty in international relations: Actor transformation and global hierarchy«, in: Global:

Jurnal Politik Internasional 21 (2), S. 262, https://doi.org/10.7454/global.v2i1i2.412.

Arsène, Séverine (2015): »Internet domain names in China«, in: China Perspectives (4), S. 25–34, https://doi.org/10.4000/chinaperspectives.6846.

Asmolov, Gregory/Kolozaridi, Polina (2020): »Run runet runaway: The transformation of the Russian internet as a cultural-historical object«, in: Daria Gritsenko/Mariëlle Wijermars/Mikhail Kopotev (Hg.), The Palgrave handbook of digital Russia studies, Cham: Palgrave Macmillan, S. 277–296.

Bangkok Post (Hg.) (2021): »How Russia built its digital Iron Curtain«, in: Bangkok Post vom 23.10.2021. Online unter: https://www.bangkokpost.com/world/2202931/how-russia-built-its-digital-iron-curtain, abgerufen am 23.06.2022.

Bleher, Hannah/Braun, Matthais (2022): »Diffused responsibility: attributions of responsibility in the use of AI-driven clinical decision support systems«, in: AI and Ethics, https://doi.org/10.1007/s43681-022-00135-x

BMI/ITZBund/BSI/BfDI (2021): Bundescloud. Der Beauftragte der Bundesregierung für Informationstechnik. Online unter: https://www.cio.bund.de/Web/DE/Dienstekonsolidierung/Infrastruktur/Bundescloud/bundescloud_inhalt.html, abgerufen am 23.06.2022.

Braud, Arnaud/Fromentoux, Gaël/Radier, Benoit/Le Grand, Olivier (2021): »The road to European digital sovereignty with Gaia-X and IDSA«, in: IEEE Network 35 (2), S. 4–5, https://doi.org/10.1109/mnet.2021.9387709.

Braun, Matthias/Bleher, Hannah/Hummel, Patrik (2021): »A leap of faith: Is there a formula for ›trustworthy‹ AI?«, in: The Hastings Center Report 51 (3), S. 17–22, https://doi.org/10.1002/hast.1207.

Brown, Wendy (2010): Walled states, waning sovereignty, New York: Zone.

Budnitsky, Stanislav/Jia, Lianrui (2018): »Branding internet sovereignty: Digital media and the Chinese–Russian cyberalliance«, in: European Journal of Cultural Studies 21 (5), S. 594–613, https://doi.org/10.1177/1367549417751151

Burnard, Philip (1991): »A method of analysing interview transcripts in qualitative research«, in: Nurse Education Today 11 (6), S. 461–466, https://doi.org/10.1016/0260-6917(91)90009-y.

Cardullo, Paolo/Kitchin, Rob (2018): »Smart urbanism and smart citizenship: The neoliberal logic of ›citizen-focused‹ smart cities in Europe«, in: Environment and Planning C: Politics and Space 37 (5), S. 813–830, https://doi.org/10.1177/0263774x18806508.

Cattaruzza, Amaël/Danet, Didier/Taillat, Stéphane/Laudrain, Arthur (2016): »Sovereignty in cyberspace: Balkanization or democratization«, in: 2016

International Conference on Cyber Conflict (CyCon U.S.), Washington, D.C., S. 1–9, https://doi.org/10.1109/CYCONUS. 2016.7836628.

Celeste, Edoardo/Fabbrini, Federico (2021): »Competing jurisdictions: Data privacy across the borders«, in: Theo Lynn/John G. Mooney/Lisa van der Werff/Grace Fox (Hg.), Data Privacy and Trust in Cloud Computing, Cham: Palgrave Macmillan, S. 43–58.

Cooper, Lydia R. (2019): »A future perfect: Queer digital sovereignty in Joshua Whitehead's *Jonny Appleseed* and *full-metal indigiqueer*«, in: Contemporary Literatur 60 (4), S. 491–514, https://doi.org/10.3368/cl.60.4.491.

Couture, Stephane/Toupin, Sophie (2019): »What does the notion of ›sovereignty‹ mean when referring to the digital?«, in: New Media & Society 21 (10), S. 2305–2322, https://doi.org/10.1177/1461444819865984.

Dammann, Finn/Glasze, Georg (2021): »Regieren und Steuern«, in: Tabea Bork-Hüffer/Henning Füller/Till Straube (Hg.), Handbuch Digitale Geographien. Welt – Wissen – Werkzeuge, Paderborn/Leiden: Brill, Schöningh, S. 64–76.

D'Elia, Danilo (2016): »The economics of cybersecurity: From the public good to the revenge of the industry«, in: Adrien Bécu/Nora Cuppens-Boulahia/Frédéric Cuppens/Sokratis Katsikas/Costas Lambrinoudakis (Hg.), Security of Industrial Control Systems and Cyber Physical Systems. CyberICS WOS-CPS 2015 (= Lecture Notes in Computer Science, Band 9588), Cham: Springer, S. 3–15.

Demidov, Oleg (2014): »ICT in the Brics agenda before the 2015 summit: Installing the missing pillar?«, in: Security Index: A Russian Journal on International Security 20 (2), S. 127–132, https://doi.org/10.1080/19934270.2014.965968.

Domańska, Maria (2019): Gagging Runet, silencing society. »Sovereign« Internet in the Kremlin's political strategy. Centre for Eastern Studies (OSW) Commentary Number 313 vom 04.12.2019. Online unter: http://aei.pitt.edu/102358/, abgerufen am 23.06.2022.

Ermoshina, Ksenia/Musiani, Francesca (2017): »Migrating servers, elusive users: Reconfigurations of the Russian internet in the post-Snowden era«, in: Media and Communication 5 (1), S. 42–53, https://doi.org/10.17645/mac.v5i1.816.

Fabiano, Nicola (2020): »Digital sovereignty between ›accountability‹ and the value of personal data«, in: Advances in Science, Technology and Engineering Systems Journal 5 (3), S. 270–274, https://doi.org/10.25046/aj050335.

Farrell, Henry (2018): »China is weaponizing online distraction«, in: The Washington Post vom 01.10.2018. Online unter: https://www.washingtonpost.com/news/monkey-cage/wp/2018/10/01/china-is-weaponizing-online-distraction/, abgerufen am 23.06.2022.

Floridi, Luciano (2015): Die 4. Revolution. Wie die Infosphäre unser Leben verändert, Berlin: Suhrkamp.

Floridi, Luciano (2020): »The fight for digital sovereignty: What it is, and why it matters, especially for the EU«, in: Philosophy & Technology 33 (3), S. 369–378, https://doi.org/10.1007/s13347-020-00423-6.

Freedom House (2021a): China. Freedom on the Net 2021. Online unter: https://freedomhouse.org/country/china/freedom-world/2021, abgerufen am 23.06.2022.

Freedom House (2021b): Freedom on the Net. The Global Drive to Control Big Tech, Washington/New York: Freedom House.

Freedom House (2021c): Russia. Freedom on the Net 2021. Online unter: https://freedomhouse.org/country/russia/freedom-net/2021, abgerufen am 23.06.2022.

Galloway, Scott (2018): The Four. Die geheime DNA von Amazon, Apple, Facebook und Google, Kulmbach: Plassen.

Glasze, Georg/Dammann, Finn (2021): »Von der ›globalen Informationsgesellschaft‹ zum ›Schengenraum für Daten‹ – Raumkonzepte in der Regierung der ›digitalen Transformation‹ in Deutschland«, in: Thomas Döbler/Christian Pentzold/Christian Katzenbach (Hg.), Räume digitaler Kommunikation. Lokalität – Imagination – Virtualisierung, Köln: Halem, S. 159–182.

Griffiths, James (2021): The great firewall of China. How to build and control an alternative version of the internet, London: Bloomsbury.

Henry, Nicholas (2017): Public Administration and Public Affairs, New York/London: Routledge.

Hummel, Patrik/Braun, Matthias (2020): »Just data? Solidarity and justice in data-driven medicine« in: Life Sciences, Society and Policy 16 (1), S. 8, https://doi.org/10.1186/s40504-020-00101-7.

Hummel, Patrik/Braun, Matthias/Augsberg, Steffen/Dabrock, Peter (2018): »Sovereignty and data sharing«, in: ITU Journal: ICT Discoveries, Special Issue 2. Online unter: https://www.itu.int/en/journal/002/Documents/ITU2018-11.pdf, abgerufen am 23.06.2022.

Hummel, Patrik/Braun, Matthias/Augsberg, Steffen/von Ulmenstein, Ulrich/Dabrock, Peter (2021): Datensouveränität. Governance-Ansätze für den Gesundheitsbereich, Wiesbaden: Springer VS.

Hummel, Patrik/Braun, Matthias/Dabrock, Peter (2019): »Data donations as exercises of sovereignty«, in: Jenny Krutzinna/Luciano Floridi (Hg.), The ethics of medical data donation, Cham: Springer, S. 23–54.

Hummel, Patrik/Braun, Matthias/Dabrock, Peter (2020): »Own data? Ethical reflections on data ownership«, in: Philosophy & Technology 34 (3), S. 545–572, https://doi.org/10.1007/s13347-020-00404-9.

Hummel, Patrik/Braun, Matthias/Tretter, Max/Dabrock, Peter (2021): »Data sovereignty: A review«, in: Big Data & Society 8 (1), https://doi.org/10.1177/2053951720982012.

Jacob, Steve/Lawarée, Justin (2020): »The adoption of contact tracing applications of COVID-19 by European governments«, in: Policy Design and Practice, S. 1–15, https://doi.org/10.1080/25741292.2020.1850404.

Jesson, Jill K./Matheson, Lydia/Lacey, Fiona M. (2011): Doing your literature review. Traditional and systematic techniques, New York: Sage.

Kagermann, Henning/Streibich, Karl-Heinz/Suder, Katrin (2021): Digitale Souveränität. Status quo und Handlungsfelder, München: Acatech.

Kerr, Jaclyn A. (2018): The Russian model of internet control and its significance. Lawrence Livermore National Laboratory vom 21.12.2018. Online unter: https://www.osti.gov/servlets/purl/1491981/, abgerufen am 23.06.2022.

Keshet, Yael (2020): »Fear of panoptic surveillance: Using digital technology to control the COVID-19 epidemic«, in: Israel Journal of Health Policy Research 9 (1), S. 67, https://doi.org/10.1186/s13584-020-00429-7.

Klafki, Anika/Würkert, Felix/Winter, Tina (Hg.) (2017): Digitalisierung und Recht, Hamburg: Bucerius Law School Press.

Klenk, Tanja/Nullmeier, Frank/Wewer, Göttrik (Hg.) (2020): Handbuch Digitalisierung in Staat und Verwaltung, Wiesbaden: Springer VS.

Kosorukov, Artem A. (2017): »Digital government model. Theory and practice of modern public administration«, in: Journal of Legal, Ethical and Regulatory Issues 20 (3).

Kravchenko, Maria (2019): »Russian anti-extremism legislation and internet censorship«, in: The Soviet and Post-Soviet Review 46 (2), S. 158–186, https://doi.org/10.1163/18763324-04602004.

Kukkola, Juha (2018a): »Civilian and military information infrastructure and the control of the Russian segment of Internet«, in: 2018 International Con-

ference on Military Communications and Information Systems (ICMCIS), https://doi.org/10.1109/ICMCIS. 2018.8398700.

Kukkola, Juha (2018b): »Russian Cyber Power and Structural Asymmetry«, in: Jim Q. Chen/John S. Hurley (Hg.), Proceedings of the 13th International Conference on Cyber Warfare and Security (ICCWS 2018), S. 362–368.

Kukkola, Juha/Ristolainen, Mari (2018): »Projected territoriality: A case study of the infrastructure of Russian digital borders«, in: Journal of Information Warfare 17 (2), S. 83–100.

Lams, Lutgard (2018): »Examining strategic narratives in Chinese official discourse under Xi Jinping«, in: Journal of Chinese Political Science 23 (3), S. 387–411, https://doi.org/10.1007/s11366-018-9529-8.

Leberknight, Christopher S./Chiang, Mung/Poor, Harold V./Wong, Felix (2010): A taxonomy of internet censorship and anti-censorship. Princeton University vom 31.10.2010. Online unter: https://www.princeton.edu/~chiangm/anticensorship.pdf, abgerufen am 23.06.2022.

Linder, Courtney (2021): The NSA wants big tech to build software »back doors«. Should we be worried? Popular Mechanics vom 21.06.2021. Online unter: https://www.popularmechanics.com/technology/security/a34533340/nsa-tech-back-doors-software/, abgerufen am 23.06.2022.

Livshitz, Irina/Neklyudov, Aleksey V./Lontsikh, Pavel A. (2018): »Evaluation of IT security – genesis and its state-of-art«, in: Journal of Physics: Conference Series 1015 (4), https://doi.org/10.1088/1742-6596/1015/4/042029.

Lonkila, Markku/Shpakovskaya, Larisa/Torchinsky, Philip (2019): »The occupation of Runet? The tightening state regulation of the Russian-language section of the internet«, in: Mariëlle Wijermars/Katja Lehtisaari (Hg.), Freedom of expression in Russia's new mediasphere, London/New York: Routledge, S. 17–38.

Markl, Volker (2019): »Eine nationale Daten- und Analyseinfrastruktur als Grundlage digitaler Souveränität«, in: Informatik-Spektrum 41 (6), S. 433–439, https://doi.org/10.1007/s00287-018-01136-z.

Mau, Steffen (2021): Sortiermaschinen. Die Neuerfindung der Grenze im 21. Jahrhundert, München: C.H. Beck.

Misterek, Fokko (2017): »Digitale Souveränität. Technikutopien und Gestaltungsansprüche demokratischer Politik« in: MPlfG Discussion Paper 17 (11). Online unter: https://pure.mpg.de/pubman/faces/ViewItemOverviewPage.jsp?itemId=item_2452828, abgerufen am 23.06.2022.

Moher, David/Liberati, Alessandro/Tetzlaff, Jennifer/Altman, Douglas G. (2009): »Preferred reporting items for systematic reviews and meta-analy-

ses: The PRISMA statement«, in: BMJ 339, b2535, https://doi.org/10.1136/bmj.b2535.

Möllers, Norma (2020): »Making digital territory: Cybersecurity, techno-nationalism, and the moral boundaries of the state«, in: Science, Technology, & Human Values 46 (1), S. 112–138, https://doi.org/10.1177/0162243920904436.

Müller, Jane/Thumel, Mareike/Potzel, Katrin/Kammerl, Rudolf (2020): »Digital sovereignty of adolescents«, in: MedienJournal 44 (1), S. 30–40, https://doi.org/10.24989/medienjournal.v44i1.1926.

Murdoch, Steven J./Anderson, Ross (2008): »Tools and technology of internet filtering«, in: Ronald Deibert/John Palfrey/Rafael Rohozinski/Jonathan Zittrain (Hg.), Access denied. The practice and policy of global internet filtering, Cambridge: The MIT Press, S. 57–72.

Nation World News Desk (2021): »Russia uses coercion and black boxes to erect a digital Iron Curtain«, in: Nation World News vom 25.10.2021. Online unter: https://nationworldnews.com/russia-uses-coercion-and-black-boxes-to-erect-a-digital-iron-curtain/, abgerufen am 23.06.2022.

Nguyen-Thu, Giang (2018): »Vietnamese media going social: Connectivism, collectivism, and conservatism«, in: The Journal of Asian Studies 77 (4), S. 895–908, https://doi.org/10.1017/s0021911818002504.

Nicholson, Michael (1998): International relations. A concise introduction, London: Palgrave.

Nikkarila, Juha-Pekka/Ristolainen, Mari (2017): »›RuNet 2020‹ – deploying traditional elements of combat power in cyberspace?« in: IEEE, 2017 International Conference on Military Communications and Information Systems (ICMCIS), S. 1–8, https://doi.org/10.1109/ICMCIS. 2017.7956478.

Nocetti, Julien (2016): »The hacked world order: How nations fight, trade, maneuver, and manipulate in the digital age. By Adam Segal. Internet wars: The struggle for power in the 21st century. By Fergus Hanson«, in: International Affairs 92 (5), S. 1263–1266, doi.org/10.1111/1468-2346.12717.

O'Driscoll, Aimee (2020): List of websites and apps blocked in Russia. Comparitech vom 07.11.2020. Online unter: https://www.comparitech.com/blog/vpn-privacy/websites-blocked-russia/, abgerufen am 23.06.2022.

Perunicic, Kristina (2021): »The complete list of blocked websites in China & how to access them«, in: VPNMentor vom 19.10.2021. Online unter: https://www.vpnmentor.com/blog/the-complete-list-of-blocked-websites-in-china-how-to-access-them/, abgerufen am 23.06.2022.

Philpott, Daniel (2003): »Sovereignty«, in: Edward N. Zalta (Hg.), The Stanford Encyclopedia of Philosophy. Online unter: https://plato.stanford.edu/entries/sovereignty/, abgerufen am 23.06.2022.

Pierri, Paola/Herlo, Bianca (2021): »Exploring digital sovereignty: Open questions for design in digital healthcare«, in: Design for Health 5 (1), S. 161–175, https://doi.org/10.1080/24735132.2021.1928381.

Pohle, Julia (2020): »Digitale Souveränität«, in: Tanja Klenk/Frank Nullmeier/Göttrik Wewer (Hg.), Handbuch Digitalisierung in Staat und Verwaltung, Wiesbaden: Springer VS, S. 1–13.

Pohle, Julia (2021): »Digitale Souveränität. Das Ringen um Handlungs- und Entscheidungsfreiheit im Netz«, in: WZB-Mitteilungen 171, S. 6–8.

Pohle, Julia/Thiel, Thorsten (2020): »Digital sovereignty«, in: Internet Policy Review 9 (4), https://doi.org/10.14763/2020.4.1532.

Pohle, Julia/Thiel, Thorsten (2021): »Digital sovereignty«, in: Bianca Herlo/Daniel Irrgang/Gesche Joost/Andreas Unteidig (Hg.), Praciticing Sovereignty. Digital Involvement in Times of Crises, Bielefeld: transcript, S. 47–67.

Reckwitz, Andreas (2017): Die Gesellschaft der Singularitäten. Zum Strukturwandel der Moderne, Berlin: Suhrkamp.

Renz, André/Hilbig, Romy (2020): »Prerequisites for artificial intelligence in further education: Identification of drivers, barriers, and business models of educational technology companies«, in: International Journal of Educational Technology in Higher Education 17 (1), https://doi.org/10.1186/s41239-020-00193-3.

Ristolainen, Mari (2017): »Should ›RuNet 2020‹ be taken seriously? Contradictory views about cyber security between Russia and the West«, in: Journal of Information Warfare 16 (4), S. 113–131.

Roberts, Margaret E. (2014): Fear, friction, and flooding: Methods of online information control, Harvard University, Cambridge. Online unter: https://dash.harvard.edu/handle/1/12274299, abgerufen am 23.06.2022.

Roberts, Margaret E. (2018): Distraction and diversion. Inside China's great firewall, Princeton: Princeton University Press.

Rottwilm, Christoph (2016): »Chinas erfolgreiche Klone von Facebook, Google und Co.«, in: Manager Magazin vom 26.05.2016. Online unter: https://www.manager-magazin.de/unternehmen/artikel/zensur-in-china-die-erfolgreichen-klone-von-facebook-google-und-co-a-1094124.html, abgerufen am 23.06.2022.

Ruan, Lotus/Knockel, Jeffrey/Crete-Nishihata, Masashi (2020): »Information control by public punishment: The logic of signalling repression in China«, in: China Information 35 (2), S. 133–157, https://doi.org/10.1177/0920203x20963010.

Sargsyan, Tatevik (2016): »Data localization and the role of infrastructure for surveillance, privacy, and security«, in: International Journal of Communication 10, S. 2221–22237.

Savelyev, Alexander (2016): »Russia's new personal data localization regulations: A step forward or a self-imposed sanction?«, in: Computer Law & Security Review 32 (1), S. 128–145, https://doi.org/10.1016/j.clsr.2015.12.003.

Schneider, Ingrid (2020): »Democratic governance of digital platforms and artificial intelligence?«, in: JeDEM – eJournal of eDemocracy and Open Government 12 (1), S. 1–24, https://doi.org/10.29379/jedem.v12i1.604.

Schünemann, Wolf/Kneuer, Marianne (2021): Do not disturb! Studying discourses of democratic sovereignty as potential drivers of internet fragmentation through online control. Paper presented at the ISA Annual Convention 2021. Online unter: https://www.researchgate.net/publication/353351837_Do_not_disturb_Studying_discourses_of_democratic_sovereignty_as_potential_drivers_of_Internet_fragmentation_through_online_control, abgerufen am 23.06.2022.

Shaffer, Gregory C./Pollack, Mark A. (2010): »Hard vs. soft law: Alternatives, complements, and antagonists in international governance«, in: Minnesota Law Review 94, S. 706–799. Online unter: https://www.minnesotalawreview.org/wp-content/uploads/2011/08/ShafferPollack_MLR.pdf abgerufen am 23.06.2022.

Sharma, Sanjay (Hg.) (2020): Data Privacy and GDPR Handbook, Hoboken: Wiley.

Singer, Peter W./Friedman, Allan (2014): Cybersecurity and cyberwar. What everyone needs to know, Oxford: Oxford University Press.

Stadnik, Ilona (2019): Sovereign RUnet: What does it mean? Internet Governance Project vom 12.02.2019. Online unter: https://www.internetgovernance.org/research/sovereign-runet-what-does-it-mean/, abgerufen am 23.06.2022.

Stalder, Felix (2015): Kultur der Digitalität, Berlin: Suhrkamp.

Stewart, Michelle (2017): »Of digital selves and digital sovereignty: Of the North«, in: Film Quarterly 70 (4), S. 23–38, https://doi.org/10.1525/fq.2017.70.4.23.

Strech, Daniel/Sofaer, Neema (2012): »How to write a systematic review of reasons«, in: Journal of Medical Ethics 38 (2), S. 121–126, https://doi.org/10.1136/medethics-2011-100096.

Ternès von Hattburg, Anabel (Hg.) (2020): Digitalisierung als Chancengeber. Wie KI, 3D-Druck, Virtual Reality und Co. neue berufliche Perspektiven eröffnen, Wiesbaden: Springer Gabler.

Tretter, Max (2021): »Perspectives on digital twins and the (im)possibilities of control«, in: Journal of Medical Ethics 47 (6), S. 410–411, https://doi.org/10.1136/medethics-2021-107460.

Véliz, Carissa (2020): Privacy is power. Why and how you should take back control of your data, London: Bantam.

Vladimir, Ukolov/Vitaly, Cherkasov (2019): »Development of digital economy regulatory environment in supply chain operations«, in: International Journal of Supply Chain Management 8 (6), S. 555–559.

Zuboff, Shoshana (2018): Das Zeitalter des Überwachungskapitalismus, Frankfurt a.M./New York: Campus.

»*Demokratische* digitale Souveränität«
Plädoyer für einen normativen Begriff am Beispiel des digitalen Wahlkampfs

Eva Odzuck

Abstract *Der Artikel plädiert am Beispiel des digitalen Wahlkampfs dafür, den Begriff der »digitalen Souveränität« in liberalen Demokratien stärker als einen normativen Begriff auszubuchstabieren und ihn damit für die Beurteilung und Gestaltung der Demokratie unter digitalen Bedingungen fruchtbar zu machen. Der Artikel ist folgendermaßen gegliedert: In einem ersten Schritt skizziert er Herkunft, Dimensionen und gegenwärtige Verwendungsweisen des Souveränitätsbegriffs (s. Abschnitt 1.). In einem zweiten Schritt wird die Praxis des digitalen Wahlkampfs vorgestellt, in der Parteien danach streben, politische Gestaltungsmacht durch digitale Tools (insb. Microtargeting) zu erlangen und auszubauen (s. Abschnitt 2.). In einem dritten Schritt wird die deliberative Demokratietheorie von John Rawls als mögliche Grundlage eines normativen Begriffs »demokratischer digitaler Souveränität« entfaltet (s. Abschnitt 3.): Hierzu wird zunächst Rawls' Konzept der deliberativen Demokratie und sein demokratiepolitisches Prinzip des »öffentlichen Vernunftgebrauchs« und der »Pflicht zur Bürgerlichkeit« skizziert (s. Abschnitt 3.1). Anschließend wird aufgezeigt, dass nach Rawls auch Parteien im digitalen Wahlkampf einer »Pflicht zur Bürgerlichkeit« unterliegen. (s. Abschnitt 3.2) Im dritten Schritt wird überlegt, was diese Verpflichtung zur »Bürgerlichkeit« für Parteien im digitalen Wahlkampf konkret beinhalten könnte, d.h. wie sich das Prinzip der »demokratischen digitalen Souveränität« für Parteien im digitalen Wahlkampf ausbuchstabieren lässt (s. Abschnitt 3.3). In einem letzten Schritt wird das Ergebnis zusammengefasst und auf einer allgemeinen Ebene dafür plädiert, normative, demokratietheoretische Perspektiven in die Digitalisierungsdebatte einzuspeisen, weil liberale Demokratien für die angemessene Beurteilung und demokratiepolitisch verantwortliche Gestaltung der Digitalisierung auf ein entsprechendes normatives Vokabular angewiesen sind (s. Abschnitt 4.).*

1. Zum Begriff »digitale Souveränität«: Herkunft, Dimensionen, gegenwärtige Verwendung

»Souveränität« ist ein Begriff aus der neuzeitlichen Staatstheorie. Ursprünglich dem theologischen Kontext entstammend, in dem Gott als allmächtige Quelle des Rechts begriffen wurde, ist auch für die neuzeitliche Staatstheorie die Verknüpfung von Machtdimension und Rechtsdimension konstitutiv: In einem Zeitalter, in dem weltliche und geistliche Macht sich zunehmend voneinander lösen und verschiedene Akteur*innen politische Gestaltungsmacht beanspruchen, geht es darum, politische Gestaltungsmacht als *rechtmäßige Macht* zu legitimieren.

Exemplarisch lässt sich diese Verknüpfung von Machtdimension und Rechtsdimension in der neuzeitlichen Staatstheorie am Beispiel von Thomas Hobbes' Souveränitätsbegriff beobachten. Hobbes schreibt im Zeitalter von (auch religiös motivierten) Bürgerkriegen und widmet sein politiktheoretisches Werk der Aufgabe, einen weltlichen Souverän mit umfassenden Machtbefugnissen als Ermöglichungsbedingung des Friedens zu plausibilisieren. Hobbes' Ruhm bzw. sein schlechter Ruf (der in dem Namen »Monster von Malmesbury« zum Ausdruck kommt) rührt u.a. daher, dass er die Machtbefugnis von Souveränen kaum einschränkt. Doch Hobbes' Souveränitätsbegriff zeichnet sich trotz seiner Fixierung auf eine umfassende Machtfülle der Souveränität auch durch legitimationstheoretische Kontexte und naturrechtliche Elemente aus, die Grundlagen und Grenzen der legitimer souveräner Macht ausbuchstabieren.

Grundsätzlich entwickelt Hobbes' Staatstheorie die bereits seit der Antike bestehende Figur des Gesellschaftsvertrages wirkungsmächtig weiter: Hobbes benutzt das Bild eines freiwillig eingegangenen Vertrages, um für die Rechtmäßigkeit des Staates zu argumentieren: Wenn man sich vorstellen und plausibel machen kann, dass der Staat das Ergebnis eines freiwillig eingegangenen Vertrages sein könnte, kann der entsprechende Staat als rechtmäßig (weil auf fiktiver Zustimmung beruhend) und daher als legitim gelten. Die Grundidee ist die, dass Individuen sich wechselseitig verpflichten, sich einer Autorität mit umfassender politischer Gestaltungsmacht freiwillig zu unterwerfen, um dadurch dem blutigen Naturzustand und der ständigen Gefahr des Krieges und des gewaltsamen Todes zu entgehen. Das berühmte Frontispiz des *Leviathan* zeigt, wie der Hobbes'sche Souverän legitimationstheoretisch aus vielen einzelnen Individuen, die alle ihre Zustimmung gegeben haben, aufgebaut ist. Nach Hobbes' Definition ist der Staat »eine Person […], bei der sich jeder ein-

zelne einer großen Menge durch gegenseitigen Vertrag eines jeden mit jedem zum Autor ihrer Handlungen gemacht hat, zu dem Zweck, daß sie die Stärke und Hilfsmittel aller so, wie sie es für zweckmäßig hält, für den Frieden […] einsetzt. Wer diese Person verkörpert, wird Souverän genannt […].« (L, 17: 134f.)[1]

Ebenso wie Recht und Gesetz des Souveräns für ihre Umsetzung und Einhaltung auf Macht (bspw. Sanktionen bei Übertritt, Strafe etc.) angewiesen sind,[2] ist aber nach Hobbes auch die Macht grundsätzlich angewiesen auf Zustimmung und Anerkennung. Als *rechtmäßig*, weil auf (fiktiver, aber möglicher) *freiwilliger Zustimmung* beruhend, kann ein Staat nur dann begriffen werden, wenn er den Zielen und Zwecken, die die Individuen beim Vertragsschluss anstrebten, nicht zuwiderläuft. Verträge, die die eigene Selbsterhaltung gefährden oder dem Überleben abträglich sind, können nach Hobbes daher nicht als gültige, freiwillige Verträge begriffen werden – die Fiktion der freiwilligen Zustimmung zur Herrschaft lässt sich also dann nicht mehr aufrechterhalten, wenn die souveräne Macht das natürliche Recht der Individuen auf Überleben gefährdet.[3] Die Souveränität ist nach Hobbes »die [sterbliche, E.O.] Seele des Staates, von der die Glieder keinen Bewegungsantrieb empfangen können, wenn sie einmal den Körper verlassen hat« (L, 21: 171). Bei Befehlen, die der Selbsterhaltung zuwiderlaufen – wie beispielsweise beim Befehl, »auf Nahrung, Luft, Arznei oder andere lebensnotwendige Dinge zu verzichten, hat […] [der Untertan nach Hobbes, E.O.] die Freiheit, den Gehorsam zu verweigern« (L, 21: 168). Die Souveränität ist nach Hobbes also grundsätzlich sterblich bzw. verlierbar – wird der legitimatorische Kontext (in Hobbes' Fall: das natürliche Recht auf Selbsterhaltung als Grundlage möglicher freiwilliger Zustimmung) missachtet, stirbt die Souveränität. Trotz umfassender, absolut anmutender rechtlicher Befugnisse von Hobbes' Souverän: Als *legitime* Macht wird nur *der* Souverän anerkannt, der sich in den Schranken des legitimatorischen Kontextes, d.h. des freiwilligen, um der Selbsterhaltung willen eingegangenen Vertrages, bewegt.

---

1 Ich zitiere nach der bei Suhrkamp erschienenen Fetscher-Ausgabe (Euchner-Übersetzung) des Leviathan (Hobbes 1966), im Folgenden mit der Abkürzung »L« für *Leviathan* sowie unter Angabe der Kapitel- und Seitenzahl.

2 Vgl. die umfassenden Machtbefugnisse, die im 18. Kapitel des *Leviathan* aufgeführt werden.

3 Vgl. Odzuck 2014.

Auch wenn Hobbes ganz sicher kein uneingeschränkter Verfechter des Rechtsstaates und der Demokratie war, so transportiert sein Begriff sterblicher Souveränität dennoch Elemente, die für die weitere Entwicklung der liberalen Demokratie entscheidend werden sollten: die Idee der freiwilligen Zustimmung, die Idee der wechselseitigen Respektierung der Bürger*innen als frei und gleich und die Idee natürlicher Rechte, die gültigen freiwilligen Verträgen (und damit der Legitimitätskonstruktion insgesamt) Grenzen setzt – wird die naturrechtliche Ebene (bei Hobbes: das natürliche Recht auf Überleben) nicht beachtet, erlischt die Legitimitätsfiktion.

Für die demokratische Weiterentwicklung und konstitutionelle Verankerung des Souveränitätsbegriffs spielt diese doppelte Dimension von freiwilliger Zustimmung und naturrechtlichem Fundament eine zentrale Rolle: Für moderne, konstitutionelle, repräsentative Demokratien ist der Gedanke der Volkssouveränität – dass nämlich alle Macht vom Volke ausgeht und Repräsentant*innen diese Macht nur vertretungsweise ausüben – bestimmend. Zugleich geht man in republikanischen, deliberativen und in anspruchsvollen liberalen Theorien der Demokratie davon aus, dass der politische Wille des Volkes sich erst im gemeinsamen Austausch von Gründen in der Öffentlichkeit entwickelt und ausdifferenziert. Und das rechtsstaatliche Denken, was konstitutionellen Demokratien zugrunde liegt, geht davon aus, dass die Grenzen dessen, was ein Volk als Ergebnis der politischen Willensbildung legitimerweise wollen kann, durch die Verfassung (und deren naturrechtliche Elemente) vorgegeben sind.

Der kurze Exkurs in die politische Ideengeschichte zeigt, dass der staatstheoretische Begriff »Souveränität« von Anfang an Macht- und Rechtsdimensionen inkludierte. Auch wenn der Begriff verwendet wurde, um die politische Gestaltungsmacht sehr unterschiedlicher Akteur*innen und Entitäten zu rechtfertigen (bspw. souveräner Fürst vs. souveränes Volk), bleibt die Verschränkung von Macht- und Rechtsdimensionen und die Verbindung mit (auch naturrechtlich fundierten) Legitimitätskriterien zentral für den Begriff, wie er in der europäischen politischen Ideengeschichte entwickelt wurde.

Betrachtet man den gegenwärtigen Diskurs um »digitale Souveränität«, dann fallen einige Dinge auf: Erstens wird der Begriff »Souveränität« weitgehend aus dem staatstheoretischen Legitimationskontext herausgelöst, wenn beispielsweise von der Souveränität von Individuen, Firmen, Bibliotheksnutzer*innen oder Arbeitnehmer*innen gesprochen wird.[4] Zweitens wird der Be-

4 Vgl. dazu bspw. Sauer/Staples/Steinbach 2022 sowie Leyrer/Hagenhoff 2022.

griff im Kontext autoritärer Staaten offenbar mindestens ebenso gern benutzt wie im Kontext westlicher Demokratien – ohne dass im Einzelnen jeweils klar erkennbar wäre, wodurch sich die genutzten Begriffe unterscheiden lassen.[5] Diese zwei Tendenzen lassen sich durch einen dritten Befund ergänzen bzw. zum Teil erklären: Meist wird bei den zum Einsatz kommenden Begriffen von »digitaler Souveränität« eher auf die Machtdimension (»digitale Souveränität« als eine bestimmte Handlungsmacht bzw. Handlungsfähigkeit im Digitalen) rekurriert, während die rechtlichen und genuin legitimatorischen Dimensionen des Begriffs, die im staatstheoretischen Kontext entscheidend waren, oftmals außen vor bleiben.[6] Aus diesem diskurstheoretischen Befund lassen sich nun höchst unterschiedliche Schlüsse ziehen: Während einige Kommentator*innen angesichts der begrifflichen Vielfalt und der Popularität des Begriffs in autoritären Kontexten neuerdings den Schluss ziehen, den Begriff in demokratischen Kontexten vorsichtshalber zu verwerfen und sich stattdessen nach anderen Begriffen zur Kritik, Analyse und Gestaltung der digitalen Transformation umzusehen,[7] plädiere ich dafür, den Begriff ideengeschichtlich fundiert und demokratietheoretisch reflektiert für die Beurteilung und proaktive Gestaltung der digitalen Transformation liberaler Demokratien zu nutzen. Wie der Exkurs in die Ideengeschichte zeigt, weist der Begriff von Anfang an Machtdimensionen und Rechtsdimensionen auf, die für die Herausbildung der konstitutionellen Demokratie wichtig wurden und die es ermöglichen, die Konturen des Begriffs einer »demokratischen digitalen Souveränität« auszubuchstabieren. Eine zentrale Aufgabe für den gegenwärtigen Diskurs um »digitale Souveränität« dürfte daher darin bestehen, der machttheoretischen Reduktion des Begriffs entgegenzuarbeiten und ihn normativ und

5 Vgl. zu China bspw. Creemers 2020 und zu Russland bspw. Maréchal 2017 sowie für einen Diskursüberblick den Beitrag der Politischen Geographie (Dammann/Glasze 2022) und der theologischen Ethik (Tretter 2022) in diesem Band.

6 Deutlich wird dies bspw. an der Rede von Plattformunternehmen als »Quasi-Souveränen« (vgl. Pohle/Thiel 2021: 327) oder wenn in Bezug auf die US-amerikanische und chinesische Einflusssphäre die Notwendigkeit einer europäischen »digitalen Souveränität« eingefordert wird. Vgl. zur kaum adressierten Legitimitätsproblematik auch Floridi (2020: 375).

7 Vgl. Thiel (2020: 72): »Die gegenwärtige Wiederbelebung des Souveränitätsbegriffs ist so falsch wie unnötig: Sie versucht etwas zu reanimieren, was längst überwunden sein sollte.« Vgl. ebenso auch Pohle/Thiel (2021: 340) sowie die (dort ebenfalls zitierte) These Herzogs, es sei Zeit, das Konzept der Souveränität zu beerdigen – die im provokant gewählten Buchtitel *Sovereignty, RIP* zum Ausdruck kommt (vgl. Herzog 2020).

demokratietheoretisch anzureichern: Ohne Zweifel erleiden Demokratien in der digitalen Transformation Souveränitätsverluste in Form eines Verlustes an Handlungsmacht. Sie sehen sich im Zeitalter von Tech-Giganten und Plattformökonomie neuen mächtigen Akteuren und neuartigen Machtkonstellationen gegenüber und müssen angesichts autoritärer Staaten, die aktiv eine Zersetzungspolitik der liberalen Demokratie betreiben, immer auch die Perspektive nationaler Handlungs- und Gestaltungsmacht einnehmen. Die Renaissance des Souveränitätsbegriffs ist insofern kein problematischer Abwehrreflex (vgl. Thiel 2020: 72), sondern eine nicht nur verständliche, sondern auch notwendige Perspektive liberaler Demokratien, die die wertvolle Freiheit, die in demokratischen Verfassungsstaaten möglich ist, schützen und aufrechterhalten wollen. Für liberale Demokratien ist jedoch ein ganz bestimmter Umgang mit politischer Gestaltungsmacht (und deren Erwerb) gefordert, der den Legitimationsprinzipien der konstitutionellen Demokratie genügen muss. Eine angemessene Gefährdungsdiagnose und Ansätze für die Stärkung der Demokratie unter digitalen Bedingungen lassen sich daher nur mit einem Souveränitätsbegriff gewinnen, der die Rechtsdimension des Begriffs stark macht und dessen demokratie- und legitimationstheoretische Dimension ausbuchstabiert. Wie eine solche demokratietheoretische Rückbindung und Explikation eines normativ erweiterten Souveränitätsbegriffs aussehen könnte, soll in diesem Aufsatz exemplarisch am Beispiel des digitalen Wahlkampfs und des für liberale Demokratien konstitutiven Akteurs der politischen Partei gezeigt werden. Als zentrale Akteure der öffentlichen politischen Willensbildung haben sich in liberalen, repräsentativen Demokratien die Parteien herausgebildet, die der Öffentlichkeit nicht nur Kandidat*innen für öffentliche Ämter präsentieren, sondern (im Idealfall) auch Gründe für die Vorzugswürdigkeit einer bestimmten politischen Position in den öffentlichen Diskurs einbringen und damit zur informierten, argumentativ abgewogenen und ausdifferenzierten öffentlichen politischen Willensbildung des als Souverän begriffenen Volkes beitragen.[8]

8 Zum Spannungsfeld parteilicher Kommunikation zwischen der verfassungsrechtlich festgelegten Aufgabe der »Mitwirkung an der politischen Willensbildung des Volkes« und dem legitimen Streben nach politischer Gestaltungsmacht vgl. Potthast 2021.

2. Die Praxis des digitalen Wahlkampfs: Erwerb politischer Gestaltungsmacht durch digitale Werkzeuge?[9]

Wie viele andere Wahlkampftechniken auch, wurde das digitale politische Microtargeting zunächst im Rahmen der Werbeindustrie entwickelt (vgl. Chester/Montgomery 2017). Es handelt sich hierbei grundsätzlich um ein Geschäftsmodell personalisierter Werbung, welches auf kontinuierlichen und umfassenden Datensammlungen, auf der Nachverfolgung individueller Online-Verhaltensmuster und auf der psychometrischen Auswertung dieser Daten beruht (vgl. Kosinski/Stilwell/Graepel 2013). Übertragen auf politische Wahlkampagnen, lässt sich das Phänomen des digitalen politischen Microtargeting als eine Kombination aus datengestützter Wähler*innenanalyse und aus personalisierter digitaler politischer Werbung beschreiben.[10] Parteien versprechen sich vom Einsatz des Instruments typischerweise folgende Ziele: Zum einen sollen mit dem Instrument diejenigen Wähler*innen, die für bestimmte politische Werbebotschaften am empfänglichsten sind, identifiziert werden – diese *Identifikationsfunktion* ist insbesondere in Zeiten abnehmender Stammwähler*innen ein verlockendes Versprechen. Zum anderen soll das Instrument die *Effektivität* der Ansprache des Elektorats steigern: Durch Zuschnitt der digitalen Werbebotschaften auf die spezifischen sozialen Kontexte, Interessen, Vulnerabilitäten (ggf. auch vulnerable Zeitpunkte) und weitere individuelle Merkmale, d.h. durch Personalisierung, soll es möglich sein, die Werbung effektiver zu gestalten: So kann z.B. an unentschlossene, aber potenzielle Wähler*innen der eigenen Partei Werbung gesendet werden, um diese davon zu überzeugen, dass die Partei ein attraktives Programm für die durch Datenauswertung bekannten/vermuteten politischen Überzeugungen und Policy-Präferenzen des potenziellen Wählers bzw. der potenziellen Wählerin hat (oder um sich als Single-Issue-Partei entsprechend der vermuteten stärksten Präferenz zu präsentieren). Umgekehrt kann ein Ziel darin bestehen, Wähler*innen, die mit großer Sicherheit eine andere Partei wählen, durch Negativinformationen über die Konkurrenzpartei zu demobilisieren und von einer Wahlteilnahme abzuhalten.

---

9 Die nachfolgende Beschreibung der Genese, Praxis und Einsatzmöglichkeiten des digitalen politischen Microtargeting entspricht weitgehend dem Kapitel eines Aufsatzes, den ich in der Zeitschrift für Politik (Odzuck 2020) veröffentlicht habe.

10 Vgl. für eine hilfreiche Analyse Zuiderveen Borgesius et al. (2018: 82–84).

Das Phänomen wurde zunächst von US-amerikanischen Parteien benutzt, tritt aber zunehmend im europäischen Raum auf (vgl. Bennett 2016: 262–264). Verschiedene Firmen bieten in den USA Parteien an, Wähler mit Anzeigen auf Facebook, LinkedIn und an weiteren Stellen im Netz zu versorgen. So beanspruchte beispielsweise Cambridge Analytica, bis zu 5.000 Datenpunkte über 230 Millionen US-amerikanische Wähler gesammelt zu haben, und versucht laut eigenen Angaben, Persönlichkeitsaspekte zu identifizieren, die Rückschlüsse darauf zulassen, welche Art von Nachricht am überzeugendsten für die entsprechende Person wäre. Eine weitere Firma gibt ein Beispiel für eine Zielgruppe an: Väter im Alter von 35 bis 44 Jahren in Texas, die Waffenliebhaber-Internetseiten besuchen.[11] Neue Forschungen zum Einfluss von Social-Media-Firmen legen nahe, diese stärker als bisher als aktive Teilnehmer des politischen Prozesses zu betrachten und zu analysieren (vgl. Kreiss/McGregor 2018).

Im Vergleich zu den USA ist Microtargeting in Europa und Deutschland weniger verbreitet, was mit verschiedenen strukturellen Voraussetzungen, etwa anderen Datenschutzbestimmungen, der anderen Parteienfinanzierung, einem anderen Parteien- und Wahlsystem, aber auch mit einer anderen politischen Kultur erklärt werden kann. Der vergleichende Blick, der strukturelle Unterschiede ernst nimmt, muss jedoch nicht notwendigerweise zu einer Relativierung des Phänomens für den europäischen Raum führen. Obwohl die Schlussfolgerung verlockend ist, dass Microtargeting ein Phänomen der US-amerikanischen Politik und Gesellschaft ist, das dem liberalen Wahlfinanzierungssystem, dem traditionell umfassenden Schutz politischer Rede, dem Zwei-Parteien-System, der starken Industrie des politischen Consulting, Tech-Firmen, die in einem höchst kompetitiven elektoralen Umfeld ihre Vorhersagemodelle und Algorithmen aggressiv bewerben, sowie vergleichsweise schwachen und fragmentierten Datenschutzgesetzen zuzuordnen sei, sollte man – wie Bennett (2016) überzeugend argumentiert – vorsichtig sein mit dieser Schussfolgerung. Auch die These, dass Europa mit stärkeren Datenschutzregelungen und der Negativerfahrung mit autoritärer Herrschaft vor diesem Phänomen ausreichend geschützt sei, hält Bennett für voreilig (vgl. Bennett 2016: 274). Das Phänomen »Politisches Microtargeting« (PMT) entstand in einer Zeit, in der traditionelle Parteibindungen nachgelassen

11 Siehe Zuiderveen Borgesius et al. (2018: 83) mit weiteren Belegen zu diesem und dem zuletzt genannten Cambridge-Analytica-Beispiel.

haben und die Zahl unentschiedener Wähler*innen, die naturgemäß empfänglicher für Marketingmaßnahmen sind, angestiegen ist. Diese gestiegene Zahl der Unentschlossenen und daher potenziell Beeinflussbaren mache Methoden der Beeinflussung, wie es das PMT sei, zu einem verlockenden Instrument auch für europäische Parteien. Insofern lässt sich, wie Bennett argumentiert, die Perspektive umdrehen und erwarten, dass der Druck auf die europäischen Datenschutzgesetze größer werden wird (vgl. ebd.). Der Blick der europäischen Parteien richtet sich westwärts auf die Erfahrungen der US-amerikanischen Parteien mit den neuen digitalen Wahlkampfmitteln und verbindet sich mit Hoffnungen auf deren Potenzial (vgl. Bennett 2013). Publikationen mit vielversprechenden Titeln wie *The victory lab. The secret science of winning campaigns* (Issenberg 2012) oder *Hacking the electorate: How campaigns perceive voters* (Hersh 2015) sowie aggressive Marketingtechniken der Anbieter digitaler Dienstleistungen tun das Ihrige, diese Hoffnungen zu befeuern. Als Möglichkeit, politische Gestaltungsmacht auszuüben, werden digitale Tools nicht nur von Parteien in westlichen Demokratien benutzt,[12] sondern auch von autoritären Regimen, die der westlichen Demokratie insgesamt schaden wollen. Prominent diskutiert wurden in diesem Zusammenhang beispielsweise der Versuch Russlands, die US-Wahlen 2016 zu manipulieren (vgl. Zeit Online 2018), bzw. Versuche des Iran und Russlands, auf die US-Wahl 2020 einzuwirken (Tagesschau 2021). Die globale Verfügbarkeit nationalstaatlich relevanter geopolitischer Daten über die Wahlberechtigten stellt die Souveränität westlicher Demokratien vor neue, immense Gefährdungen von außen, weil sich autoritäre Regime dieser Daten bemächtigen und sie für ihre Zwecke der Manipulation von Wahlen und Destabilisierung von Demokratien nutzen können. Ein Problem entsteht jedoch auch, wenn sich Akteure innerhalb liberaler Demokratien dieses Instruments bemächtigen: Wie argumentiert werden soll, sind stabile konstitutionelle Demokratien auf eine politische Kultur angewiesen, die politische Gestaltungsoptionen in Form von freiheitsbeschränkenden Gesetzen anspruchsvoll öffentlich diskutiert und begründet. Parteien tragen als Akteure mit besonderer Einflussstärke auf den öffentlichen Diskurs daher eine besondere Verantwortung für die Gestaltung und Aufrechterhaltung der demokratischen politischen Kultur – und der Begriff einer »demokratischen digitalen Souveränität« kann unseres Erachtens fruchtbar herangezogen werden, um die Konturen dieser Verantwortung und notwendigen demokratiepolitischen Gestaltungsaufgabe zu umreißen.

12 Für einen Überblick zur Situation in Deutschland vgl. Papakyriakopoulos et al. 2017.

3. Die Verantwortung der Parteien im digitalen Wahlkampf: »*demokratische* digitale Souveränität«

Wir haben im vorangegangenen Abschnitt gesehen, dass Parteien im digitalen Wahlkampf digitale Techniken und Plattformangebote nutzen, um ihr Ziel des Erwerbs politischer Gestaltungsmacht zu erreichen. Techniken wie das Microtargeting werden benutzt, um das Elektorat zu analysieren, zu segmentieren und zielgerichtet zu adressieren – und so das eigene Wahlergebnis zu optimieren und die durch die Stimmen gewährte Macht auszubauen. Parteien nehmen das Angebot der Plattformen (und weiterer Akteure des digitalen Wahlkampfs), digitale Handlungsmacht zu erlangen und auszubauen, also gerne an. In diesem Abschnitt[13] soll nun der Blick auf die deliberative Demokratietheorie von John Rawls gerichtet werden, um ausgehend davon einen normativ gehaltvolleren Begriff »demokratischer digitaler Souveränität« für Parteien im digitalen Wahlkampf zu entwickeln: Nach Rawls können Demokratien nur dann stabil und legitim sein, wenn sie eine bestimmte politische Kultur des bürgerlichen Respekts entwickeln und kultivieren und sich in der öffentlichen Kommunikation über Gesetze (als freiheitsbeschränkende Maßnahmen des Staates) den Regeln des öffentlichen Vernunftgebrauchs unterwerfen (s. Abschnitt 3.1). Für Parteien, die durch den Wahlkampf politische Gestaltungsmacht erlangen und ihre Kandidaten in öffentliche Ämter bringen möchten, gelten diese Regeln, wie gezeigt werden soll, in besonderem Maße (s. Abschnitt 3.2). Hieraus lässt sich für Parteien im digitalen Wahlkampf ein normativer Begriff »*demokratischer* digitaler Souveränität« gewinnen: Neben ihrer eigenen Macht sollten Parteien in der öffentlichen Kommunikation immer auch die besonderen Anforderungen öffentlicher Begründungspraxis in der liberalen Demokratie und die Stabilität, Qualität und Legitimität der Demokratie im Blick behalten, um demokratiepolitisch souverän zu agieren (s. Abschnitt 3.3).

13 Abschnitt 3 stützt sich auf Vorarbeiten zur Anwendung von Rawls' Demokratietheorie auf digitales Microtargeting, die ich in der Zeitschrift für Politikwissenschaft veröffentlicht habe (vgl. Odzuck/Günther 2021). Die dortigen Ausführungen zu Rawls' Demokratietheorie wurden für den vorliegenden Text übersetzt, überarbeitet und mit Belegen aus den deutschen Übersetzungen von Rawls' Werken ergänzt.

3.1 Rawls' Konzept der deliberativen Demokratie: Demokratiepolitik, öffentlicher Vernunftgebrauch und die Pflicht zur Bürgerlichkeit

John Rawls' Demokratietheorie ist vor dem Hintergrund der blutigen konfessionellen Bürgerkriege des 17. Jahrhunderts zu sehen, die unbedingt vermieden werden sollen. Für Rawls sind zivilisierte, friedliche konstitutionelle Demokratien nicht selbstverständlich, sondern eine prekäre und von vielen Seiten gefährdete historische Errungenschaft. Für ihre Qualität, für ihre Stabilität und für ihre Legitimität werden nicht nur bestimmte Institutionen benötigt, sondern auch ein bestimmtes demokratischen Ethos, eine bestimmte Art und Weise des bürgerlichen öffentlichen Umgangs, ein bestimmter Modus der öffentlichen Rechtfertigung. Diese besondere Art und Weise der öffentlichen Rechtfertigung bezeichnet Rawls auch als »öffentlichen Vernunftgebrauch«. Was ist darunter zu verstehen? Grundsätzlich bezieht sich die Idee der öffentlichen Vernunft bei Rawls auf das Verhältnis zwischen Regierung und Bürger*innen sowie auf das Verhältnis zwischen Bürgerinnen und Bürgern (vgl. Rawls 2002: 167). Rawls geht davon aus, dass sich die Zwangsmacht des liberalen Staates und einzelner Gesetze vor allen Bürgerinnen und Bürgern, die als frei und gleich begriffen werden, zu rechtfertigen hat. Auch wenn Rawls den Souveränitätsbegriff selten explizit verwendet (vgl. Lister 2014), lässt sich seiner Demokratietheorie ein ganz bestimmter Begriff demokratischer Souveränität entnehmen. Als Volkssouveränität ist demokratische Souveränität nach Rawls[14] vor allem auf eine bestimmte Form der öffentlichen Rechtfertigung der Ausübung staatlicher Macht angewiesen, die sich an alle Bürger gleichermaßen richtet:

> »Während politische Macht – mit dem Regierungsmonopol der legalen Gewaltanwendung im Rücken – stets Zwang beinhaltet, ist sie im Rahmen eines demokratischen Staatswesens auch die Macht der Öffentlichkeit, d.h. die Macht der als Körperschaft aufgefaßten freien und gleichen Bürger. Doch wenn jeder Bürger den gleichen Anteil an der politischen Macht hat, dann sollte die politische Macht […] nach Möglichkeit so ausgeübt werden, daß alle Bürger dieses Vorgehen im Lichte ihrer eigenen Vernunft gutheißen können.« (Rawls 2003: 146f.)

14 Ein davon abweichendes Verständnis von Volkssouveränität skizzieren Ritzi/Zierold (2019: 38f.) im Anschluss an Habermas.

Diese Rechtfertigung soll sich an alle *Bürgerinnen und Bürger als freie und gleiche* richten – d.h., sie soll nicht auf partikularen Weltanschauungen oder religiösen Ansichten gegründet sein, sondern auf Gerechtigkeitsprinzipien, die von allen Bürger*innen als freie und gleiche Akteurinnen und Akteure geteilt werden können. Die Ausübung von Zwangsmacht ist nach Rawls also nur dann legitim, wenn sie mit Gründen gerechtfertigt werden kann, die von allen als freie und gleiche akzeptiert werden können (vgl. Rawls 2002: 172). Rawls schlägt insofern eine konstitutionell-demokratische Alternative zum Hobbes'schen uneingeschränkten Souverän vor, die Stabilität »aus den richtigen Gründen« möchte und im Rahmen einer konstitutionell eingehegten Demokratie auf bürgerliche Freundschaft und wechselseitiges Vertrauen zwischen Bürgerinnen und Bürgern setzt, die sich gegenseitig als freie und gleiche, politisch souveräne Bürger*innen anerkennen.[15]

Als Legitimitätsprinzip für die Zwangsmacht des Staates ist der öffentliche Vernunftgebrauch nach Rawls nicht für alle Fragen, die legislativ entschieden werden, anzuwenden, sondern vor allem dann, wenn Verfassungsgrundsätze und Fragen grundlegender Gerechtigkeit auf dem Spiel stehen (vgl. Rawls 2002: 167). Wichtig ist, dass die Verpflichtung zum öffentlichen Vernunftgebrauch nicht bedeutet, umfassende Weltanschauungen oder religiöse Argumente aus der Öffentlichkeit komplett auszuschließen. Rawls macht deutlich, dass Anhänger*innen von Religionen oder umfassender philosophischer Lehren selbstverständlich Argumente in die Öffentlichkeit einbringen dürfen, die auf Basis der jeweiligen umfassenden Lehre formuliert sind. Dies habe sogar den Vorteil, dass Bürger gegenseitig besser verstehen können, wo der jeweils andere steht (ebd.: 190f.). Es bestehe aber dann die Verpflichtung, zusätzlich und innerhalb eines gewissen Zeitrahmens Argumente zu entwickeln, die ohne Anleihen bei umfassenden Lehren auskommen und den Kriterien des öffentlichen Vernunftgebrauchs entsprechen – Rawls nennt dies die »Vorbehaltsregelung« (Rawls 2002: 191; vgl. auch Rawls 2003: 146). Rawls' Idee des öffentlichen Vernunftgebrauchs schränkt also die im öffentlichen Bereich zugelassenen Argumente nicht restriktiv ein, sondern lässt andere Argumente zu, solange immer auch innerhalb eines gewissen Zeitrahmens der Versuch unternommen wird, Argumente nachzuliefern, die dem öffentlichen Vernunftgebrauch entsprechen. Als Beispiele für Argumente, die ursprünglich oftmals religiös begründet wurden, aber tatsächlich durch Rückbezug

15 Zu Rawls' Souveränitätsbegriff und zu Hobbes als Kontrastmodell vgl. Lister (2014: 801).

auf die Grundwerte der Verfassung und politische Gerechtigkeitsprinzipien begründet werden können, nennt Rawls die Sklavenbefreiung und die US-amerikanische Bürgerrechtsbewegung (vgl. 2002: 191).

Um das Prinzip des »Öffentlichen Vernunftgebrauchs« adäquat zu verstehen, ist es notwendig, dieses auch als Prinzip der Qualität und Stabilität demokratischer konstitutioneller Regime zu begreifen: Denn um Qualität und Stabilität zu erreichen, sind demokratische Regime auf bestimmte Tugenden und ein bestimmtes demokratisches Ethos der Bürger angewiesen – und dieses wiederum hängt wesentlich von der Struktur und Qualität des öffentlichen Diskurses ab.

Rawls' Lamento über den horriblen Zustand der gegenwärtigen politischen Debatte liegt die These zugrunde, dass bürgerliche Tugenden im öffentlichen Diskurs erworben und eingeübt werden und deshalb besonders bedroht sind, wenn in öffentlichen Debatten bürgerliche Tugenden der Fairness, des Kompromisses und des wechselseitigen Respekts nicht mehr adäquat ausgedrückt werden. Die Tatsache, dass »ein großer Teil der politischen Auseinandersetzung […] Zeichen der Kriegsführung an den Tag [legt, E.O.]«, indem man »seine Truppen zusammentrommelt und die Gegenseite einschüchtert« (Rawls 2003: 185), ist also gerade deshalb ein Problem, weil dadurch der Erwerb und die Einübung der für ein demokratisches Gemeinwesen essenziellen kooperativen Tugenden gefährdet wird: Nach Rawls gehören »die kooperativen politischen Tugenden der Vernünftigkeit und des Sinns für Fairneß, der Kompromissbereitschaft und des Willens zur Respektierung des öffentlichen Anstands« zum »politischen Kapital der Gesellschaft« (ebd.: 185f.). Wie Kapital werden diese Tugenden nur sehr langsam aufgebaut, bergen die Gefahr, abgewertet zu werden, und müssen ständig erneuert werden, »indem man sie in der Gegenwart bestätigt und dem Handeln zugrunde legt« (ebd.: 186). Der Schutz dieses Kapitals der konstitutionellen Demokratie erfordert, in politischen Debatten, die zu freien Vereinbarungen führen sollen, Argumente zu benutzen und Gründe ins Feld zu führen, die auch von anderen akzeptiert werden können.

Als Qualitäts- und Stabilitätsprinzip formuliert, scheint die »Pflicht zur Bürgerlichkeit« also umfassender zu sein als das Legitimitätsprinzip, denn sie gilt nicht nur für »wesentliche Verfassungselemente«, sondern »auch in anderen Fällen, […] insofern diese an solche Verfassungselemente grenzen und politisch konfliktträchtig werden« (Rawls 2003: 184f., vgl. auch 147). Die öffentliche politische Kultur hat nach Rawls Auswirkungen auf den »politischen Charakter« der Bürger (ebd.: 186). Die Pflicht zur Bürgerlichkeit impliziert somit

eine Pflicht, »eine bestimmte Art von sozialer Welt zu schaffen« (ebd.) – eine Pflicht also, die konstitutionelle Demokratie im täglichen Reden und Handeln durch öffentlichen Vernunftgebrauch zu stützen. Rawls warnt davor, die Notwendigkeit einer ständigen Pflege der bürgerlichen Tugenden zu unterschätzen, die er als unabdingbare Voraussetzung für die Stabilität und Qualität aller bestehenden konstitutionellen Demokratien ansieht (Rawls 2002: 211f.).

Die Pflicht zur Bürgerlichkeit setzt dem *Inhalt* öffentlicher Reden keine harten Grenzen, sondern verlangt vielmehr die Anwendung eines bestimmten staatsbürgerlichen Modus, der dem Grundsatz der Reziprozität gehorcht und Ausdruck gegenseitigen Respekts ist. »Öffentliche Rechtfertigungen« sind nach Rawls daher »nicht einfach gültige Begründungen, sondern Argumente, die sich an andere wenden« (2002: 191). Richterinnen und Richter, der Gesetzgeber und generell alle Regierungsbeamtinnen und -beamte erfüllen ihre Pflicht zur Bürgerlichkeit, wenn sie »anderen Bürgern ihre Gründe dafür, warum sie bestimmte grundlegende politische Positionen unterstützen, in Begriffen einer politischen Gerechtigkeitskonzeption erklären« (ebd.: 169). Sie richten diese Gründe an andere Bürger *als Bürger*, d.h. an Bürger, die sich selbst als frei und gleich betrachten, und weder an Individuen, die umfassenden Doktrinen anhängen, noch an sozial situierte Individuen, die bestimmte gruppenbezogene Interessen vertreten. Rawls führt aus:

> »Wenn wir Gründe für alle Bürger vorbringen, betrachten wir sie nicht als sozial situierte oder auf andere Art verwurzelte Personen, das heißt nicht als Wesen in dieser oder jener sozialen Klasse oder in dieser oder jener Besitz- und Einkommensgruppe oder als Vertreter dieser oder jener umfassenden Lehre. Wir appellieren auch nicht an das Eigeninteresse jeder Person oder Gruppe, obwohl wir an einem bestimmten Punkt diese Interessen in Betracht ziehen müssen.« (Rawls 2002: 208)

Die Aufgabe des Kriteriums der Reziprozität, das der öffentliche Gebrauch der Vernunft zum Ausdruck bringt, besteht insgesamt darin, »das Wesen der politischen Beziehungen in einer konstitutionellen demokratischen Ordnung als eines der bürgerlichen Freundschaft zu bestimmen« (ebd.: 172).

Ausgehend von diesen Überlegungen können wir Rawls' Idee der »öffentlichen Vernunft« als ein Prinzip der Legitimität und ein Prinzip, das zur Qualität und Stabilität konstitutioneller Demokratien beiträgt, zusammenfassen. Die Pflicht zur Bürgerlichkeit ist eine moralische, keine rechtliche Pflicht: Wenn Bürger öffentlich sprechen, sollten sie ihre Position mit Argumenten begründen, denen andere Menschen als freie und gleiche Bürgerinnen und Bürger zu-

stimmen könnten. Sie sollten eine Sprache und einen Modus der Argumentation wählen, der Respekt vor freien und gleichen Bürgerinnen und Bürgern zum Ausdruck bringt und so dazu beiträgt, dass die politischen Beziehungen in der konstitutionellen Demokratie als Beziehungen bürgerlicher Freundschaft begriffen werden können.

3.2 Politische Parteien in Rawls' Konzept deliberativer Demokratie und die Pflicht der Parteien zur »Bürgerlichkeit«

Rawls trennt zwischen einer sogenannten Hintergrundkultur, zu der beispielsweise Kirchen und Universitäten gehören, und der öffentlichen politischen Kultur bzw. dem öffentlichen Forum im eigentlichen Sinne. Er macht deutlich, dass die Pflicht zur Bürgerlichkeit und die hiermit verbundene freiwillige Einschränkung in Bezug auf den gewählten Argumentationsmodus nicht in der Hintergrundkultur gilt, sondern nur im öffentlichen politischen Forum (vgl. Rawls 2002: 167). Im öffentlichen politischen Forum gilt diese Pflicht zur Bürgerlichkeit prinzipiell aber für alle beteiligten Akteure. Auch wenn die moralische Pflicht in einem besonderen Maße für Verfassungsrichter gilt, die qua ihres Amtes auf eine sorgfältige, unparteiliche Begründung von Gesetzen verpflichtet sind, sind die Anforderungen an öffentliche Rechtfertigung immer dieselben und gelten prinzipiell für alle Akteure im öffentlichen Bereich. Idealerweise sollten sich daher Bürgerinnen und Bürger im politischen Forum so verstehen, als wären sie Gesetzgeber, die Gesetze durch Gründe rechtfertigen, denen alle Bürgerinnen und Bürger als Freie und Gleiche zustimmen könnten – und sollten Kandidatinnen und Kandidaten um öffentliche Ämter und Regierungsbeamtinnen und -beamte an dieser Pflicht messen und auswählen (vgl. ebd.: 170). Die moralische Pflicht zum öffentlichen Vernunftgebrauch bzw. zur Bürgerlichkeit sollte daher prinzipiell auch für wahlkämpfende Parteien im politischen Forum gelten, die sich im Bereich des Wahlkampfs klar im öffentlichen Forum bewegen. Rawls' Aufzählung von Akteuren, die der Pflicht zum öffentlichen Vernunftgebrauch unterworfen sind, ist nicht auf Richter*innen oder Regierungsbeamtinnen und -beamte beschränkt. In seiner letzten großen Veröffentlichung zum »öffentlichen Vernunftgebrauch« geht Rawls explizit auch auf Parteien im Wahlkampf ein und macht deutlich, dass diese ebenso eine Pflicht zur Bürgerlichkeit haben:

> »Innerhalb dieses Forums lassen sich drei Teile unterscheiden: der Diskurs von Richtern in ihren Urteilen und insbesondere von Verfassungsrichtern,

> der Diskurs der Regierungsbeamten und insbesondere der leitenden Personen und Gesetzgeber und schließlich der Diskurs der Kandidaten für öffentliche Ämter und derjenigen, die ihre Wahlkämpfe organisieren, insbesondere wenn es um öffentliche Ansprachen, Parteiprogramme und politische Stellungnahmen geht.« (Rawls 2002: 168)[16]

Während von diesen Ausführungen her bereits klar ist, dass für Rawls *auch* Parteien der Pflicht zur Bürgerlichkeit unterliegen, sind die Gründe dafür an dieser Stelle noch sehr allgemein. Es lässt sich aber argumentieren, dass Parteien nicht nur *ebenso* wie andere Akteure einer Pflicht zur Bürgerlichkeit unterliegen, sondern dass Parteien als besondere Akteure in Rawls' Konzeption der deliberativen Demokratie eine besondere Verantwortung und Vorbildfunktion für die öffentliche politische Kultur einnehmen. In den letzten 10 Jahren gab es in der Rawls-Forschung Arbeiten zu Parteien in dessen Demokratietheorie, die überzeugend argumentiert haben, dass Rawls' Arbeiten Elemente einer normativen Theorie der Partei als spezifischer deliberativer Akteur enthält (vgl. Muirhead/Rosenblum 2006 und Bonotti 2017).[17] Es ist nun gerade diese einzigartige Rolle der politischen Parteien in der öffentlichen Deliberation, aus der sich ihre besondere Verantwortung im Wahlkampf ergibt. Einer der Gründe für diese besondere Stellung ist das große öffentliche Interesse der Wahlbeteiligten, das die Wahlkampagnen der politischen Parteien in der Regel auf sich ziehen, wodurch sie die politische Willensbildung stärker beeinflussen können als andere Akteure. Wenn öffentliche Kommunikation immer den Status eines ermöglichenden Umfelds zur Herausbildung bürgerlicher Tugenden innehat, dann folgt daraus, dass Akteure mit substanziellem Einfluss auf die öffentliche Kommunikation auch eine besondere politische Verantwortung zu tragen haben; wenn die allgemeine Pflicht zur Bürgerlichkeit die Pflicht impliziert, zur Herausbildung einer demokratischen öffentlichen politischen Kultur beizutragen, dann gilt dies erst recht für Akteure, deren Rolle in diesem öffentlichen Forum ihnen eine spezifische Fähigkeit verleiht, »die soziale Welt zu gestalten«. Rawls' Forderung nach einer öffentlichen Finanzierung des Wahlkampfs politischer Parteien impliziert die Auffassung, dass Parteien im Wahl-

16 Rawls führt in einer zugehörigen Fußnote aus, dass er jeweils die Kandidatinnen und Kandidaten dafür verantwortlich macht, was in einer Wahlkampagne von offiziellen Repräsentantinnen und Repräsentanten der Partei oder Wahlkampfmanagerinnen und -managern getan wird (vgl. Rawls 2002: 168, n. 9)

17 Für eine kritische Diskussion aktueller Literatur zur normativen Theorie von Parteien vgl. Muirhead/Rosenblum 2020.

kampf zentrale Akteure im öffentlichen Gebrauch der Vernunft sind, zu dem sie nur dann einen angemessenen Beitrag leisten können, der frei vom verzerrenden Einfluss unternehmerischer und anderer organisierter Interessen ist, wenn sie so weit wie möglich »vom Fluch des Geldes befreit« werden (Rawls 2002: 174).

Ein zweiter Grund für eine besondere deliberative Verantwortung der politischen Parteien im Wahlkampf ist ihr Beitrag zu einem sogenannten »überlappenden Konsens«, der nach Rawls die Stabilität in vielfältigen Gesellschaften garantiert (s. Bonotti 2017: 3f.): Indem Parteien als »Lautsprecher« fungieren, die politische Agenda setzen und strukturieren sowie politische Programme vorantreiben, tragen sie zur Legitimation und zur Sicherung einer stabilen gemeinsamen Basis für öffentliche Deliberation in einem demokratischen Verfassungssystem bei. Diese Vorbild-, Legitimations- und Stabilisierungsfunktion der politischen Parteien ergibt sich aus ihrer einzigartigen Rolle, die, wie Muirhead und Rosenblum (2006: 104) argumentieren, in ihrer Vermittlung zwischen Gesellschaft und Staat, zwischen Hintergrundkultur und öffentlicher Kultur besteht. Als Vermittlungsinstitutionen müssen die politischen Parteien die Kunst der »zweisprachigen« Kommunikation beherrschen (ebd.): In ihrer repräsentativen und artikulatorischen Funktion müssen sie die Partikularinteressen und Standpunkte ihrer Mitglieder (und die nicht öffentlichen Gründe ihrer Wähler; Bonotti 2017: 5) ausreichend berücksichtigen. In Wahlkämpfen treten Parteien, genauer gesagt Parteimitglieder, aber zugleich als Kandidatinnen und Kandidaten für öffentliche Ämter auf und repräsentieren damit potenzielle Gesetzgeber. Parteien repräsentieren also – zumindest potenziell – den Staat, insofern sie Kandidatinnen und Kandidaten für öffentliche Ämter präsentieren, die sich in ihrer öffentlichen Argumentationsführung an alle Bürgerinnen und Bürger *als Bürger* wenden und daher dem Modus des öffentlichen Vernunftgebrauchs Rechnung tragen müssen. Im Wahlkampf und bei ihren Versuchen, ihre Kandidatinnen und Kandidaten in öffentliche Ämter zu bringen, tragen Parteimitglieder, wie Bonotti (2017: 67) es ausdrückt, eine »tragbare Öffentlichkeit« mit sich herum und unterliegen damit der Pflicht zur Bürgerlichkeit.

Als Vertreter des Pluralismus, von dem Rawls' politischer Liberalismus ausgeht, haben politische Parteien, die ihre Kandidatinnen und Kandidaten der Öffentlichkeit als künftige Inhaber*innen öffentlicher Ämter präsentieren, die staatsbürgerliche Pflicht, den Einsatz der öffentlichen Vernunft als angemessene Form der Moderation dieses Pluralismus zu vertreten. Diese Rolle und Verantwortung macht es für die politischen Parteien unabdingbar, die

Wählerinnen und Wähler nicht einfach als manipulierbare, apathische oder politisierbare Individuen anzusprechen. Im Wahlkampf und als (potenzielle) Repräsentantinnen und Repräsentanten des Staates und des Gemeinwohls sind die politischen Parteien und ihre Mitglieder auch Vorbilder für die öffentliche Argumentation und besitzen eine transformative Kraft für die Bildung der bürgerlichen Identität und der politischen Kultur einer Gesellschaft. Gerade angesichts des fragilen und gefährdeten Zustands der bürgerlichen Tugenden als »politisches Kapital« liegt es nahe, das öffentliche Reden und Handeln von Parteien und Kandidaten in Wahlkämpfen konsequent (wenn auch nicht unbedingt ausschließlich) in Bezug auf ihren möglichen Beitrag zu diesem politischen Kapital zu beurteilen. Für unsere Perspektive auf die demokratietheoretische Anreicherung des Begriffs der »digitalen Souveränität« bedeutet dies: Obwohl Parteien im Wahlkampf legitimer- und notwendigerweise nach politischer Gestaltungsmacht streben, sollte der Wunsch der Parteien nach »digitaler Souveränität« im Wahlkampf immer begleitet werden von einer selbstkritischen Reflexion hinsichtlich der besonderen demokratiepolitischen Verantwortung von Parteien. Eine »demokratische digitale Souveränität« würde den Parteien abverlangen, mit ihren Tweets und Ads nicht nur auf eine Maximierung der Stimmen abzuzielen, sondern sich der grundlegenden demokratiepolitischen Verantwortung im Wahlkampf bewusst zu sein. Wie Fukuyama herausarbeitete, tragen US-amerikanische und europäische Parteien und deren Entscheidung für eine bestimmte Art des identitätspolitischen Wahlkampfs eine Mitverantwortung an problematischen Auswüchsen fragmentierender und polarisierender Auswüchse der Identitätspolitik (vgl. Fukuyama 2019: 141f.). Im nächsten Abschnitt soll daher gefragt werden, wie eine solche »demokratische digitale Souveränität« für Parteien im Wahlkampf konkret aussehen könnte – und wie damit zwischen legitimen und illegitimen Modi des digitalen Wahlkampfs unterschieden werden könnte.

3.3 Demokratiepolitik durch Parteien, oder: Wie sieht eine »*demokratische* digitale Souveränität« im digitalen Wahlkampf aus?

Nachdem nun mit Rawls für die These argumentiert wurde, *dass* politische Parteien im Wahlkampf einer besonderen Verantwortung für den öffentlichen Vernunftgebrauch unterliegen, kann nun gefragt werden, welche Schlussfolgerungen sich hieraus für die Gestaltung und Bewertung digita-

ler Wahlkampagnen ziehen lassen – d.h., wie eine »demokratische digitale Souveränität« für Parteien im digitalen Wahlkampf aussehen könnte. Rawls' Pflicht zur Bürgerlichkeit beinhaltete zunächst grundsätzlich das Gebot, politische Positionen im öffentlichen Forum mit Argumenten zu begründen, die Wähler als freie und gleiche Bürger ansprechen, und das Prinzip der Reziprozität zu respektieren, welches es ermöglicht, politische Beziehungen als Beziehungen bürgerlicher Freundschaft zu begreifen.

Auf Basis dieser Rekonstruktion ließe sich zunächst vermuten, dass Techniken des digitalen politischen Microtargeting grundsätzlich gegen die »Pflicht zur Bürgerlichkeit« verstoßen, weil die typische politische Werbung nicht von ausgefeilten und abgewogenen Argumenten begleitet wird. Oft sprechen die Einzeiler die argumentativen und deliberativen Fähigkeiten der Bürger gar nicht umfassend an, sondern beschränken sich darauf, Wähler mit Forderungen oder Ankündigungen künftiger Maßnahmen zu »bombardieren«. Das Fehlen von Begründungen allein stellt jedoch nicht unbedingt einen Verstoß gegen die Pflicht zur Bürgerlichkeit dar. Rawls' normative Theorie der politischen Parteien ist insofern realistisch, als dieser einräumt, dass Parteien und politische Vertreter nicht in der Lage sein werden, ein apathisches und zynisches Volk zu überzeugen (vgl. Rawls 2002: 175). Ungeachtet der von Rawls formulierten Verpflichtung, sich an Bürger *als Bürger* zu wenden und nicht zu versuchen, an bestimmte Spezialinteressen von Gruppen oder Individuen zu appellieren,[18] räumt er ein, dass das Eigeninteresse von Personen und Gruppen zu einem bestimmten Zeitpunkt berücksichtigt werden muss (vgl. Rawls 2002: 208). Geht man davon aus, dass die politischen Parteien die Bürger mobilisieren und politisieren müssen, um sie zur Teilnahme an Wahlen und öffentlichen Beratungen zu bewegen, lässt sich ggf. ein legitimer Platz für begründungsarme, thesenstarke politische Werbung ableiten. Politische Werbung kann grundsätzlich zur Darstellung von Pluralität und zur Strukturierung von Debatten beitragen und damit den Boden für eine gemeinsame politische Willensbildung bereiten, diese initiieren und die Menschen dazu anregen, über ihre politischen Präferenzen nachzudenken.[19]

18 Vgl. Rawls (2002: 208): »Wenn wir Gründe für alle Bürger vorbringen, betrachten wir sie nicht als sozial situierte oder auf andere Art verwurzelte Personen, das heißt nicht als Wesen in dieser oder jener sozialen Klasse oder in dieser oder jener Besitz- oder Einkommensgruppe oder als Vertreter dieser oder jener umfassenden Lehre.«

19 Denkbar wäre auch, für begründungsarme politische Werbung einen ähnlichen Vorbehalt zu formulieren, wie er bei Rawls im öffentlichen Forum für Argumente auf Basis umfassender religiöser oder philosophischer Lehren gilt: Beides, also sowohl das Feh-

Während begründungsarme digitale politische Wahlwerbung, die politisch mobilisieren will, also grundsätzlich eine bestimmte Funktion für den öffentlichen Vernunftgebrauch erfüllen könnte, gilt es im nächsten Schritt, Bedingungen herauszuarbeiten, denen Anzeigen genügen müssten, um diese potenziell deliberative Funktion nicht gleichzeitig zu gefährden.

Wenn das »Bombardement« mit maßgeschneiderter parteipolitischer Werbung nur die potenziellen Wählerinnen und Wähler dieser Partei auf der Grundlage vermuteter Präferenzen trifft, findet keine Pluralisierung der Standpunkte und keine Strukturierung der Debatte statt; stattdessen verengt die Werbung den Marktplatz der Ideen und behandelt die Bürger hinsichtlich ihres Rechts auf politische Information ungleich (vgl. Bay 2018: 1726); als Beschreibungen dieses Problems und seiner Auswirkungen haben sich die Begriffe »Filterblasen« und »Echokammern« etabliert. Aus Sicht des einzelnen Wählers verletzen sogenannte »*dark ads*«, die nur für bestimmte Nutzerinnen und Nutzer sichtbar sind, und/oder selektiv verbreitete Werbung den Grundsatz des gleichberechtigten Zugangs zu politischen Informationen. Wenn Menschen, von denen man annimmt, dass sie die gegnerischen Parteien unterstützen, bei einer Wahl mit negativen Informationen über die Partei oder die Kandidat*innen »bombardiert« werden, um sie davon abzuhalten, ihre vermeintlichen Wahlabsichten zu verwirklichen, besteht die Gefahr, dass sich abwägungsfeindliche Haltungen wie Apathie und Zynismus durchsetzen. Darüber hinaus macht es die digitale Infrastruktur leicht, dass negative Wahlkampfpraktiken in Richtung von Verleumdungskampagnen gehen und so die gegenseitige Achtung der freien und gleichen Bürger nicht aufrechterhalten wird; hier besteht die Gefahr, dass das »politische Kapital der Demokratie«, d.h. die bürgerlichen Tugenden der Fairness und des gegenseitigen Respekts unter freien und gleichen Bürgern, Schaden nimmt. Mit Rawls lässt sich also schließen, dass argumentationsarme digitale Werbung nur dann zum öffentlichen Vernunftgebrauch und zur Stärkung der konstitutionellen Demokratie beitragen kann, wenn sie die Praktiken des negativen *campaigning* und der *dark ads* so weit wie möglich vermeidet und sich stattdessen auf die

len von Begründungen als auch das Einbringen problematischer Begründungen, könnte im Rahmen des öffentlichen Gebrauchs der Vernunft wichtige Zwecke erfüllen und zulässig sein, sofern der betreffende Akteur seine Äußerungen innerhalb eines angemessenen Zeitraums nach Veröffentlichung durch Begründungen ergänzt, die sich an freie und gleiche Bürger richten und dem öffentlichen Vernunftgebrauch entsprechen.

(möglichst gleichmäßige) Information, Mobilisierung und Politisierung der Wähler konzentriert.

Der gleichmäßige Zugang zu verschiedenen politischen Anzeigen und die Möglichkeit des Vergleichs verschiedener Anzeigen und Begründungen (sowohl innerhalb einer Partei als auch zwischen Parteien) kann nicht nur mit dem Grundsatz der Achtung der Bürger*innen als Freie und Gleiche begründet werden. Er ermöglicht zudem Konsistenzprüfungen sowie den Vergleich zwischen Parteiprogrammatiken und fördert damit eine gut informierte, freie politische Willensbildung (und bürgerliche Souveränität). Um ihrer Pflicht zur Bürgerlichkeit nachzukommen und einer genuin »demokratischen digitalen Souveränität« im Wahlkampf zu genügen, sollten politische Parteien daher einen gleichberechtigten Zugang zu politischen Informationen und öffentlichen Begründungen ermöglichen, indem sie a) ihre eigenen, parteispezifischen Anzeigenarchive einrichten und b) begründungsarme Anzeigen (oder solche, die mit problematischen Begründungen operieren) um Links ergänzen, die auf anspruchsvolle Begründungen (und eine Einbettung in das gesamte Wahlprogramm) verweisen.

Darüber hinaus ist es auf einer anderen Ebene wichtig, die soziotechnischen Grundlagen und möglichen identitätspolitischen Effekte des digitalen Wahlkampfs in den Blick zu nehmen. Anders als die Wahlkampfwerbung des vordigitalen Zeitalters, die ebenfalls oft keine detaillierten Begründungen für ihre Positionen lieferte, basieren die Praktiken des digitalen Wahlkampfs auf umfangreichen Datensammlungen, die eine Informationsasymmetrie zwischen Parteien und Bürgern schaffen und diese Asymmetrie zusammen mit Erkenntnissen der Verhaltenspsychologie ausnutzen, um in die Prozesse der politischen Willensbildung des Bürgers einzugreifen. Die soziotechnische Grundlage (umfangreiche Datenerfassung) und die Ziele (Verhaltensänderung durch Appelle an individuelle Präferenzen oder bereits bestehende Vorurteile) des digitalen Microtargeting lassen somit insgesamt wenig Respekt für den Wert der Privatsphäre, für symmetrische Kommunikationsbeziehungen und für die staatsbürgerliche Fähigkeit sowie das Recht auf freie politische Willensbildung eines jeden Bürgers erkennen. Auch wenn in Bezug auf verschiedene Fälle diskutiert werden müsste, wo genau die Grenze zwischen legitimer Überredung und illegitimer Manipulation verläuft, spricht die Asymmetrie der Information, die Reduktion der Adressat*innen auf kalkulierbare Präferenzen und Interessen und die Aufspaltung des Elektorats in identitätspolitische Teilsegmente dafür, digitales Microtargeting als eine Praxis einzustufen, die die Autonomie und politische Souveränität des

Bürgers sowie die Notwendigkeit zur gemeinsamen politischen Willensbildung unzureichend achtet und ermöglicht. Das viel gepriesene potenzielle Gegenmittel gegen mögliche Autonomieverluste durch Microtargeting (vgl. Susser/Roessler/Nissenbaum 2019: 14), nämlich die Erhöhung der Transparenz und die Aufklärung der Wähler über die gesammelten Daten und deren Verwendung, stellt unter Umständen keine einfache Problemlösung dar, weil es nur die Diskrepanz zwischen dem auf Gruppenidentitäten und Präferenzen reduzierten, beeinflussbaren Wähler und dem zu einem eigenen freien politischen Urteil befähigten und zu gemeinsamer politischer Willensbildung aufgerufenen Bürger offenlegt.

Wenn ein Bürger über »bürgerliche Selbstachtung« verfügen soll, d.h. sich als jemand begreifen soll, der wie alle anderen Bürger in der Lage und berechtigt ist, sich eigene Vorstellungen vom Guten und vom politisch Richtigen zu machen und diese im Laufe des Lebens zu verändern, muss dieser Bürger nach Rawls in rechtlichen und sozialen Strukturen aufwachsen, die die Entwicklung dieser bürgerlichen Selbstachtung nicht behindern. Rawls unterstreicht die Notwendigkeit einer öffentlichen politischen Kultur, die diese Selbstachtung unterstützt und ermutigt:

> »Damit die Bürger einer wohlgeordneten Gesellschaft einander als freie und gleiche Personen anerkennen, müssen sie von den Grundinstitutionen erzogen und zur Einsicht in diese Auffassung ihrer selbst gebracht werden. Außerdem müssen die Institutionen dafür sorgen, daß dieses Ideal der politischen Gerechtigkeit öffentlich vorgeführt und gefördert wird. […] Die Vertrautheit mit dieser öffentlichen Kultur und die Beteiligung daran ist eine Möglichkeit für die Bürger, sich nach und nach als freie und gleiche Personen zu begreifen.« (Rawls 2003: 97)

Rawls' These der rechtlich-sozialen Grundlagen der bürgerlichen Selbstachtung lässt sich daher als These der soziotechnischen Grundlagen der bürgerlichen Selbstachtung (vgl. Hoffmann 2020) umformulieren und so auf das Phänomen des digitalen Wahlkampfs anwenden:

Da die Praxis des digitalen politischen Microtargeting auf massiven Informations- (vgl. Tufekci 2014) und Machtasymmetrien (vgl. Bay 2018: 1727) zwischen Partei und Wähler sowie zwischen einzelnen Wählern beruht, scheint sie zur Ausbildung der Selbstwahrnehmung eines Bürgers als jemand mit gleichen Chancen und Rechten zur freien Bildung eigener politischer Urteile wenig förderlich. Dies ist besonders dann der Fall, wenn die Werbung stark personalisiert ist und auf komplexen psychologischen Persönlichkeits-

profilen basiert, wie beim sogenannten »psychographischen Profiling« (vgl. Burkell/Regan 2019: 2). Da die Praxis des digitalen politischen Microtargeting auf die Konstruktion einer personalisierten Wahlumgebung hinausläuft und damit einen Eingriff in die persönliche Sphäre der politischen Willensbildung eines Individuums mit dem Ziel der Verhaltensmanipulation darstellt, scheint sie nicht zuträglich dafür, das Selbstverständnis einer Person als freier, autonomer Bürger, der zu eigenem politischen Urteil und zu gemeinsamer politischen Willensbildung aufgerufen ist, zu fördern.[20] Auch wenn die Bürger entgegen einiger Warnungen vor ihrer extremen Manipulierbarkeit nicht einfach nur Marionetten ohne eigenen Willen sind,[21] sind sie für die Herausbildung und Ausübung ihrer staatsbürgerlichen Fähigkeiten auf eine Vorstellung von sich selbst als frei und gleich angewiesen und als grundsätzlich fähig und berechtigt, ihre eigenen Vorstellungen vom Guten zu entwickeln und diese nach eigenem Ermessen zu revidieren. Soziotechnische Strukturen und Praktiken, die hinsichtlich der von ihnen verwendeten Daten und Techniken des psychografischen Profilings oder der identitätspolitischen Spaltung transparent sind und damit ein Bild des Bürgers als Bündel von Präferenzen und Voreingenommenheiten transportieren, das durch Macht- und Informationsasymmetrien manipulierbar ist, sind der Herausbildung eines solchen Selbstverständnisses als freier und gleicher Bürger sicher nicht förderlich.[22] Eine Erhöhung der Transparenz bezüglich der verwendeten Daten und deren Benutzung bei der Erstellung von Anzeigen, die als Lösung für das Problem der Asymmetrie diskutiert wird, scheint also neue Probleme aufzuwerfen, weil sie ein Bild des Wählers transportiert (und unter Umständen zu deren Zementierung beiträgt), die der bürgerlichen Selbstwahrnehmung in liberalen Demokratien nicht förderlich ist.

Wie also könnte eine »demokratische digitale Souveränität« der Parteien im digitalen Wahlkampf aussehen? Wenn Parteien grundsätzlich einer Pflicht zur Bürgerlichkeit unterliegen und eine Mitverantwortung für das politische

20 Ein ähnliches Argument in Bezug auf Nudging wird formuliert von Nys/Engelen 2017.

21 Für einen Überblick über die These der Manipulationsgefahr durch Microtargeting vgl. Burkell/Regan 2019; Susser/Roessler/Nissenbaum 2019; Gorton 2016.

22 Aktuelle Studien betonen nicht nur Privatheitsbedenken, sondern warnen zudem vor Schweigespiralen und Selbstzensur als Folgen eines erhöhten Bewusstseins von Online-Überwachung, die für manipulative Zwecke verwendet werden könnte, vgl. Dobber et al. 2019 und Harker 2020.

Kapital der Demokratie, d.h. für die Formation eines bürgerlichen Selbstverständnisses, tragen, dann sollten Parteien ihre Microtargeting-Praktiken auch in Bezug auf ihren formativen Beitrag zur politischen Kultur der Demokratie reflektieren.

Auch wenn empirische Forschungen zur Auswirkung von Microtargeting auf das Wahlverhalten und auf das bürgerliche Selbstverständnis noch ausstehen, lassen sich aufgrund der besonderen Verantwortung und Einflussgröße politischer Parteien folgende Empfehlungen aussprechen:

Es scheint grundsätzlich ratsam, dass die politischen Parteien a) zumindest auf psychografisches Profiling verzichten, b) allen Bürgern den gleichen Zugang zu all ihren Anzeigen gewähren (gut zugängliche, gut gegliederte und leicht durchsuchbare parteispezifische Anzeigenarchive) und c) die Anzeigen mit Links zu Materialien ergänzen, die öffentliche Begründungen liefern und eine Einbettung in die Gesamtprogrammatik erlauben. Neben das Bild der politischen Konsumentin, der präferenzorientierte Werbung zugespielt wird, träte so das Bild des politischen Bürgers, dem das Recht und die Fähigkeit zugestanden wird, sich (im Dialog mit anderen Bürger*innen) ein eigenes politisches Urteil zu bilden – und zu gemeinsamer öffentlicher politischer Willensbildung befähigt und berechtigt zu sein. Während ein machttheoretisch verengter Begriff »digitaler Souveränität« im digitalen Wahlkampf als Beherrschung digitaler Techniken zum Zwecke der Stimmenmaximierung, also zur Maximierung politischer Gestaltungsmacht verstanden werden könnte, ließe sich ein normativ erweiterter Begriff »demokratische digitale Souveränität« von vornherein als eine Form der Souveränität ausbuchstabieren, die dem größeren legitimationstheoretischen Zusammenhang liberaler Demokratien – und d.h. dem besonderen Stellenwert öffentlicher Rechtfertigung – Rechnung trägt. Eine »demokratische digitale Souveränität« von Parteien lenkt den Blick darauf, dass Parteien nicht erst dann Gestaltungsmacht haben, wenn sie Kandidat*innen in öffentlichen Ämtern platziert haben, sondern dass sie als zentrale Akteure des öffentlichen Forums mit ihrem Modus der öffentlichen Kommunikation die politische Kommunikationskultur und das bürgerschaftliche Selbstverständnis in liberalen Demokratien extrem prägen und beeinflussen können. Politische Parteien sollten die digitale Wahlwerbung also nicht nur als ein Instrument zum »Stimmenfang« betrachten, sondern all ihr öffentliches Reden und Handeln immer auch als Möglichkeit begreifen, die Entwicklung einer spezifisch bürgerlichen Identität zu unterstützen, die für die Qualität und die Stabilität rechtsstaatlicher demokratischer Regime dringend erforderlich ist.

4. Fazit: Das Desiderat einer »*demokratischen* digitalen Souveränität«

Gibt es gute Gründe, am Begriff der »digitalen Souveränität« festzuhalten – oder sollte man diesen, wie unlängst vorgeschlagen wurde, verwerfen? Wie ich in meinem ideengeschichtlichen Exkurs zu Thomas Hobbes gezeigt habe (s. Abschnitt 1), weist der Souveränitätsbegriff der europäischen Staatstheorie eine spezifische Kombination aus Machtdimensionen und Rechtsdimensionen auf, die der Entwicklung und Herausbildung einer liberalen, konstitutionellen Demokratie förderlich waren. Es ist also nicht so, dass der Souveränitätsbegriff per se undemokratisch oder autoritär wäre und insofern als Orientierungsbegriff für liberale Demokratien unbrauchbar wäre (vgl. Thiel 2020 und Pohle/Thiel 2021). Vielmehr vereint der Begriff von Beginn an die Idee einer *rechtssetzenden* Macht mit der Idee einer *rechtmäßigen* – weil auf (möglicher) Zustimmung beruhenden – Macht und inkludiert zudem (bei Hobbes wenigstens rudimentäre) *naturrechtliche* Elemente, die dem, was legitimerweise politisch gewollt werden kann, Grenzen setzt. Dem Souveränitätsbegriff, wie er in der europäischen Staatstheorie entwickelt wurde, wohnt also von Anfang an eine dezidiert normative Dimension inne, die die Entwicklung eines liberal-konstitutionell eingehegten Verständnisses von Volkssouveränität (wie es sich etwa in John Rawls' Demokratietheorie finden lässt) ermöglichte und der mit dieser Dimension für den gegenwärtigen Digitalisierungsdiskurs fruchtbar gemacht werden kann. Der Begriff birgt insofern Potenzial dafür, dass liberale, rechtsstaatliche Demokratien den spezifischen Legitimationskontext des Begriffs stark machen und den Souveränitätsbegriff dezidiert als normativen, demokratietheoretisch eingebetteten Begriff konturieren. Die Entwicklung eines demokratietheoretisch fundierten Begriffs »digitaler Souveränität« stellt aber nicht nur eine ideengeschichtliche und begriffsfunktionale *Möglichkeit* dar, wie durch den ideengeschichtlichen Exkurs gezeigt wurde. Die Entwicklung eines normativen Begriffs »demokratischer digitaler Souveränität« ist zudem eine dringende demokratiepolitische *Notwendigkeit*, wie in diesem Aufsatz am Beispiel des digitalen Wahlkampfs und auf der Grundlage der normativen Demokratietheorie von John Rawls argumentiert wurde: Parteien streben legitimerweise nach politischer Gestaltungsmacht. Sie sollten dabei aber auch ihrer Verantwortung für die demokratische politische Kultur einer Gesellschaft, für den öffentlichen Vernunftgebrauch und für die bürgerliche Selbstwahrnehmung gerecht werden. Auch wenn Rawls selbst den Souveränitätsbegriff selten explizit verwendet oder definiert, lässt sich

seiner konstitutionell-deliberativen Demokratietheorie ein Begriff »demokratischer digitaler Souveränität« entnehmen, der die öffentliche Rechtfertigung staatlicher Gestaltungsmacht vor den als frei und gleich begriffenen Bürgern ins Zentrum rückt. Ein solcher deliberativ und konstitutionell eingerahmter Begriff von Volkssouveränität umfasst mehr als nur Mehrheitsentscheidungen und rückt die Möglichkeit einer vernünftigen öffentlichen Rechtfertigung in den Mittelpunkt:

> »Wenn also alle zuständigen Regierungsbeamten in Hinsicht auf wesentliche Verfassungsinhalte und Angelegenheiten grundlegender Gerechtigkeit im Sinne der öffentlichen Vernunft handeln und ihr folgen, und wenn alle vernünftigen Bürger sich selbst idealerweise so betrachten, als wären sie Gesetzgeber, die der öffentlichen Vernunft folgen, dann sind legale Satzungen, die Ausdruck einer Mehrheitsmeinung sind, legitimes Recht.« (Rawls 2002: 172)

Das legitime Ziel der Erlangung politischer Gestaltungsmacht sollte also nicht mit Mitteln erreicht werden, die dem Legitimationskontext liberaler Verfassungsstaaten zuwiderlaufen – als potenzielle Amtsinhaber*innen sowie Repräsentantinnen und Repräsentanten des Staates sollten Parteien und Kandidat*innen auch im Wahlkampf *demokratisch souverän agieren* und dazu beitragen, dass eine zivilisierte politische Kultur und eine freie, vernünftige, öffentliche politische Willensbildung ermöglicht wird.

Welche Anforderungen an eine derart verstandene »demokratische digitale Souveränität« für Parteien im digitalen Wahlkampf zu stellen wären, wurde im Artikel diskutiert. Das Beispiel des digitalen Wahlkampfs diente hierbei als Brennglas dafür, wie demokratische Gesellschaften ganz allgemein in der Digitalisierung herausgefordert werden – und dazu aufgerufen sind, diese demokratiepolitisch verantwortlich mitzugestalten.

Digitale Strukturen führen nicht nur zur Entgrenzung des politischen Raumes und zu empfindlichen Begrenzungen der staatlichen Handlungsmacht, sondern auch zu neuen Herausforderungen demokratischer Öffentlichkeiten und der demokratischen Legitimationslogik. Neben all ihrem demokratiepolitischen Potenzial zur Verbreitung von Informationen und zur politischen Mobilisierung bergen digitale Strukturen, weil sie von demokratisch indifferenten oder demokratiefeindlichen Kräften benutzt werden können, immer auch die Gefahr einer Delegitimierung und Zersetzung der Demokratie – von außen und von innen. Autoritäre Staaten betreiben zunehmend nicht nur demokratiefeindliche, sondern demokratiezersetzende

Politik, sie intervenieren mit digitalen Tools (Desinformationskampagnen, *social bots* etc.) in Wahlen und betreiben aktiv die Spaltung liberaler Demokratien (vgl. Ó Fathaigh et al. 2021). Auch digitale Wahlkampftechniken demokratischer Parteien, die das Elektorat in Teilsegmente zerlegen und individuell mit gruppenspezifischen oder individuellen Informationen und Werbebotschaften beschießen, sind nicht nur wenig förderlich für die gemeinsame demokratische politische Willensbildung, sondern bergen Gefahren der identitätspolitischen Fragmentierung der Gesellschaft und der schleichenden Transformation des Ideals des öffentlich deliberierenden Bürgers in ein von Präferenzen oder Gruppenidentitäten getriebenes Individuum. Ganz allgemein steht in der Digitalisierung nicht nur die souveräne Handlungsmacht demokratischer Staaten auf dem Spiel, sondern auch die Stabilität und Legitimität der Demokratie. Die Digitalisierung kann und muss daher aktiv von demokratischen Gesellschaften gestaltet werden. Diese Gestaltung setzt selbstverständlich Machtressourcen und Handlungsfähigkeit voraus – aber eben auch den klaren Blick für Ziele und für ermöglichende sowie gefährdende Bedingungen. Um die Digitalisierung demokratiepolitisch verantwortlich gestalten zu können, bedarf es daher eines normativen Begriffs »demokratischer digitaler Souveränität«. Geistes- und Sozialwissenschaften, Staats- und Rechtstheorie, politische Theorie und Ideengeschichte sowie insbesondere die Demokratietheorie sollten stärker als bisher geschehen dabei mithelfen, Konturen eines solchen normativ reichhaltigen Begriffs »demokratischer digitaler Souveränität« für unterschiedliche Ebenen und Akteure der Demokratie zu erarbeiten[23] – um damit der gesellschaftlichen Selbstverständigung und der gesellschaftlichen Arbeit an der Zukunft der Demokratie notwendiges Orientierungs- und Gestaltungswissen an die Hand zu geben.

Literaturverzeichnis

Bay, Morten (2018): »Social media ethics: A Rawlsian approach to hypertargeting and psychometrics in political and commercial campaigns«, in: ACM Transactions on Social Computing 1 (4), Article 16 (December 2018), 14 Seiten, https://doi.org/10.1145/3281450.

23 Der Orientierungsbedarf ist groß. Vgl. für aktuelle Bemühungen im Diskurs, einen wertbezogenen Begriff digitaler europäischer Souveränität zu entwickeln, Roberts et al. 2021.

Bennett, Colin J. (2013): »The politics of privacy and the privacy of politics: Parties, elections and voter surveillance in Western democracies«, in: First Monday 18 (8), https://doi.org/10.5210/fm.v18i8.4789.

Bennett, Colin J. (2016): »Voter databases, micro-targeting, and data protection law: Can political parties campaign in Europe as they do in North America?«, in: International Data Privacy Law 6 (4), S. 261–275.

Bonotti, Matteo (2017): Partisanship and political liberalism in diverse societies, Oxford: Oxford University Press.

Burkell, Jacquelyn/Regan, Priscilla M. (2019): »Voter preferences, voter manipulation, voter analytics: Policy options for less surveillance and more autonomy«, in: Internet Policy Review 8, S. 1–24, https://doi.org/10.14763/2019.4.1438.

Chester, Jeff/Montgomery, Kathryn C. (2017): »The role of digital marketing in political campaigns«, in: Internet Policy Review 6 (4), S. 1–20.

Creemers, Rogier (2020): »China's conception of cyber sovereignty: Rhetoric and realization«, in: Dennis Broeders/Bibi van den Berg (Hg.), Governing cyberspace: Behaviour, diplomacy and power, Lanham: Rowman & Littlefield, S. 107–145.

Dammann, Finn/Glasze, Georg (2022): »›Wir müssen als Deutsche und Europäer unsere digitale Souveränität zurückgewinnen!‹ Historische Rekonstruktion und internationale Kontextualisierung der Diskurse einer ›digitalen Souveränität‹ in Deutschland«, in: Georg Glasze/Eva Odzuck/Ronald Staples (Hg.), Was heißt digitale Souveränität? Diskurse, Praktiken und Voraussetzungen »individueller« und »staatlicher Souveränität« im digitalen Zeitalter, Bielefeld: transcript, S. 29–60.

Dobber, Tom/Trilling, Damian/Helberger, Natali/de Vreese, Claes (2019): »Spiraling downward: The reciprocal relation between attitude toward political behavioral targeting and privacy concerns«, in: new media and society 21, S. 1212–1231, https://doi.org/10.1177/1461444818813372.

Floridi, Luciano (2020): »The fight for digital sovereignty: What it is, and why it matters, especially for the EU«, in: Philosophy & Technology 33, S. 369–378, https://doi.org/10.1007/s13347-020-00423-6.

Fukuyama, Francis (2019): Identität. Wie der Verlust der Würde unsere Demokratie gefährdet, Hamburg: Hoffmann & Campe.

Gorton, William A. (2016): »Manipulating citizens: How political campaigns' use of behavioral science harms democracy«, in: New Political Science 38, S. 61–80, https://doi.org/10.1080/07393148.2015.1125119.

Harker, Michael (2020): »Political advertising revisited: Digital campaigning and protecting democratic discourse«, in: Legal Studies 40, S. 151–171, https://doi.org/10.1017/lst.2019.24.

Hersh, Eitan D. (2015): Hacking the electorate: How campaigns perceive voters, New York: Cambridge University Press.

Herzog, Don (2020): Sovereignty, RIP, New Haven/London: Yale University Press.

Hobbes, Thomas (1966): Leviathan oder Stoff, Form und Gewalt eines kirchlichen und bürgerlichen Staates. Herausgegeben und eingeleitet von Iring Fetscher. Übersetzt von Walter Euchner, Frankfurt a.M.: Suhrkamp.

Hoffmann, Anna Lauren (2020): »Rawls, information technology, and the sociotechnical bases of self-respect«, in: Shannon Vallor (Hg.), The Oxford Handbook of Philosophy of Technology, Oxford: Oxford University Press, S. 231–249, https://doi.org/10.1093/oxfordhb/9780190851187.013.15.

Issenberg, Sasha (2012): The victory lab. The secret science of winning campaigns, New York: Crown.

Kosinski, Michal/Stilwell, David/Graepel, Thore (2013): »Private traits and attributes are predictable from digital records of human behavior«, in: Proceedings of the National Academy of Sciences of the United States of America 110 (15), S. 5802–5805.

Kreiss, Daniel/McGregor, Shannon (2018): »Technology firms shape political communication: The work of Microsoft, Facebook, Twitter, and Google with campaigns during the 2016 U.S. Presidential Cycle«, in: Political Communication 35 (2), S. 155–177.

Leyrer, Katharina/Hagenhoff, Svenja (2022): »›Digitale Souveränität‹ in der medienvermittelten öffentlichen Kommunikation: die Beziehung zwischen Rezipient*in und Gatekeeper«, in: Georg Glasze/Eva Odzuck/Ronald Staples (Hg.), Was heißt digitale Souveränität? Diskurse, Praktiken und Voraussetzungen »individueller« und »staatlicher Souveränität« im digitalen Zeitalter, Bielefeld: transcript, S. 247–286.

Lister, Matt (2014): »Sovereignty«, in: Jon Mandle/David A. Reidy (Hg.), The Cambridge Rawls lexicon, Cambridge: Cambridge University Press, S. 800–803, https://doi.org/10.1017/CBO9781139026741.211.

Maréchal, Nathalie (2017): »Networked authoritarianism and the geopolitics of information: Understanding Russian internet policy«, in: Media and Communication 5 (1), S. 29–41. https://doi.org/10.17645/mac.v5i1.808.

Muirhead, Russell/Rosenblum, Nancy L. (2006): »Political liberalism vs. ›the great game of politics‹: The politics of political liberalism«, in: Perspectives on Politics 4, S. 99–108, https://doi.org/10.1017/S1537592706060105.

Muirhead, Russell/Rosenblum, Nancy L. (2020): »The political theory of parties and partisanship: Catching up«, in: Annual Review of Political Science 23, S. 95–110, https://doi.org/10.1146/annurev-polisci-041916-020727.

Nys, Thomas R.V./Engelen, Bart (2017): »Judging nudging: Answering the manipulation objection«, in: Political Studies 65, S. 199–214, https://doi.org/10.1177/0032321716629487.

Odzuck, Eva (2014): »Narration und Argument in der Politik. Das Konzept der Fiktionalität in der Autorisierungstheorie von Hobbes' Leviathan«, in: Wilhelm Hofmann/Katja Renner/Judith Teich (Hg.), Narrative Formen der Politik, Wiesbaden: Springer VS, S. 105–121.

Odzuck, Eva (2020): »Personalisierter Wahl-Kampf oder öffentliche Willens-Bildung? Digitales Politisches Micro-Targeting als Richtungsentscheidung der Demokratie«, in: Zeitschrift für Politik (2), S. 153–184.

Odzuck, Eva/Günther, Sophie (2021): »Digital campaigning as a policy of democracy promotion: Applying deliberative theories of democracy to political parties«, in: Zeitschrift für Politikwissenschaft vom 23.12.2021, https://doi.org/10.1007/s41358-021-00308-w.

Ó Fathaigh, Ronan/Dobber, Tom/Zuiderveen Borgesius, Frederik/Shires, James (2021): »Microtargeted propaganda by foreign actors: An interdisciplinary exploration«, in: Maastricht Journal of European and Comparative Law 28 (6), S. 856–877, https://doi.org/10.1177/1023263X211042471.

Papakyriakopoulos, Orestis/Shahrezaye, Morteza/Thieltges, Andree/Serrano, Juan Carlos Medina/Hegelich, Simon (2017): »Social Media und Microtargeting in Deutschland«, in: Informatik Spektrum 40, S. 327–335, https://doi.org/10.1007/s00287-017-1051-4.

Pohle, Julia/Thiel, Thorsten (2021): »Digitale Souveränität. Von der Karriere eines einenden und doch problematischen Konzepts«, in: Chris Piallat (Hg.), Der Wert der Digitalisierung: Gemeinwohl in der digitalen Welt (= Digitale Gesellschaft, Band 36), Bielefeld: transcript, S. 319–340.

Potthast, Keno Christoffer (2021): »Wahlkampf ohne Diskurs?«, in: Verfassungsblog: On Matters Constitutional. Online unter: https://verfassungsblog.de/wahlkampf-ohne-diskurs/vom 08.11.2021.

Rawls, John (2002): Das Recht der Völker. Enthält: »Nochmals: Die Idee der öffentlichen Vernunft«. Übersetzt von Wilfried Hinsch, Berlin/New York: de Gruyter.

Rawls, John (2003): Gerechtigkeit als Fairneß. Ein Neuentwurf. Herausgegeben von Erin Kelly. Aus dem Amerikanischen von Joachim Schulte, Frankfurt a.M.: Suhrkamp.

Ritzi, Claudia/Zierold, Alexandra (2019): »Souveränität unter den Bedingungen der Digitalisierung«, in: Isabelle Borucki/Wolf Schünemann (Hg.), Internet und Staat: Perspektiven auf eine komplizierte Beziehung, Baden-Baden: Nomos, S. 33–56, https://doi.org/10.5771/9783845290195-33.

Roberts, Huw/Cowls, Josh/Casolari, Federico/Morley, Jessica/Taddeo, Mariarosaria/Floridi, Luciano (2021): »Safeguarding European values with digital sovereignty: An analysis of statements and policies«, in: Internet Policy Review 10 (3), S. 1–26, https://doi.org/10.14763/2021.3.1575.

Sauer, Stefan/Staples, Ronald/Steinbach, Vincent (2022): »Der relationale Charakter von ›digitaler Souveränität‹ .Zum Umgang mit dem ›Autonomie/Heteronomie‹-Dilemma in sich transformierenden Arbeitswelten«, in: Georg Glasze/Eva Odzuck/Ronald Staples (Hg.), Was heißt digitale Souveränität? Diskurse, Praktiken und Voraussetzungen »individueller« und »staatlicher Souveränität« im digitalen Zeitalter, Bielefeld: transcript, S. 287–315.

Susser, Daniel/Roessler, Beate/Nissenbaum, Helen (2019): »Technology, autonomy, and manipulation«, in: Internet Policy Review 8, S. 1–22, https://doi.org/10.14763/2019.2.1410.

Tagesschau (2021): »Bericht der US-Geheimdienste: Putin bei US-Wahl für Trump«. Online unter: https://www.tagesschau.de/ausland/amerika/us-wahl-einfluss-geheimdienst-101.html vom 16.03.2021.

Thiel, Thorsten (2020): »Gewollte Kontrolle«, in: Internationale Politik, Special, Digitales Europa 2030, Nr. 3, S. 68–73.

Tretter, Max (2022): »›Digitale Souveränität‹ als Kontrolle. Ihre zentralen Formen und ihr Verhältnis zueinander«, in: Georg Glasze/Eva Odzuck/Ronald Staples (Hg.), Was heißt digitale Souveränität? Diskurse, Praktiken und Voraussetzungen »individueller« und »staatlicher Souveränität« im digitalen Zeitalter, Bielefeld: transcript, S. 89–126.

Tufekci, Zeynep (2014): »Engineering the public: Big data, surveillance and computational politics«, in: First Monday 19, S. 1–39, http://dx.doi.org/10.5210/fm.v19i7.4901.

Zeit Online (2018): »US-Wahl 2016: Forscher weisen Russland Einmischung in US-Wahlkampf nach«. Online unter: https://www.zeit.de/politik/ausland/2018-12/us-wahl-2016-russland-einmischung-soziale-medien vom 18.12.2018.

Zuiderveen Borgesius, Frederik/Moeller, Judith/Kruikemeier, Sanne/Ó Fathaigh, Ronan/Irion, Kristina/Dobber, Tom/Bodó, Balázs/de Vreese, Claes H. (2018): »Online political microtargeting: Promises and threats for democracy«, in: Utrecht Law Review 14 (1), S. 82–96.

Souveränität, Integrität und Selbstbestimmung – Herausforderungen von Rechtskonzepten in der digitalen Transformation

Christian Rückert, Christoph Safferling, Franz Hofmann

Abstract *Der Begriff der »digitalen Souveränität« lässt sich aus einer rechtswissenschaftlichen Perspektive in die drei Unterbegriffe der Souveränität, der Integrität und der Selbstbestimmung untergliedern. Mit ihnen können die Rechtsbeziehungen zwischen Staaten, Bürger*innen sowie zwischen Staat und Bürger*innen beschrieben werden. Alle diese Konzepte stehen durch die Digitalisierung vor neuen Herausforderungen. Hinsichtlich der zwischenstaatlichen Souveränität geht es vor allem um sogenannte transnationale Datenzugriffe. Ein praktischer Anwendungsfall ist der Zugriff auf personenbezogene Daten von Bürger*innen im Ausland zu Zwecken der Strafverfolgung. In diesen Fällen, die bislang vor allem unter klassischen staatsrechtlichen Souveränitätsaspekten diskutiert wurden, sollte künftig der Blick vermehrt auf die digitale Integrität der betroffenen Bürger*innen und die entsprechenden Schutzpflichten der Staaten gerichtet werden. Aber auch die selbstbestimmte Regelung der eigenen Verhältnisse erscheint gefährdet. Das Recht hat insbesondere sicherzustellen, dass die Entscheidungsfreiheit auch in der Digitalgesellschaft gewährleistet bleibt.*

Der Datenverkehr hat durch die Weiterentwicklung der digitalen Kommunikation, durch die zunehmende Vernetzung von Alltagsgegenständen (»Internet der Dinge«) und durch die Automatisierung kommunikativer Abläufe nicht nur enorm zugenommen, sondern ist gerade durch sogenanntes »Cloud-Computing« grenzenlos geworden. Das Recht mit seinen häufig aus dem 19. Jahrhundert stammenden Vorstellungen, Konzepten und Normen, wird dabei besonders herausgefordert.

In diesem Beitrag sollen zwei Aspekte untersucht werden: Strafrecht und Privatrecht. Der bislang unscharf gebliebene Begriff der »digitalen Souveränität« wird dabei in verschiedene Teilaspekte des Konzepts aufge-

gliedert: Um klassische Souveränität im staatsrechtlichen Sinn geht es im Verhältnis von Nationalstaaten untereinander. Hier stellt sich im Bereich des grenzüberschreitenden Datenverkehrs und der Nutzung grenzüberschreitender digitaler Dienstleistungen wie Cloud-Computing die Frage, ob sich die staatliche Souveränität auch auf den digitalen Raum erstreckt, ob also im Jellinek'schen Sinne (vgl. Jellinek 1922) das Staatsgebiet auch einen digitalen Bereich umfasst. Besonders relevant wird diese Frage bei grenzüberschreitenden Dateneingriffen durch staatliche Behörden, z.B. Strafverfolgungsbehörden. Stellt eine Datenerhebung »auf« fremdem Staatsgebiet einen Eingriff in die Souveränität desjenigen Staates dar, auf dessen Staatsgebiet sich der Datenspeicher befindet?

Im Verhältnis des Staates zu (seinen) Bürger*innen geht es dagegen juristisch betrachtet nicht um die »digitale Souveränität« der Bürger*innen, sondern um deren digitale Integrität, welche ihnen durch die Grund- und Menschenrechte des Grundgesetzes, der Europäischen Grundrechtecharta und der Europäischen Menschenrechtskonvention garantiert wird. Noch weiter entfernt vom traditionellen juristischen Verständnis des Begriffs der Souveränität ist schließlich der letzte rechtliche Teilaspekt »digitaler Souveränität«: Im Verhältnis der Bürger*innen untereinander – also im Privatrecht – geht es um die Wahrung und den Ausgleich der »digitalen Selbstbestimmung« oder der »digitalen Privatautonomie« der handelnden Rechtssubjekte. Die Rechtskonzepte des Privatrechts werden hier in vielfacher Hinsicht herausgefordert: So wird allen voran die Gestaltung und Nutzung des digitalen Raums nahezu ausschließlich von großen (zumeist ausländischen) Technologiekonzernen bestimmt, welche dem*der Einzelnen nicht als Gleichgestellte, sondern als Konstrukte mit staatsähnlicher Macht gegenübertreten. Auch die schnell wachsende Bedeutung von digitalen Gütern, insbesondere Daten, spiegelt sich nicht immer hinreichend in der Ordnung des deutschen Zivilrechts wider. Namentlich die selbstbestimmte Verwertung personenbezogener Daten ist bisher nicht zufriedenstellend geklärt.

Der folgende Beitrag beleuchtet die Teilkonzepte der »digitalen Souveränität« (staatliche Souveränität über Daten im Verhältnis von Staaten untereinander, digitale Integrität der Bürger*innen gegen staatliche Dateneingriffe und digitale Selbstbestimmung/Privatautonomie im Verhältnis der Bürger*innen untereinander einschließlich gegenüber staatsähnlich agierenden Technologiekonzernen) unter zwei verschiedenen Blickwinkeln: Im Straf- und Strafverfahrensrecht wird der Blick auf mögliche Verletzungen staatlicher Souveränität und digitaler Integrität der Bürger*innen durch

grenzübergreifende Dateneingriffe gerichtet und das Verhältnis unter dem Gesichtspunkt des Grund- und Menschenrechtsschutzes neu austariert (Teil I). Das Privatrecht muss dagegen klären, wie digitale Selbstbestimmung und Privatautonomie auch unter Eindruck der Übermächtigkeit der Tech-Unternehmen funktionieren kann. Zur Illustration wird das Verhältnis von Datenschutz und Selbstbestimmung angerissen (Teil II).

Teil I: Menschenrechtsschutz und Datensouveränität im Strafprozess

Heute ist es bei strafrechtlichen Ermittlungen häufig erforderlich, Daten zu sammeln, deren physischer Speicherort (auch) im Ausland liegt. Die Datenerfassung im Ausland stellt möglicherweise einen Eingriff in die »(digitale) Souveränität« des ausländischen Staates dar und darf daher ohne die Zustimmung dieses Staates – nach klassischem Völkerrecht – nicht erfolgen. Außer in den eher seltenen Fällen des Schutzes von Staatsgeheimnissen sind staatliche Interessen bei strafrechtlichen Ermittlungen in virtuellen Speichern aber nicht unmittelbar betroffen. Die Speicher selbst sind in aller Regel auch nicht staatliches Eigentum, sondern werden von global agierenden Unternehmen (Google, Microsoft, Apple etc.) betrieben. Es geht hauptsächlich um personenbezogene Daten und damit um den Schutz der Betroffenen vor staatlicher Einmischung überhaupt. Dass diese durch eine ausländische Regierung erfolgt, ist nur ein zusätzlicher Aspekt, der an der unmittelbaren Betroffenheit des Individuums kaum etwas ändert. Damit kommt es aber auf die Qualität des Eingriffs selbst an, auf dessen Rechtsstaatlichkeit und dessen Respekt vor den Grund- und Menschenrechten der Betroffenen. Mangelt es an solchen Garantien und Schutzmaßnahmen, müssen die liberalen Staaten sicherstellen, dass sowohl ihre Bürger*innen als auch die im jeweiligen Staat lebenden Ausländer*innen vor der Ausforschung durch ausländische Regierungen geschützt sind. Bislang ist die Rechtsprechung in Deutschland eher einer völkerrechtlichen Vorstellung zugetan und differenziert danach, ob der betroffene Staat die Souveränitätsverletzung rügt. Der folgende Beitrag plädiert daher sowohl für die Ausarbeitung künftiger völkerrechtlicher Vereinbarungen (z.B. der E-Evidence-Verordnung auf Ebene der Europäischen Union auf der Grundlage des Prinzips der gegenseitigen Anerkennung) als auch für die Lösung bestimmter Rechtsfragen (z.B. betreffend die Durchsuchungsmöglichkeit externer Speichermedien in § 110 Abs. 3 StPO) für eine Verlagerung des Fokus weg von Fragen der

Souveränität (im klassischen Sinn der Staatsrechtslehre und des Völkerrechts) hin zu Fragen des Schutzes der Menschenrechte bei grenzüberschreitenden Dateneingriffen durch ausländische Staaten.

1. Die praktische Bedeutung transnationaler Dateneingriffe für das Strafverfahren

1.1 Digitale Daten als Beweismittel im Strafverfahren

In der Praxis der Strafverfolgung sind transnationale Dateneingriffe nicht nur in klassischen Cybercrime-Verfahren relevant. Daten als solche werden mehr und mehr zu einem »Standardbeweismittel« in Strafverfahren wegen ganz unterschiedlicher Delikte. Grund hierfür ist die immer stärker werdende Durchdringung aller Lebensbereiche der Bürger*innen mit digitalen Technologien. Große Teile der Berufswelt, aber auch die Verwaltung des eigenen Lebens und die Kommunikation sind weitgehend digitalisiert. Daher hinterlassen Bürger*innen – und damit auch Tatverdächtige – stetig mehr Datenspuren, die in Strafverfahren als Beweismittel oder, praktisch nochmals deutlich relevanter, als Grundlage eines Tatverdachts für weitere – ggf. realweltliche (z.B. Durchsuchungen) – Ermittlungsmaßnahmen Verwendung finden. Neben Spuren der klassischen Individualkommunikation mittels E-Mail, Messengerdiensten und Voice-over-IP-Telefonie sowie der Datenverarbeitung und -speicherung auf privaten informationstechnischen Systemen wie Smartphones, Laptops, Tablets und Smart Watches werden auch in zunehmendem Maße Gegenstände des täglichen Lebens als Geräte des »Internet of Things« (IoT) angeboten. Diese Geräte – wie z.B. Stromzähler, Kühlschränke, Automobile, Heim-Assistenzsysteme und Kaffeemaschinen – speichern und verarbeiten ebenfalls Daten und kommunizieren über das Internet mit anderen IoT-Geräten und Personen (vgl. Rückert 2020a).

1.2 Praktisch bedeutsame Arten der transnationalen Dateneingriffe

Die Datensätze, welche für deutsche Strafverfolgungsbehörden relevant sind, befinden sich dabei nicht ausschließlich auf deutschem Staatsgebiet. In vielen Fällen sind gerade Daten verfahrensrelevant, die außerhalb des deutschen Hoheitsgebiets lokalisiert sind. Als »Ort« der Daten gilt dabei nach hergebrachtem Verständnis derjenige Ort, an dem sich der Datenträger physisch befindet, auf dem die Daten gespeichert sind (vgl. Brodowski/Eisenmenger 2014). Der traditionelle und hinsichtlich staatlicher Souveränitätsansprüche unproblematische Weg, im Ausland gespeicherte Daten zu erhalten, besteht

in der Rechtshilfe. Hierbei ersucht derjenige Staat, in dem die strafrechtlichen Ermittlungen stattfinden, denjenigen Staat, auf dessen Hoheitsgebiet die Daten gespeichert sind, darum, die Daten durch seine Strafverfolgungsbehörden erheben zu lassen und diese dann an die Strafverfolgungsbehörden des ersuchenden Staates herauszugeben. Trotz Beschleunigung und Effektivierung des Rechtshilfeverfahrens durch bi- und multilaterale völkerrechtliche Abkommen (z.B. Vertrag vom 14. Oktober 2003 zwischen der Bundesrepublik Deutschland und den Vereinigten Staaten von Amerika über die Rechtshilfe in Strafsachen mit Zusatzvertrag vom 18. April 2006) und insbesondere europarechtliche Regelungen (v.a. die Richtlinie über die Europäische Ermittlungsanordnung, RL 2014/41/EU) wird das Rechtshilfeverfahren von Strafverfolgungsbehörden insgesamt als zu langsam und ineffektiv empfunden. Dies gilt sowohl im Allgemeinen als auch im Besonderen für digitale Daten als Beweismittel, bei denen die Flüchtigkeit und Veränderlichkeit von Datensätzen eine besondere Herausforderung darstellt (vgl. Rückert 2020a). Daher fordern Strafverfolgungsbehörden seit Langem, unmittelbaren Zugriff auf Daten, welche im Ausland lokalisiert sind, zu erhalten.

Die praxisrelevanten Konstellationen der Erhebung von Daten im Ausland lassen sich dabei in drei Fallgruppen unterteilen: (1) Zunächst können öffentlich zugängliche Daten im Ausland lokalisiert sein, wenn sich der Server, über den das jeweilige allgemein zugängliche Internetangebot – z.B. Foren, Webseiten, Boards, Handelsplattformen und soziale Medien – betrieben wird, im Ausland befindet. Die von dem*der Tatverdächtigen stammenden öffentlich zugänglichen Daten wie Foreneinträge, Angebote auf Handelsplattformen oder Postings in sozialen Medien befinden sich dann auch »im« Ausland. (2) Besonders interessant für strafrechtliche Ermittlungen sind außerdem Daten von Telekommunikations- oder Telemedienanbietern wie z.B. Internetzugangsdienste, Cloud-Dienstleister, Soziale Netzwerke, Messengerdienste, Voice-over-IP-Anbieter. Diese halten Bestandsdaten (§§ 3 Nr. 6, 172 TKG und §§ 2 Abs. 2 Nr. 2, 22 Abs. 1 S. 1 TTDSG) ihrer Kunden vor, verarbeiten Verkehrs- und Nutzungsdaten (§§ 9, 12 TTDSG, § 2 Abs. 2 Nr. 3 TTDSG) und verfügen oftmals auch über Inhaltsdaten der von ihnen vermittelten Kommunikationsvorgänge oder gehosteten Inhalte. Nicht selten haben die genannten Dienstleister ihren Sitz im Ausland und betreiben auch die Serverinfrastrukturen, auf denen die relevanten Daten verarbeitet und gespeichert werden, im Ausland. (3) Schließlich können auch auf privaten, im Ausland befindlichen informationstechnischen Systemen verarbeitete Daten von Interesse für Ermittler*innen sein. In vielen Kriminalitätsbereichen –

z.B. dem Handel mit illegalen Gütern und Dienstleistungen im sogenannten Darknet, bei klassischen Cybercrime-Delikten, aber auch im Bereich der organisierten Kriminalität (vgl. Goger/Stock 2017) – befinden sich Täter*innen, Gehilf*innen oder Datenspeicher im Ausland und Täter*innengruppierungen operieren hier zunehmend grenzüberschreitend (vgl. Burchard 2018a). Besonders relevant ist dies bei denjenigen Delikten, bei denen sich die deutsche Strafgewalt – z.B. aufgrund des sogenannten Weltrechtsprinzips – auch auf Taten erstreckt, die im Ausland begangen wurden (vgl. Rückert 2020b).

Die Zugriffe auf die im Ausland belegenen Daten erfolgt in den drei gerade genannten Fallkonstellationen auf unterschiedliche Weise: (1) Auf öffentlich zugängliche Daten im Internet, z.B. in Foren und sozialen Medien, wird durch sogenannte Open Source Intelligence-Maßnahmen (OSINT) zugegriffen, zu denen sowohl einfache »Online-Streifen« als auch automatisierte Datensammlungen mittels sogenannter Crawler zählen (vgl. Kalpakis et al. 2016; Staffler/Jany 2020). (2) Der Zugriff auf Daten, die bei Telekommunikations- und Telemediendienstanbietern gespeichert sind oder von diesen verarbeitet werden, erfolgt entweder im Rahmen einer Telekommunikationsüberwachung (§ 100a StPO), durch die Abfrage von bei den Anbietern gespeicherten Daten (§§ 100g, 100j, 100k StPO) oder im Wege der Beschlagnahme (§§ 94ff. StPO; vgl. BVerfG 2009). (3) Der Zugriff auf private informationstechnische Systeme im Ausland betrifft in der Praxis vor allem sogenannte Cloud-Dienstleistungen (vgl. BVerfG 2016; Krcmar 2016). Auf diese Daten wird entweder im Wege einer elektronischen Durchsicht nach § 110 Abs. 3 StPO (vgl. Wicker 2013a) oder mittels einer Online-Durchsuchung unter Nutzung von Spähprogrammen (vgl. Grözinger 2019) zugegriffen.

2. Die bisherige – souveränitätsgeprägte – Debatte um strafprozessuale transnationale Dateneingriffe

Die bisher – und bisweilen recht intensiv – geführte Debatte über die Zulässigkeit von strafprozessualen Zugriffen auf Daten im Ausland dreht sich bislang um die staatliche Souveränität über Daten, die auf staatlichem Hoheitsgebiet gespeichert wurden. Das grundlegende Argumentationsmuster lautet dabei, dass Daten auf staatlichem Hoheitsgebiet der Souveränität des jeweiligen Staates unterfallen und Zugriffe von ausländischen Staaten daher eine Verletzung der staatlichen Souveränität mit sich brächten. Im Übrigen spaltet sich die Diskussion danach auf, ob es sich um den Zugriff auf öffentlich zugängliche Daten, auf Daten bei Telekommunikations- und Te-

lemediendienstanbietern oder auf private informationstechnische Systeme, insbesondere Cloud-Speicher, handelt.

2.1 Der Anknüpfungspunkt: staatliche Souveränität über Daten?

Dreh- und Angelpunkt der bisherigen Debatte ist damit die Grundannahme, dass Daten, die auf einem Datenträger gespeichert sind, der sich physisch im Hoheitsgebiet eines Staates befindet, der Hoheitsgewalt des jeweiligen Staates unterfallen. Diese Annahme wird zwar in zahlreichen Publikationen zum Problemkreis gemacht, aber nur selten hinterfragt oder ausführlich begründet (ausführliche Auseinandersetzung dagegen bei Burchard 2018a, 2018b). Dass jedenfalls die Rechtspolitik davon ausgeht, dass die Nationalstaaten ihre Herrschaftsgewalt auch über Daten ausüben, zeigt allein schon die Existenz von völkerrechtlichen Abkommen und – innerhalb von Europa – expliziten Regelungen der EU (z.B. Art. 29, 32 Cybercrime Convention, Art. 26ff., 30f. Richtlinie 2014/41/EU). Auch in deutschen (vgl. BVerfG 2018) und internationalen Strafverfahren (vgl. Jansen 2018) wurde das Problem der Souveränitätsverletzung bei grenzüberschreitenden Datenerhebungen thematisiert, und in der strafprozessualen Literatur wird die Problematik bislang ausschließlich unter dem Stichwort der Souveränitätsverletzungen diskutiert (statt vieler: Brodowski 2021; Hauschild 2014; Bruns 2019). Dass diese Grundannahme sowohl technisch-faktisch als auch normativ-juristisch nicht widerspruchsfrei durchhaltbar ist, soll später noch ausführlich gezeigt werden (s. Abschnitt 3.1). Durch die Fokussierung auf die Souveränität der Nationalstaaten über Datenbestände »auf« ihrem Hoheitsgebiet wird jedenfalls auch die Debatte um die Legitimierung von strafprozessualen Zugriffen auf diese Datenbestände über Ländergrenzen hinweg ausschließlich auf Grundlage der möglichen Souveränitätsverletzungen geführt.

2.2 Öffentlich zugängliche Daten: die Cybercrime Convention

Für die Erhebung öffentlich zugänglicher Daten existiert bereits eine Regelung in der sogenannten Cybercrime Convention, welche neben den Mitgliedstaaten des Europarates auch von zahlreichen weiteren Ländern wie z.B. den USA, vielen lateinamerikanischen Ländern, Japan, Kanada und Israel unterzeichnet wurde. Dort ist in Art. 32 lit. a geregelt, dass ein Vertragsstaat ohne Zustimmung oder Genehmigung eines anderen Vertragsstaats »auf öffentlich zugängliche gespeicherte Computerdaten (offene Quellen) zugreifen [darf], gleichviel, wo sich die Daten geographisch befinden« (Council of Europe 2001: 19). Ob aus dieser Regelung nun geschlossen werden kann, dass die

Vertragsstaaten im Umkehrschluss davon ausgehen, dass auch ein Zugriff auf öffentlich zugängliche Daten – ohne eine entsprechende Vereinbarung – eine Souveränitätsverletzung darstellt, ist unklar. Möglich wäre auch die umgekehrte Interpretation, dass es sich um eine deklaratorische Regelung handelt und der Zugriff auf öffentlich verfügbare Daten die Datensouveränität nie tangiert (so wohl die derzeit herrschende Meinung, vgl. Bruns 2019 mit weiteren Nachweisen). In der Praxis der deutschen Gerichte hat jedenfalls die Erhebung öffentlich zugänglicher Daten unter Aspekten der Souveränitätsverletzung noch keine Rolle gespielt (soweit ersichtlich). Dagegen dürfte es – angesichts der Verbreitung von Online-Streifen und anderen OSINT-Maßnahmen – naheliegen, dass es sehr häufig zu entsprechenden Erhebungen kommt.

2.3 Zugriff auf Daten bei Telekommunikations- und Telemediendienstanbietern

Für die Erhebung von Daten bei Telekommunikations- und Telemediendienstanbietern existiert auf europäischer Ebene noch keine Regel für den Direktzugriff. Bisher wird hier vor allem auf die Europäische Ermittlungsanordnung zurückgegriffen, welche grundsätzlich von allen Mitgliedstaaten anzuerkennen und zu vollstrecken ist (vgl. Art. 1 Abs. 2, Art. 9ff. Richtlinie 2014/41/EU). Auch die Telekommunikationsüberwachung im europäischen Ausland ist so möglich (s. Art. 30f. Richtlinie 2014/41/EU). Gerade für volatile Daten von Telekommunikations- und Telemediendienstanbietern erlangt auch die Möglichkeit des Erlasses von Eilmaßnahmen nach Art. 32 der Richtlinie große Bedeutung. Hier muss die zur Vollstreckung berufene Behörde des ausländischen Staates innerhalb von 24 Stunden über entsprechende Maßnahmen entscheiden (s. Art. 32 Abs. 2 Richtlinie 2014/41/EU).

Da ein grenzüberschreitender Direktzugriff der Strafverfolgungsbehörden dabei auf die Kooperation der Anbieter angewiesen ist und diese von ausländischen Strafverfolgungsbehörden nicht unmittelbar (nur mittelbar über das Rechtshilfeverfahren) zur Mithilfe verpflichtet werden können, findet die Debatte in diesem Bereich weniger anhand tatsächlicher Fälle in Rechtsprechung und Literatur, sondern vor allem auf rechtspolitischer Ebene statt.

Der Fall »Microsoft Ireland«

Insbesondere in der internationalen Debatte prominent ist der Fall »Microsoft Ireland«. In diesem Fall verlangte das FBI von Microsoft die Herausgabe von E-Mail-Daten. Microsoft verweigerte die Herausgabe mit der Begründung, die fraglichen E-Mails wären auf Datenträgern in Irland und damit außerhalb des US-Hoheitsgebietes gespeichert. Der Beschluss zur Herausgabe könne nicht auf diese im Ausland gespeicherten E-Mails erstreckt werden. Außerdem würde eine Herausgabe die in Irland geltenden Datenschutzgesetze verletzen (vgl. Jansen 2018).

CLOUD-Act, E-Evidence-VO und zweites Zusatzprotokoll zur Cybercrime Convention

Nicht zuletzt der beschriebene Fall »Microsoft Ireland« führte dazu, dass in den USA mittlerweile der sogenannte CLOUD-Act erlassen wurde. Dieser gewährt US-amerikanischen Strafverfolgungsbehörden ausdrücklich Zugriff auf die Daten von in den USA ansässigen Unternehmen auch dann, wenn diese Daten auf Datenträgern im Ausland gespeichert sind (vgl. Rath/Spies 2018). In der Europäischen Union wird seit längerer Zeit über die sogenannte E-Evidence-VO verhandelt, die europäischen Strafverfolgungsbehörden Direktzugriff auf die Daten von Telekommunikations- und Telemediendienstanbietern verschaffen soll, auch wenn die Daten im (aus Sicht der jeweiligen Strafverfolgungsbehörde) europäischen Ausland gespeichert sind (vgl. Hamel 2020). Im Zuge dessen wird auch mit den USA über ein ergänzendes völkerrechtliches Abkommen verhandelt, das den US-amerikanischen und europäischen Strafverfolgungsbehörden wechselseitigen Direktzugriff ermöglichen soll (vgl. Moechel 2021). Schließlich soll auch die bereits oben genannte Cybercrime Convention um ein zweites Zusatzprotokoll ergänzt werden. Dieses Protokoll, das Ende 2021 vom Komitee der Minister*innen der beteiligten Staaten verabschiedet und im Mai 2022 unterschriftsreif wurde, enthält u.a. Regelungen zum Direktzugriff auf Daten von sogenannten Domain Name Services (v.a. IP-Adressen von Webseiten und weitere Informationen über Webseitenbetreiber) und auf Bestandsdaten von Telekommunikations- und Telemediendiensten (s. Art. 6 und 7 des zweiten Zusatzprotokolls). Die Verhandlungen über derartige Regulierungen und Abkommen zeigen einmal mehr, dass die einzelnen Nationalstaaten die Souveränität über auf ihrem Hoheitsgebiet gespeicherte Daten prinzipiell einfordern und diese zum Gegenstand von Verhandlungen mit anderen Staaten machen. In der Debatte über beide Regelungen (CLOUD-Act und E-Evidence-VO) sowie das flankie-

rende völkerrechtliche Abkommen zwischen den EU-Mitgliedstaaten und den USA wird von der Literatur indes zu Recht kritisiert, dass der Schutz der personenbezogenen Daten der betroffenen Bürger*innen und damit der Schutz der digitalen Grund- und Menschenrechte zu wenig thematisiert und problematisiert werde (vgl. von Galen 2020).

2.4 Zugriff auf private informationstechnische Systeme

Für transnationale Zugriffe auf private informationstechnische Systeme – vor allem im Wege der elektronischen Durchsicht nach § 110 Abs. 3 StPO – existiert nur eine sehr begrenzte Regelung in der Cybercrime Convention. Nach Art. 32 lit. b der Konvention ist für den Zugriff auf solche Daten die freiwillige und rechtmäßige Einwilligung derjenigen Person erforderlich, die berechtigt ist, die Daten abzurufen und weiterzugeben. Diese Regelung ist damit auf Fälle beschränkt, in denen der*die Berechtigte die Daten freiwillig an die Ermittlungsbehörden herausgibt. Im Umkehrschluss ergibt sich, dass – zumindest von den Unterzeichnerstaaten der Konvention – der Zugriff ohne diese Zustimmung des*der Berechtigten auf Daten im Ausland, sowohl per elektronischer Durchsicht als auch per Online-Durchsuchung, einen Eingriff in die Souveränität des ausländischen Staates darstellt.

Strafprozessuale Zulässigkeit des Zugriffs auf Daten, die (möglicherweise) im Ausland liegen

Über die strafprozessuale Zulässigkeit für transnationale Zugriffe auf Daten in privaten informationstechnischen Systemen herrscht daher Streit, welcher sich bislang vor allem um die Souveränitätsverletzung und ihre Folgen dreht. Klar ist zunächst, dass weder § 110 Abs. 3 StPO noch § 100b StPO den Zugriff auch auf im Ausland lagernde Datenbestände explizit erlaubt. Dies wäre auch gar nicht möglich bzw. eine entsprechende Erlaubnis – unter Annahme einer fremden Datensouveränität – im Verhältnis zum betroffenen ausländischen Staat nach allgemeinen Regeln des Völkerrechts unwirksam (vgl. Brodowski 2021).

Gestritten wird jedoch darüber, ob ein etwaiger Souveränitätsverstoß überhaupt – und wenn ja, unter welchen Umständen – Einfluss auf die Rechtmäßigkeit einer Maßnahme nach Maßstäben der deutschen Strafprozessordnung hat. Teilweise wird hier vertreten, dass die Maßnahme rechtmäßig ist, solange die Ermittlungshandlung im Inland stattfindet (vgl. Wicker 2013a). Die Gegenauffassung geht jedoch davon aus, dass in jedem

Zugriff auf ausländische Daten – unabhängig davon, ob der Zugriff bewusst (also in Kenntnis der ausländischen Belegenheit der zu erhebenden Daten) oder unbewusst erfolge – eine Souveränitätsverletzung liege, die zur Rechtswidrigkeit der Maßnahme auch nach deutschem Strafprozessrecht führe (vgl. Brodowski 2021). Schließlich wird teilweise danach differenziert, ob die Strafverfolgungsbehörden positiv wissen (vgl. Köhler 2021), dass sich die Daten im Ausland befinden (dann rechtswidrig) oder nicht (dann rechtmäßig).

Rechtsfolge: Beweisverwertungsverbot nur bei Rüge des betroffenen Staates

Die Frage, ob aus einer rechtswidrigen Beweisgewinnung wegen Verletzung der Souveränität eines ausländischen Staates ein Beweisverwertungsverbot entspringt, richtet sich nach deutschem Strafprozessrecht und somit in der Praxis nach der Abwägungslehre der Rechtsprechung (vgl. Hauschild 2014). Hiernach ist ein Beweisverwertungsverbot bei rechtswidriger Beweisgewinnung die Ausnahme, welche nur vorliegt, wenn eine Abwägung zwischen den (grundrechtlich geschützten) Interessen des*der Beschuldigten und dem staatlichen Strafanspruch ergibt, dass die Interessen des*der Beschuldigten im jeweiligen Einzelfall überwiegen (vgl. BGH 2007). Dies soll nach herrschender Meinung in den Fällen der Souveränitätsverletzung grundsätzlich nur der Fall sein, wenn der ausländische Staat der Verwertung der erlangten Beweismittel widerspricht (vgl. Bär 2011). Auch hier zeigt sich also die »Souveränitätszentrierung« der bisherigen Debatte um transnationale Dateneingriffe, wenn primär auf die Interessen des ausländischen Staates und nicht auf diejenigen des*der betroffenen Grundrechtsträger*in abgestellt wird.

3. Plädoyer für eine Verschiebung der Debatte weg von Souveränitätsüberlegungen hin zu einem Fokus auf Grund- und Menschenrechtsschutz

Nach unserer Auffassung erscheint die Fokussierung der Debatte um strafprozessuale transnationale Dateneingriffe auf Souveränitätsaspekte als verfehlt. Notwendig ist eine Verschiebung des Diskurses hin zu Fragen des Schutzes der digitalen Integrität der von der Datenerhebung betroffenen Menschen durch die Grund- und Menschenrechte. Es sprechen bereits grundlegende Erwägungen gegen eine Anwendung der traditionellen Vorstellungen und Konzepte staatlicher Souveränität auf Daten. Außerdem übersieht eine souveränitätsfokussierte Debatte, dass die eigentlich von der jeweiligen transnatio-

nalen Ermittlungsmaßnahme Betroffenen nicht die Nationalstaaten, sondern die betroffenen Bürger*innen sind. Bei der Erhebung und Verwertung personenbezogener Daten durch ausländische Strafverfolgungsbehörden sind nicht unmittelbar staatliche Interessen bedroht, sondern – sofern es nicht hinreichende Schutzkonzepte hierfür gibt – die grund- und menschenrechtlich geschützten Positionen und Interessen derjenigen, die vom ausländischen Staat ausgeforscht werden. Gerade im Hinblick auf das Konzept der gegenseitigen Anerkennung, wie es z.B. der E-Evidence-VO der EU zugrunde liegt, und die zunehmende Kooperation auch mit Staaten, deren Verständnis von Rechtsstaatlichkeit sich nicht mit demjenigen hierzulande deckt, besteht hier eine ernstzunehmende Bedrohungslage.

3.1 Grundlegende Bedenken gegen die Anwendung des traditionellen juristischen Souveränitätskonzepts auf digitale Daten und deren Speicherung/Übertragung

Bereits die Grundannahme, dass Nationalstaaten überhaupt Souveränität »über« Daten ausüben können, ist gewichtigen Bedenken ausgesetzt (s. hierzu auch den Beitrag von Fritzsche 2022 in diesem Band, dort insbesondere Kap. 3.). So hat die technische Entwicklung dazu geführt, dass es bereits schwierig ist, den »Ort« von Daten zu bestimmen. Zwar kann zu einem bestimmten Zeitpunkt theoretisch (praktisch ist hierfür ein uneingeschränkter physischer Zugriff auf den Datenträger notwendig) der genaue Belegenheitsort der Bits und Bytes bestimmt werden, welche die Daten physisch repräsentieren. Allerdings ist dies nur möglich, wenn die Ermittlungsbehörden zu diesem Zeitpunkt physischen Zugang zum Datenträger haben, auf dem die Bits und Bytes gespeichert sind. Für die hier beschriebenen, praktisch relevanten Konstellationen des grenzüberschreitenden Datenzugriffs ist dies dagegen technisch nur schwierig, in manchen Konstellationen gar nicht möglich (vgl. Bruns 2019). In diesen Konstellationen des »Fernzugriffs« ist zu berücksichtigen, dass viele Dienstleister, insbesondere im Bereich des Cloud-Computings, die Daten ihrer Kundinnen und Kunden nicht mehr zwingend an einem festen Ort speichern. Sowohl partielle Speicherung von Daten eines »Datensatzes« (z.B. eines Cloud-Speichers oder eines E-Mail-Kontos) auf verschiedenen Servern, die in verschiedenen Ländern stehen können, als auch der »Umzug« von Daten in zeitlichen Intervallen und teilweise über Ländergrenzen hinweg sind aus wirtschaftlichen Gründen nicht unüblich. Viele Dienstleister legen nicht offen, wo sie die Daten ihrer Kundinnen und Kunden speichern (vgl. Bruns 2019). Diese Vorgänge machen die exakte »Lokalisierung« von Daten bei

Fernzugriffen derart komplex, dass es in der Praxis kaum möglich erscheint, im entscheidenden Moment des Zugriffs eine Verletzung der Souveränität durch den Zugriff »auf« fremdem Hoheitsgebiet auszuschließen oder positiv festzustellen (vgl. Wicker 2013b).

Diese Überlegungen führen auch zu einem normativen Argument gegen die Anwendung traditioneller Souveränitätskonzepte auf Daten: Der Idee der Souveränität liegt der Gedanke der ausschließlichen Herrschaft oder Entscheidungsgewalt zugrunde (vgl. Bergmann 2014; s. zur Dekonstruktion des Konzepts der »absoluten« Souveränität die Einleitung dieses Bandes von Glasze/Odzuck/Staples 2022, dort insbesondere Kap. 3.). Der eigentliche Wert von Daten liegt nicht in den Bits und Bytes, denen ein physischer Standort (theoretisch, s.o.) zugewiesen werden kann, sondern in den Informationen, welche die Daten enthalten. In zunehmendem Maße und gerade bei Cloud-Lösungen existieren jedoch von Datensätzen mehrere Kopien (sog. Back-ups) an verschiedenen Speicherorten (nicht nur bei dem*der Nutzer*in selbst, also auf dessen*deren lokalen Speichergeräten, sondern auch bei den Cloud-Dienstleistern, um Datenverlust vorzubeugen). Damit lässt sich jedoch der exakte Ort der wertentscheidenden Information eigentlich gar nicht bestimmen, was das Konzept der Souveränität über Daten (eigentlich über die Information in den Daten) grundsätzlich infrage stellt. Dem zugrunde liegt das Problem, dass Souveränität bislang nur anhand von dinglichen Bezugsgegenständen gedacht wurde (s. hierzu auch mit historischen Bezügen Fritzsche 2022): Staatsvolk und Staatsgebiet (inklusive aller dinglichen Gegenstände, die sich auf dem Staatsgebiet befinden bzw. im Falle von Menschen aufhalten). Die Information bzw. das Wissen, um das es bei Souveränität über Daten eigentlich geht (s.o.), ist jedoch gerade nicht dinglich. Denkbar wäre es allenfalls, das Souveränitätskonzept an Rechten bezüglich der Information/des Wissens anzuknüpfen, wie wir das von Immaterialgüterrechten u.Ä. kennen (s. hierzu noch Teil II). Dabei geht es dann aber um die Frage, welche natürliche oder juristische Person das Recht hat, die Information (ausschließlich) zu kennen/zu nutzen und über ihre Verbreitung zu entscheiden. Dieses Recht steht jedoch in unserer Eigentums- und Rechtsordnung (s. dazu ebenfalls noch Teil II) – mit Ausnahme von Staatsgeheimnissen (vgl. Safferling/Rückert 2020) – gerade nicht dem Staat, sondern den einzelnen Grundrechtsträger*innen zu. Damit ist beim Schutz dieser Rechte nicht die »digitale Souveränität« des Staates, sondern die digitale Integrität des Individuums betroffen. Und deren Schutz ist Sache der Grund- und Menschenrechte.

3.2 Garantie der digitalen Integrität durch Grund- und Menschenrechte (Überblick)

Die digitale Integrität der Bürger*innen wird mittlerweile sowohl auf deutscher als auch auf europäischer Ebene durch Grund- und Menschenrechte geschützt. Die Grund- und Menschenrechte der Europäischen Menschenrechtskonvention (EMRK) und der Grundrechtecharta der EU (GRC) setzen dabei im Bereich strafprozessualer Dateneingriffe den Mindeststandard, konkrete Vorgaben für Schaffung und Anwendung der Dateneingriffsbefugnisse der Strafprozessordnung machen dagegen die »digitalen« Grundrechte des Grundgesetzes.

Das Schutzkonzept des Grundgesetzes

Im deutschen Grundgesetz ruht der umfassende Schutz der digitalen Integrität der Bürger*innen vornehmlich auf drei Säulen. Die Integrität der Telekommunikationsinfrastruktur und die Vertraulichkeit der Kommunikationsinhalte und -umstände werden umfassend durch das Telekommunikationsgeheimnis in Art. 10 Abs. 1 Var. 3 GG geschützt (vgl. BVerfG 2008 [120]). Der Schutzbereich ist dabei am Akt der Telekommunikation orientiert und schützt inhaltsunabhängig jede Form der elektronischen und digitalen Fernkommunikation (z.B. klassische Sprachtelefonie, E-Mails, Messengerdienste, Voice-over-IP-Telefonie etc.), es handelt sich mithin um einen Schutz der Systeme der Fernkommunikation (vgl. ebd.). Ebenfalls systemorientiert ist der Schutz der informationstechnischen Systeme selbst ausgestaltet: Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, welches das Bundesverfassungsgericht 2008 aus dem Allgemeinen Persönlichkeitsrecht in Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG hergeleitet hat, schützt sowohl die von Bürger*innen genutzten Systeme – inklusive vernetzter Systeme wie Cloud-Speicher (vgl. BVerfG 2016 [141]) – vor dem Zugriff des Staates (systembezogener Integritätsschutz) als auch die auf solchen Systemen verarbeiteten Daten vor einer Erhebung und Kenntnisnahme (systembezogener Vertraulichkeitsschutz; vgl. BVerfG 2008 [120]). Schließlich gewährt das Recht auf informationelle Selbstbestimmung – ebenfalls aus dem Allgemeinen Persönlichkeitsrecht nach Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG hergeleitet (vgl. BVerfG 1983 [65]) einen – systemunabhängigen – inhaltsorientierten Schutz aller personenbezogenen Daten (datenbezogener Vertraulichkeitsschutz).

Das Schutzkonzept von EMRK und GRC

Auf europäischer Ebene wird der grund- und menschenrechtliche Datenschutz von EMRK und GRC abweichend von der Konzeption des Grundgesetzes ausgestaltet. In der EMRK findet sich mit Art. 8 lediglich eine Vorschrift zum Schutz des Privatlebens. Diese umfasst dabei neben dem Recht auf informationelle Selbstbestimmung auch das Recht auf Vertraulichkeit der individuellen Kommunikation (vgl. EGMR 2015). In der GRC schützt Art. 7 ausdrücklich die Kommunikation, wobei hierbei ebenfalls nur die Individualkommunikation (wie z.B. Sprachtelefonie, E-Mails) und nicht die Massenkommunikation (z.B. Rundfunk) gemeint ist. Ebenfalls von Art. 7 GRC umfasst ist der Schutz des Privatlebens, welcher auch die informationelle Selbstbestimmung umfasst (vgl. EuGH 2014). Hierbei kommt es zu Schutzbereichsüberschneidungen mit dem spezielleren Art. 8 GRC, in dem explizit ein Grundrecht auf Schutz der personenbezogenen Daten geregelt ist. Erfasst wird dabei jede Art der Datenverarbeitung – von der Erhebung über die Auswertung bis hin zu der Speicherung und Übermittlung von Daten (vgl. Jarass 2021). Ein spezielles Grund- oder Menschenrecht zum Schutz von informationstechnischen Systemen gibt es dagegen auf europäischer Ebene bislang nicht.

Verhältnis von Grundgesetz zu EMRK und GRC im Bereich strafprozessualer Dateneingriffe

Das Verhältnis zwischen dem digitalen Grundrechtsschutz auf nationaler Ebene und dem digitalen Grund- und Menschenrechtsschutz auf europäischer Ebene lässt sich für den Bereich strafprozessualer Dateneingriffe vereinfacht wie folgt beschreiben: Während EMRK und GRC verbindliche Mindeststandards vorgeben, ist primärer Prüfungsmaßstab für deutsche Eingriffsbefugnisse weiterhin das Grundgesetz. Der Grund hierfür liegt in der aktuellen Rechtsprechung des Bundesverfassungsgerichts in den Entscheidungen »Recht auf Vergessen I + II« und »Europäischer Haftbefehl III«. Ausgangspunkt ist, dass durch die Datenschutzrichtlinie 2016/680/EU nunmehr sämtliche Datenverarbeitungen durch Strafverfolgungsbehörden innerhalb der EU den Mindeststandards der Richtlinie entsprechen müssen. Nach den sehr extensiven Kriterien der Rechtsprechung des Europäischen Gerichtshofs zur Frage, wann es sich um eine »Durchführung von Unionsrecht« i.S.v. Art. 51 Abs. 1 GRC (Voraussetzung zur Anwendung der Grundrechte der Charta) durch die Mitgliedstaaten handelt (vgl. Safferling 2014), ist demnach

nunmehr (wohl) jede Datenverarbeitung durch Strafverfolgungsbehörden eine »Durchführung von Unionsrecht« (vgl. Safferling/Rückert 2021). Da auch die Menschenrechte der EMRK über die »Brücken« des Art. 6 Abs. 3 EUV und Art. 52 Abs. 3 GRC zumindest faktisch als Grundrechte in der EU gelten, ist hier auch die EMRK anwendbar und steht nicht nur – wie sonst bei der Rechtsanwendung in Deutschland – im Rang eines einfachen Bundesgesetzes, sondern ranggleich mit den Grundrechten der GRC und damit über der deutschen Strafprozessordnung (vgl. Rückert 2020a). Allerdings wendet das BVerfG auch bei der Durchführung von Unionsrecht weiterhin primär die Grundrechte des Grundgesetzes an, wenn die europäischen Rechtsvorgaben dem deutschen Gesetzgeber einen echten Umsetzungsspielraum belassen und der deutsche Grundrechtsschutz dem Schutz aus GRC und EMRK mindestens gleichkommt (vgl. BVerfG 2020a, 2020b, 2021). Die allermeisten Vorgaben der Richtlinie 2016/680/EU – und vor allem diejenigen, die für alle Datenverarbeitungsvorgänge gelten – sind nur Mindestvorgaben, häufig lediglich sehr abstrakter Natur (z.B. Datenverarbeitung nach »Treu und Glauben«) und in aller Regel durch den nationalen Gesetzgeber ausfüllungsbedürftig. Dementsprechend kommt GRC und EMRK in diesem Bereich »nur« die Funktion zu, verbindliche Mindestvorgaben für den Schutz vor strafprozessualen Dateneingriffen zu machen (vgl. Safferling/Rückert 2021; Rückert 2020a).

3.3 Bedrohung der Garantie des Schutzes durch Grund- und Menschenrechte durch strafprozessuale transnationale Dateneingriffe

Aus einer grund- und menschenrechtlichen Perspektive macht es für die Betroffenen wenig Unterschied, ob die Dateneingriffe von demjenigen Nationalstaat, in dem sie leben, oder einem fremden Nationalstaat ausgehen. Ein Unterschied ergibt sich zwar grundsätzlich hinsichtlich der konkreten (nachteiligen) Rechtsfolgen für die Betroffenen: Die Gefahr eines strafrechtlichen Ermittlungsverfahrens und die Verhängung von Freiheits- oder Geldstrafen als typische Folgen strafprozessualer Ermittlungen stellen sich zwar auf den ersten Blick nur bei Dateneingriffen des Heimatstaates. Nicht aus dem Blick geraten darf aber, dass vor dem Hintergrund von Auslieferungsersuchen (s. §§ 3 Abs. 1, 78ff. IRG für die EU), internationalen Haftbefehlen (s. §§ 17ff., 21ff. IRG) oder der Zugriffsmöglichkeit bei Ein- oder Durchreise in den zugreifenden Staat heute auch die Strafverfolgung im ausländischen Staat ein reales Risiko darstellt (vgl. Safferling 2021). Überdies findet nicht selten eine Durchmischung strafverfolgender und geheimdienstlicher Interessen und Tätigkeiten

bei der Ausforschung im Ausland lebender Staatsbürger*innen statt. Eine besondere Bedeutung kommt hier der Ausforschung von Exilant*innen, Dissident*innen und Asylsuchenden zu (vgl. Safferling/Rückert 2020).

Für innerstaatliche strafprozessuale Dateneingriffe enthalten die Eingriffsbefugnisse der deutschen Strafprozessordnung dabei zahlreiche Eingriffsschwellen und Schutzmechanismen – wie z.B. Straftatenkataloge, Anforderungen an den Grad des Tatverdachts, Subsidiaritätsklauseln, Beschränkungen hinsichtlich des Adressat*innenkreises, Richter*innenvorbehalte, Benachrichtigungs- und Mitteilungspflichten –, welche das Bundesverfassungsgericht aus den einschlägigen Grundrechten des Grundgesetzes herleitet (vgl. Bode 2012; Schwabenbauer 2013; Hauck 2014; Tanneberger 2014, jeweils mit weiteren Nachweisen aus der Rechtsprechung des Bundesverfassungsgerichts). Für Zugriffe deutscher Strafverfolgungsbehörden auf Daten im Ausland ist außerdem vor Kurzem vom Bundesverfassungsgericht klargestellt worden, dass die deutsche Staatsgewalt und damit ebenso die deutschen Strafverfolgungsbehörden auch bei Handeln im Ausland an die Grundrechte des deutschen Grundgesetzes gebunden sind (vgl. BVerfG 2020c; Schmahl 2020). Umgekehrt ergeben sich aus den »digitalen« Grundrechten auch Schutzpflichten für den Staat zugunsten der Grundrechtsträger*innen (auch zugunsten von Asylsuchenden, Exilant*innen, Dissident*innen usw., vgl. Safferling/Rückert 2020) gegen Eingriffe von fremden Staaten in deren Grundrechte (vgl. Durner 2021). Dieser Schutz der digitalen Integrität erlangt gerade dann besondere Bedeutung, wenn es sich bei den zugreifenden ausländischen Staaten um solche handelt, deren Rechtsstaatlichkeitsniveau rechtlich oder faktisch nicht mit demjenigen Deutschlands zu vergleichen ist.

4. Conclusio: Verschiebung der Debatte weg von Souveränitätsüberlegungen hin zur Garantie von Grund- und Menschenrechten auch bei transnationalen Dateneingriffen

Wir haben gezeigt, dass grundlegende Bedenken gegen eine Übertragung des traditionellen Konzepts der staatlichen Souveränität – wie sie vom derzeitigen juristischen Diskurs weitgehend ohne Problembewusstsein vorgenommen wird – auf Datenbestände »auf« dem Hoheitsgebiet eines Staates sprechen. Gleichzeitig sind die digitalen Grund- und Menschenrechte der von Dateneingriffen betroffenen Grundrechtsträger*innen bei transnationalen Dateneingriffen in ähnlichem Maße bedroht wie bei innerstaatlichen strafprozessualen Ermittlungen. Nicht zuletzt aufgrund der extraterritorialen

Geltung der deutschen Grundrechte und der aus den Grund- und Menschenrechten erwachsenden Schutzpflichten des Staates gegenüber seinen Bürger*innen, aber auch Asylsuchenden, Exilant*innen und Dissident*innen aus anderen Staaten, ist daher eine Neufokussierung des Diskurses weg von einer klassischen Souveränitätsdebatte hin zu einem Diskurs über die notwendigen Mechanismen und Regelungen nötig, um den Schutz der digitalen Grund- und Menschenrechte auch bei transnationalen strafprozessualen Dateneingriffen zu garantieren.

4.1 Rechtspolitische Erwägungen zur E-Evidence-VO und zu den Verhandlungen mit Drittstaaten (CLOUD-Act, Zweites Zusatzprotokoll zur Cybercrime Convention)

Für die rechtspolitische Debatte um Regelungen für den Direktzugriff von nationalen Strafverfolgungsbehörden auf Datenbestände von Telekommunikations- und Telemedienprovidern – wie beispielsweise die E-Evidence-VO der EU, dem zweiten Zusatzprotokoll zur Cybercrime Convention oder die Verhandlungen über ein die VO ergänzendes völkerrechtliches Abkommen mit den USA – bedeutet dies folgendes:

Derartige Regelungen und Übereinkommen sollten ausschließlich mit solchen Staaten getroffen werden, die ein vergleichbares grund- und menschenrechtliches sowie rechtsstaatliches Niveau aufweisen, wie dies in Deutschland der Fall ist. Dabei ist nicht nur die Lage »auf dem Papier« zu betrachten, sondern welche Rolle die Grund- und Menschenrechte in der Praxis der Strafverfolgung im jeweiligen Land spielen. So sind beispielsweise durchaus Zweifel angebracht, ob Polen oder Ungarn derzeit tatsächlich ein vergleichbares Schutzniveau aufweisen (vgl. Oberlandesgericht Karlsruhe 2020; Diel-Gligor 2021). Außerdem müssen die aus den Grundrechten fließenden Eingriffsschwellen und Schutzmechanismen auch bei transnationalen Dateneingriffen Geltung beanspruchen. Zur Gewährleistung der Einhaltung dieser Mechanismen ist weiterhin die Gewährleistung von effektiven Rechtsschutzmöglichkeiten notwendig. Bei heimlichen Maßnahmen muss daher auch eine nachträgliche Benachrichtigung – wie z.B. in § 101 StPO – der Betroffenen gewährleistet sein, damit diese Rechtsschutz in Anspruch nehmen können. Zur Gewährleistung der Beachtung rechtsstaatlicher Grundsätze und zur Wahrung der Grund- und Menschenrechte des*der Betroffenen ist schließlich eine Informationspflicht zugunsten der nationalen Datenschutzbehörden zu erwägen.

4.2 Maßstab für die Rechtmäßigkeit von strafprozessualen transnationalen Dateneingriffen (inklusive Beweisverwertungsverbote)

Bei der Frage des Durchschlagens einer etwaigen Völkerrechtswidrigkeit auf die Rechtmäßigkeit nach deutschem Strafverfahrensrecht sollte intensiv diskutiert werden, ob bei einem transnationalen Dateneingriff überhaupt eine Souveränitätsverletzung vorliegt (s. Argumente oben) und – falls ja – ob diese einen Einfluss auf die Rechtmäßigkeit nach deutschem Strafverfahrensrecht hat. Es ließe sich hier auch gut vertreten, dass aufgrund der Unterschiedlichkeit der beteiligten Subjekte und Verhältnisse im Völkerrecht (Staat – Staat) und im Strafverfahrensrecht (Staat – Bürger*in) ein Durchschlagen zu verneinen ist. Für die Rechtmäßigkeit bei transnationalen Datenzugriffen im Verhältnis ausländischer Staat – Bürger*in muss vielmehr entscheidend sein, dass die Grund- und Menschenrechte der betroffenen Bürger*innen gewährleistet sind. Im Falle Deutschlands bedeutet dies, dass die Vorgaben, Eingriffsschwellen und Schutzmechanismen aus den oben beschriebenen digitalen Grundrechten des Grundgesetzes und den Grund- und Menschenrechten der EMRK und der GRC beachtet werden.

Teil II: »Digitale Souveränität« und Privatrecht

1. Digitalgesellschaft als Herausforderung für die Privatrechtsgesellschaft

1.1 Privatrechtsgesellschaft

Das Privatrecht beschäftigt sich mit den rechtlichen Beziehungen der Privatrechtssubjekte untereinander. Anders als im öffentlichen Recht geht es – wie in der Einleitung schon aufgezeigt – nicht um das Verhältnis des Staates zu seinen Bürger*innen oder gar um das Verhältnis souveräner Staaten untereinander, sondern um die Rechtsverhältnisse zwischen den einzelnen gleichgeordneten Mitgliedern der Gemeinschaft (vgl. Brox/Walker 2020: § 1 Rn. 10). Das Privatrecht basiert auf den Ideen individueller Freiheit und Selbstbestimmung (vgl. näher Grigoleit 2008; Riesenhuber 2009: 4ff.). Freie, rechtlich gleiche Bürger*innen gestalten in der Privatrechtsgesellschaft (vgl. Böhm 1966: 75) ihre Beziehungen untereinander nach Maßgabe ihrer individuellen Vorstellungen ohne staatliche Bevormundung eigenverantwortlich aus. Interessengegensätze

werden durch Verhandlungen ausgeglichen. Das Privatrecht vertraut darauf, dass der*die Einzelne selbst am besten weiß, wie er*sie seine*ihre Verhältnisse zu Dritten regeln möchte. Dezentralen Lösungen wird der Vorzug vor zentraler Steuerung eingeräumt. Zugleich liegt dem Privatrecht die Einsicht zugrunde, dass Individuen in der Lage sind, die Konsequenzen ihres Handelns selbst einzuschätzen. Selbst in ihrer Rolle als Verbraucher*innen werden Private als verantwortlich handelnde Personen verstanden. Es besteht das Leitbild eines*einer durchschnittlich informierten, situationsadäquat aufmerksamen und verständigen Verbraucher*in (vgl. Bornkamm/Feddersen 2021: § 5 Rn. 1.76; s. auch Erwägungsgrund 18 RL 2005/29/EG [UGP-RL]).

Rechtlich wird dies über die Privatautonomie abgesichert (zur Privatautonomie vgl. Flume 1975: § 1; Petersen 2011; Brehm 2008: § 5 Rn. 82ff.). Der*die Einzelne kann im Grundsatz seine*ihre Rechtsbeziehungen zu anderen durch Rechtsgeschäft (Verträge) frei gestalten (vgl. Köhler 2017: § 5 Rn. 1). Es gilt die Vertragsfreiheit mit den Kerninhalten Abschlussfreiheit (das Ob eines Vertragsschlusses liegt grundsätzlich in den Händen der Privatrechtssubjekte genauso wie die Wahl des*der Vertragspartner*in), Inhaltsfreiheit (der Inhalt des Rechtsgeschäfts kann im Ausgangspunkt frei ausgehandelt werden) und Formfreiheit (im Grundsatz ist rechtsgeschäftliches Handeln formfrei) (vgl. Brox/Walker 2020: § 2 Rn. 5; Medicus/Lorenz 2015: § 9 Rn. 61ff.). Durch zwei übereinstimmende Willenserklärungen gestalten die Parteien ihre Verhältnisse zueinander frei aus (»Konsensprinzip«; vgl. Brehm 2008: § 1 Rn. 5, § 5 Rn. 84; s. § 311 Abs. 1 BGB). Die Parteien müssen sich an ihren Erklärungen festhalten lassen (*pacta sunt servanda*, s. § 145 BGB). Die Gestaltung der Rechtsverhältnisse durch die*den Einzelne*n nach ihrem*seinem Willen ist ein Teil der allgemeinen Handlungsfreiheit (s. Art. 2 I GG) und damit verfassungsrechtlich abgesichert (vgl. BVerfG 1994; Medicus/Lorenz 2015: § 9 Rn. 66f.).

Private Eigentumsrechte unterstützen dieses System dezentralen Wirtschaftens (»Eigentumsfreiheit«; vgl. Köhler 2017: § 3 Rn. 8; zur Verknüpfung mit dem Souveränitätsbegriff Schuppert 2019: 242f.). Eigentumsrechte an Sachen in Form von Ausschließlichkeitsrechten (s. § 903 BGB als »Prototyp«; zur Struktur von Ausschließlichkeitsrechten Hofmann 2020a: 9 u. 12ff.) gewähren nicht nur einen Raum zur Verwirklichung individueller Freiheit, sondern sorgen dafür, dass über die Güterverteilung dezentral durch Verträge entschieden werden muss. Zugleich bestehen Anreize, in den Erhalt abnutzbarer Güter zu investieren. Eigentumsrechte an immateriellen Gütern (Patentrechte, Urheberrechte etc.) schaffen nicht nur Anreize zur Schöpfung unkörperli-

cher Gegenstände, sondern sie sind auch Grundlage für deren Verwertung, beispielsweise durch die Kulturindustrie. Im Übrigen werden durch die Zuweisung derartiger Ausschließlichkeitsrechte (zudem existieren Rechte zum Schutz der Persönlichkeit) die Freiheitssphären untereinander abgegrenzt. Resultieren Schäden aus Eingriffen in derartige Rechte Dritter, besteht eine Verpflichtung zum Schadensersatz, regelmäßig aber nur unter der Voraussetzung der Verletzung einer Verhaltenspflicht (»Verkehrspflicht«). Per se gefährliche Tätigkeiten sind mitunter im Grundsatz erlaubt, verpflichten aber verschuldensunabhängig zum Schadensersatz im Falle der Verletzung Rechter Dritter (Gefährungshaftung). Anderweitige Ausgestaltungen durch Verträge sind im Grundsatz aber möglich.

Für die Durchsetzung seiner Rechte ist das Privatrechtssubjekt ebenfalls selbst zuständig. Auch wenn der*die Einzelne hierbei auf staatliche Hilfe angewiesen ist, hängt die Rechtsdurchsetzung von seiner*ihrer Initiative ab. Statt kollektiver Rechtsdurchsetzung liegt es grundsätzlich in der Hand des*der Gläubiger*in, seinen*ihren Anspruch selbst zu verwirklichen (vgl. Zech 2012: 66; Brehm 2008: § 20 Rn. 608). Das subjektive Recht ist einer der zentralen Begriffe des Privatrechts (vgl. von Tuhr 1957: § 1 I, S. 53). Subjektive Rechte als dem*der Einzelnen von der Rechtsordnung verliehene Willensmacht zur Durchsetzung seiner*ihrer Interessen (vgl. Raiser 1961) vermitteln individuelle Freiheit (vgl. Brox/Walker 2020: § 28 Rn. 12).

Die Rechtswirklichkeit steht diesen Idealvorstellungen vielfach entgegen. Faktisch treten sich Private regelmäßig nicht als »Gleiche unter Gleichen« gegenüber, sondern es bestehen gravierende Verhandlungsungleichgewichte – beispielsweise durch Informationsasymmetrien oder unterschiedliche Marktmacht (s. etwa zu den unterschiedlichen Machtverhältnissen in der Arbeitswelt den Beitrag von Sauer/Staples/Steinbach 2022 in diesem Band). Vor allem auf faktische Hindernisse für selbstbestimmtes Handeln reagiert das Privatrecht mit einer Vielzahl von Instrumenten (zu den »Grenzen der Privatautonomie« vgl. Paulus/Zenker 2001). Ziel ist es dabei zuallererst, die Voraussetzungen für selbstbestimmtes Handeln zu schaffen (vgl. Grigoleit 2008: 56ff.).

Dies kann beispielsweise dadurch abgesichert werden, dass bestimmte Normen als zwingend ausgestaltet sind (vgl. Köhler 2017: § 3 Rn. 23). Ein Abweichen durch Rechtsgeschäft ist nicht möglich. In diesem Sinne stehen die Mängelgewährleistungsrechte beim Verbrauchsgüterkauf gemäß § 476 BGB nicht zur Disposition der Parteien. Auch im Falle vorformulierter, im Massenverkehr einseitig gestellter allgemeiner Geschäftsbedingungen (AGB), also wiederum dort, wo real kein Verhandlungsgleichgewicht besteht, greift

das Recht ein (vgl. Köhler 2017: § 16 Rn. 1ff.): Überraschende Klauseln werden gemäß § 305c BGB von vornherein nicht Vertragsbestandteil. Die Klauseln müssen zudem einer »Inhaltskontrolle« standhalten. Selbst wenn der Gesetzgeber die Unangemessenheit einer bestimmten Abrede nicht über abstrakte Verbote (s. z.B. § 138 BGB) oder konkrete Kontrollvorschriften (s. §§ 308f. BGB) für nichtig erklärt, kann die Generalklausel aus § 307 Abs. 1 S. 1 BGB, wonach Bestimmungen in allgemeinen Geschäftsbedingungen unwirksam sind, wenn sie den*die Vertragspartner*in des*der Verwender*in entgegen den Geboten von Treu und Glauben unangemessen benachteiligen, Abhilfe schaffen. Formvorschriften, z.B. das Schriftformerfordernis oder gar die notarielle Beurkundung, erweisen sich als Warnungen vor überstürztem Handeln (vgl. Köhler 2017: § 12 Rn. 7). Während Widerrufsrechte den*die Verbraucher*in vor Entscheidungen schützen u.a. wenn diese*r situationsspezifisch zu einem unüberlegten Geschäftsabschluss gedrängt worden ist (s. § 312b BGB; vgl. Wendehorst 2019: § 312b Rn. 2), sollen diverse Informationspflichten (z.B. § 5a UWG; § 312d BGB) insbesondere Informationsasymmetrien ausgleichen und die Voraussetzung für selbstbestimmtes Handeln schaffen (vgl. Wendehorst 2019: § 312d Rn. 1f.; Alexander 2019: § 9 Rn. 572).

Mehr und mehr ist das Privatrecht schließlich für unerwünschte Ungleichbehandlungen (»Diskriminierung«) sensibilisiert. Bei Massengeschäften des täglichen Lebens (s. § 19 AGG), vor allem aber im Arbeitsrecht ist das allgemeine Gleichbehandlungsgesetz (AGG) zu beachten. Des Weiteren werden unfaire Geschäftspraktiken durch das Lauterkeitsrecht (UWG) in Schach gehalten. Das Kartellrecht versucht dafür zu sorgen, dass überhaupt Wettbewerb besteht. Bekämpft werden der Missbrauch einer marktbeherrschenden Stellung (s. Art. 102 AEUV) und wettbewerbsbeschränkende Vereinbarungen (s. Art. 101 AEUV). Eigentumsrechte unterliegen einer Vielzahl von »Schranken«, wodurch der Rechtskreis des*der Eigentümer*in, Urheber*in oder Patentinhaber*in zugunsten von Dritt- und Allgemeininteressen beschränkt wird (exemplarisch zum Urheberrecht vgl. Geiger 2004). Ferner müssen die Grundrechte auch im Privatrecht beachtet werden (»mittelbare Drittwirkung«; vgl. allgemein Brox/Walker 2020: § 2 Rn. 9ff.; zum Gleichheitssatz vgl. BVerfG 2018). In diesem Sinne lässt sich beispielsweise im Urheberrecht eine »Konstitutionalisierung« beobachten, wonach die private Eigentumsordnung ganz maßgeblich aus den europäischen Grundrechten heraus entwickelt wird (vgl. Leistner/Roder 2016). Nicht zuletzt darf die »Steuerungswirkung« des Privatrechts nicht unterschätzt oder gar übersehen werden (vgl. grundlegend Hellgardt 2016). Regulatorische Ziele werden vielfach über

das Privatrecht, beispielsweise mittels des Haftungsrechts über Pflichten zur Schadensvermeidung (indirekt statuiert durch die andernfalls drohende Haftung auf Schadenersatz), verwirklicht (zu »autonomen Systemen« vgl. Wagner 2017). Die regulatorische Überformung des Privatrechts (nicht nur im Verbraucherschutzrecht, sondern auch im Wirtschaftsrecht) wird auch als »Veröffentlichrechtlichung« bezeichnet.

1.2 Digitalgesellschaft

Die Digitalisierung fordert dieses Privatrechtsverständnis in vielfacher Hinsicht heraus. Auch wenn nicht oft genug betont werden kann, dass sich die Grundideen des Privatrechts seit jeher in einem Spannungsverhältnis zur Rechtswirklichkeit bewegen, lassen sich die mit der Digitalisierung einhergehenden Veränderungen nicht als bloße weitere graduelle Verschiebung abtun. Es sind hier gravierende Entwicklungen zu beobachten. Vier übergreifende Gefährdungen seien dabei besonders hervorgehoben.

Erstens wird die Prämisse des Privatrechts, wonach die Bürger*innen ihre Verhältnisse selbstbestimmt und eigenverantwortlich mit Dritten aushandeln, fundamental erschüttert. Die marktmächtigen Akteure der Digitalwirtschaft setzen die Bedingungen der Digitalgesellschaft, sodass für »Verhandlungen« regelmäßig kein Raum bleibt. Die Vertragsfreiheit besteht allem Anschein nach häufig nur noch auf dem Papier. Die Rechtsordnung einschließlich der Möglichkeiten der Rechtsdurchsetzung (»Meldeprotokolle« einschlägiger Internetdienste) erscheint mehr und mehr privatisiert. Die entpersonalisierten Strukturen der Plattformökonomie erschweren es dem*der Verbraucher*in vielfach, im Falle von Streitigkeiten (individuell) Abhilfe zu bekommen (vgl. Hofmann 2020c). All dies ist zwar nicht grundsätzlich neu, wird aber wie gesagt über die digitalen Möglichkeiten, allen voran die dadurch bedingte Plattformökonomie (zur Plattformökonomie aus Sicht des Privatrechts vgl. etwa Grünberger 2017; Tonner 2017; Busch 2019; Schweitzer 2019a; Busch/Dannemann/Schulte-Nölke 2020) mit wenigen marktmächtigen internationalen Internetkonzernen wie Amazon oder Google, erheblich verstärkt.

In der Plattformökonomie wirken sich zudem Rechtsbeziehungen Dritter verstärkt auf das traditionelle Zweipersonenverhältnis zwischen Gläubiger*in und Schuldner*in aus. Ein Anbieter von Musik wird im Verhältnis zu dem*der Endnutzer*in die Klauseln, die er mit den Inhaber*innen der Rechte an der Musik akzeptieren musste, an die Nutzer*innen weitergeben. Kurzum, statt Zweipersonenverhältnissen spielen »Netzwerke« eine zentrale Rolle (vgl. Grünberger 2018: 290ff.). Oder mit Grünberger: Der »Individualvertrags-

Fixierung« der klassischen Rechtsdogmatik werde es nicht gelingen, die Verbraucher*innenerwartungen in Netzwerken abzubilden (ebd.: 291). Dazu ein Beispiel: Über die Portabilitätsverordnung hat der europäische Gesetzgeber in diesem Sinne ein Konzept zur grenzüberschreitenden Portabilität von Online-Inhaltediensten eingeführt (zur Datenportabilität nach Art. 20 DSGVO vgl. Kühling/Martini 2016: 450), indem sichergestellt wird, dass die Abonnent*innen von portablen Online-Inhaltediensten, die in ihrem Wohnsitzmitgliedstaat rechtmäßig bereitgestellt werden, während eines vorübergehenden Aufenthalts in einem anderen Mitgliedstaat als ihrem Wohnsitzmitgliedstaat auf diese Dienste zugreifen und sie nutzen können (s. Art. 1 Portabilitäts-VO). Der Regulierungsbedarf folgte vor allem aus dem urheberrechtlichen Territorialitätsprinzip, das in den jeweiligen Vertragsbeziehungen wie angedeutet abgebildet wurde.

Zweitens wird wesentliche Infrastruktur (z.B. Suchmaschinen) ebenfalls von privater Seite zur Verfügung gestellt. Private Akteure gleichen nicht nur vermehrt staatlichen Akteuren, sondern übernehmen auch verstärkt deren Aufgaben. Dies gilt nicht zuletzt für die Durchsetzung subjektiver Rechte im Internet (»Privatisierung der Rechtsdurchsetzung«, vgl. Hofmann 2019: 1223). Der*die Einzelne muss auch tatsächlich die Möglichkeit haben, seine*ihre Individualrechte gegenüber marktmächtigen Privaten zu verwirklichen. Praktisch konnte dies schon daran scheitern, dass die Plattform nicht »greifbar« war. Um eine sichere Zustellung zu gewährleisten, sah sich der Gesetzgeber daher veranlasst, gemäß § 5 Netzwerkdurchsetzungsgesetz (NetzDG) einen »Zustellungsbevollmächtigten« zu verlangen (s. BR-Drs. 315/17: 25). Gefahr droht aber auch von einer überschießenden Durchsetzung: Während allen voran bei Persönlichkeitsrechtsverletzungen *(»hate speech«)* im virtuellen Raum gravierende Rechtsdurchsetzungsdefizite zu beklagen sind, könnte mit Blick auf bestimmte Wirtschaftsrechte das Gegenteil zu befürchten sein. Über technische Möglichkeiten (»Upload-Filter«; zu Filtertechnologien vgl. Raue/Steinebach 2020; zum UrhDaG vgl. Hofmann 2021) wird die Vision von hundertprozentiger Rechtsdurchsetzung plötzlich zur greifbaren Realität. Dass Recht aber auch einmal nicht durchgesetzt wird, ist von der Rechtsordnung eingepreist. Der fein austarierte Interessenausgleich kann so aus den Fugen geraten (vgl. Hofmann 2020d). In jedem Fall muss der Staat um seine Hoheitsansprüche kämpfen. Bestimmt er die Regeln der Plattformökonomie oder werden diese letztlich über die Nutzungsbedingungen der einschlägigen Plattformen von privater Seite unwiderruflich gesetzt (vgl. Schweitzer 2019a: 4ff.)? Der staatliche Regelungsanspruch (»Souveränität«) wird durch das uni-

verselle Internet infrage gestellt (vgl. aber EuGH 2019: Rn. 48). Die Freiheit der Bürger*innen wird weniger durch den Staat als durch marktmächtige Private gefährdet. Deutlich wird dies beispielsweise im Falle der Sperrung von Facebook-Konten oder der Zugangsbedingungen für kleine Händler*innen zur Verkaufsplattform Amazon.

Drittens besteht die Gefahr einer schleichenden Entmündigung. Hier spielen nicht nur Informationsasymmetrien eine Rolle, sondern zunehmende Personalisierung (bspw. zur Preispersonalisierung vgl. Hofmann/Freiling 2020). Der*die gläserne Bürger*in ist Unternehmer*innen mitunter besser bekannt, als diese*r sich selbst kennt. Durch Präferenzmanipulationen kann selbstbestimmtes Handeln weiter untergraben werden (vgl. Wagner/Eidenmüller 2019: 234ff.). Während das Bild des*der rational handelnden Verbraucher*in auch in der analogen Welt durch die Verhaltensökonomik schon erschüttert wurde (Überblick vgl. bei Englerth/Towfigh 2010: § 7), haben die digitalen Möglichkeiten die Gefahr der »Ausnutzung von Verhaltensanomalien« freilich nochmals auf eine neue Stufe gehoben (Wagner/Eidenmüller 2019: 230ff.). Die »Filterblase« lässt grüßen.

Viertens wird auch die Eigentumsordnung herausgefordert. Physische Gegenstände verlieren gegenüber unkörperlichen Gegenständen an Bedeutung. »Smarte« Produkte schöpfen ihren Wert weniger aus der Hard- als aus der Software. Über die Möglichkeiten digitaler Vernetzung kann der Hersteller aber auch über die gesamte Lebenszeit des Produkts dasselbe kontrollieren. Über diese Fernkontrolle können Gebrauchsbeschränkungen, z.B. zur Absicherung nachgelagerter Produktmärkte (etwa für Kaffeekapseln), technisch abgesichert werden. Aber auch das Softwareurheberrecht muss sicherstellen, dass Lock-in-Effekte nicht verstärkt werden. So könnten hier weitergehende Möglichkeiten zum *reverse engineering* erforderlich sein (s. derzeit nur § 69e UrhG; vgl. Wiebe 1992).

Ferner stehen vor allem immaterielle Güter, namentlich Daten, im Fokus der Zuweisung: Wem »gehören« die Daten? Mit Blick auf Daten, dem zentralen Rohstoff der Digitalgesellschaft (das Bild passt im Grunde genommen nicht, da mit Rohstoffen vor allem physische und damit verbrauchbare, also rivale Güter gemeint sind), wird nicht nur diskutiert, wem diese zuzuweisen sind (vgl. Zech 2015a, 2015b), sondern vor allem, wie Zugang zu Daten sichergestellt werden kann (vgl. Louven 2018; Schweitzer 2019b). Schließlich drohen überkommene Ausschließlichkeitsrechte zweckentfremdet zu werden. Allen voran das Urheberrecht findet sich plötzlich in der Rolle, maßgeblich Fragen der digitalen Infrastruktur (z.B. Verbreitung von öffentlichen WLAN wegen ur-

heberrechtlicher Haftungsregelungen) zu determinieren (vgl. Hofmann 2017). Dies ist nur ein weiteres Beispiel, wie vor allem das Urheberrecht die sozialen Bedürfnisse der Digitalgesellschaft konterkarieren kann (vgl. Grünberger 2018: 261ff.).

Diese Liste ist nicht abschließend (zu denken ist beispielsweise auch an die vom Kartellrecht zu bewältigende Gefahr, dass Marktmechanismen durch wenige marktbeherrschende Plattformen ausgehebelt werden; zu dieser Herausforderung für das Kartellrecht vgl. insbesondere Podszun 2020), zeigt aber bereits deutlich, dass sich das Privatrecht seiner Rolle in der Digitalgesellschaft vergewissern muss. Oder in den Worten des Titels dieses Bandes: Schafft es das Privatrecht, »digitale Souveränität« im Verhältnis der Bürger*innen untereinander zu gewährleisten? Reaktionen sind unabdingbar.

2. Privatrechtliche Reaktionsmöglichkeiten

Was ist zu tun? Wie erwähnt ist es eine der zentralen Aufgaben des Privatrechts, die Voraussetzungen für selbstbestimmtes Handeln zu gewährleisten. Es bedarf eines Ordnungsrahmens, der freie Entscheidungen ermöglicht. Unter dem Eindruck der fortschreitenden Digitalisierung mit ihren Gefahren für die Privatrechtsgesellschaft findet sich auch in der Privatrechtswissenschaft eine breite Debatte zu möglichen Reaktionsmöglichkeiten (vgl. z.B. Körber 2016; Wagner/Eidenmüller 2019: 220; Paal/Kumkar 2021).

2.1 Transparenz und Opt-out-Regelungen

Diskutiert werden dabei beispielsweise Möglichkeiten des Abbaus von Informationsasymmetrien über Informationspflichten. Spezielle Transparenzvorgaben erscheinen vielen als das Regulierungsinstrument der Stunde (vgl. kritisch Wagner/Eidenmüller 2019: 239ff. sowie mit Blick auf Preisregulierung Hofmann 2016: 1080f.). Hinter dem Schlagwort »Algorithmentransparenz« stehen in diesem Sinne neue Regelungen wie Art. 7 Abs. 4a der Richtlinie über unlautere Geschäftspraktiken (s. RL 2005/29/EG; zur Neuregelung durch die RL 2019 [EU] 2161):

> »Wenn Verbrauchern die Möglichkeit geboten wird, mithilfe eines Stichworts, einer Wortgruppe oder einer anderen Eingabe nach Produkten zu suchen, die von verschiedenen Gewerbetreibenden oder von Verbrauchern angeboten werden, gelten, unabhängig davon, wo Rechtsgeschäfte letztendlich abgeschlossen werden, allgemeine Informationen, die die

> Hauptparameter für die Festlegung des Rankings der dem Verbraucher im Ergebnis der Suche vorgeschlagenen Produkte, sowie die relative Gewichtung dieser Parameter im Vergleich zu anderen Parametern, betreffen und die in einem bestimmten Bereich der Online-Benutzeroberfläche zur Verfügung gestellt werden, der von der Seite, auf der die Suchergebnisse angezeigt werden, unmittelbar und leicht zugänglich ist, als wesentlich.«

Über »wesentliche« Informationen hat der*die Unternehmer*in zu informieren; andernfalls begeht er*sie einen Wettbewerbsverstoß (s. §§ 8, 3, 5a UWG).

Transparenz allein wird jedoch vielfach als unzureichend empfunden. Namentlich Wagner und Eidenmüller sprechen sich daher für eine weitergehende Regulierung aus: Verbraucher*innen sollten vielmehr vermittels von »Opt-out-Rechten« in die Lage versetzt werden, namentlich personalisierte Preise abzulehnen und stattdessen ein »Angebot zum Marktpreis« zu erhalten. Es bedürfe eines Rechts, Preispersonalisierung abzuwählen (vgl. Wagner/Eidenmüller 2019: 228ff.). Um Präferenzmanipulationen vorzubeugen, sollten Verbraucher*innen allgemein eine Wahlmöglichkeit haben, zwischen »einer personalisierten und einer nichtpersonalisierten virtuellen Welt«, »zwischen einer ›Welt der Kontrolle‹, die auf der Basis vergangener Entscheidungen kuratiert wurde, und einer ›Welt der Spontaneität‹, die Präferenzen des Durchschnitts der Nutzer*innen widerspiegelt oder andere Selektionskriterien verwendet« (Wagner/Eidenmüller 2019: 242). Es müssten dafür anonyme Online-Einkaufsmöglichkeiten ohne Persönlichkeitsprofil zur Verfügung stehen (vgl. ebd.: 246). Digitale Anonymität sei zu gewährleisten (vgl. ebd.: 242). Nicht zuletzt sollten Verbraucher*innen das Recht haben, unter Einfluss von Verkaufsalgorithmen getätigte Transaktionen, die in einem Zustand besonderer Verletzlichkeit getätigt wurden, zu widerrufen (vgl. ebd.: 233f.). Größere Bedeutung kann dabei nicht zuletzt dem Trend zu *law by design* kommen. Plattformen könnten in diesem Sinne schon von vornherein zu einer bestimmten verbraucher*innenfreundlichen, verhaltensökonomischen Erkenntnis berücksichtigenden Gestaltung der Benutzeroberflächen verpflichtet werden.

2.2 Datenschutz und Selbstbestimmung

Ein weiterer, zentraler Aspekt der Debatte um »digitale Souveränität« im Privatrecht liegt im Datenschutzrecht (»Datensouveränität der Nutzer*innen«; vgl. Krüger 2016: 191). Das Verhältnis von Datenschutz und Selbstbestimmung soll im Folgenden exemplarisch etwas näher beleuchtet werden.

Um die »digitale Souveränität« zu stärken, wird in der Literatur die »Anerkennung eines Dateneigentums der Bürger an ihren Informationsdaten« vorgeschlagen (Fezer 2017). Ein »Immaterialgüterrecht sui generis an den Informationen« soll »eine zivilgesellschaftliche Gestaltungskompetenz der Bürger« begründen, »an der Architektur der digitalen Räume zur Organisation der Geschäftsmodelle einer kommerziellen Vermarktung der Informationsdaten mitzuwirken« (Fezer 2017). Schon heute erkennt das Datenschutzrecht freilich die »Hoheit« über die eigenen Daten an, wenn auch nicht im Sinne einer »eigentumsartigen« Zuweisung (vgl. BVerfG 1984). Das Datenschutzrecht als Abwehrrecht (Hofmann 2020a: 15ff.) ermöglicht es aber dem*der Einzelnen, sich gegen unbefugte Datenverarbeitungen zu wehren. Ohne gesetzlichen Erlaubnistatbestand zur Datenverarbeitung (s. insbesondere Art. 6 Abs. 1 lit. f DSGVO) bedarf es insbesondere einer »Einwilligung« des*der Betroffenen (s. Art. 6 Abs. 1 lit. a DSGVO). »Einwilligung« bedeutet jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist (s. Art. 4 Nr. 11 DSGVO). Namentlich auch bei vorformulierten Einwilligungserklärungen kommt es darauf an, dass diese in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zur Verfügung gestellt werden (s. Art. 7 Abs. 2 DSGVO mit Erwägungsgrund 42 DSGVO). Die Erklärung darf nicht in allgemeinen Geschäftsbedingungen »versteckt« werden (vgl. Wendehorst/von Westphalen 2016). Neben der Einwilligung wird vielfach der Erlaubnistatbestand aus Art. 6 Abs. 1 lit. b DSGVO vorliegen, wonach die Datenverarbeitung rechtmäßig ist, soweit sie zur Erfüllung eines Vertrags erforderlich ist. Hier muss das Datenschutzrecht aufpassen, dass ausufernde Leistungsbeschreibungen nicht mehr oder weniger zu einer praktischen Umgehung der restriktiv formulierten Erlaubnistatbestände führen (vgl. ebd.: 3746f.).

Praktisch erweist sich vor allem das Erfordernis der Einwilligung allerdings als schwaches Schwert. Dies liegt nicht nur an der nach wie vor unbefriedigenden Durchsetzung des Datenschutzrechts insgesamt, sondern auch daran, dass Einwilligungen freigiebig erteilt werden. Dies liegt aber weniger an Bürger*innen, die den Anforderungen der Digitalgesellschaft nicht gewachsen sind, sondern an den faktischen Gegebenheiten. Die Vorbedingungen für selbstbestimmtes Handeln (insbesondere: Kenntnis des einschlägigen Sachverhalts, freie Entscheidungsmöglichkeit im Lichte alternativer, gleich-

wertiger Entscheidungsoptionen) sind im digitalen Umfeld häufig nicht gegeben. Die datenschutzrechtliche Einwilligung soll nach verbreiteter Ansicht angesichts von Lock-in-Effekten und komplexen Nutzungsbedingungen »für sich genommen kaum noch ein Garant für die Datensouveränität des Einzelnen« sein (Krüger 2016). Einwilligungserklärungen decken in der Tat praktisch nicht nur eine Vielzahl von Datenverarbeitungssituationen ab, sondern entziehen sich auch dem Einfluss des*der Datenschutzberechtigten (Betroffenem). Auch wenn der europäische Gesetzgeber die »Informiertheit« zur Voraussetzung der Einwilligung erhebt und sich die Einwilligung auf jede einzelne angedachte Verarbeitung zu beziehen hat (»Zweckbindungsgrundsatz«; s. auch Erwägungsgrund 32 und 39 DSGVO; vgl. Veil 2018: 3339f.), lehrt die Rechtspraxis, dass die Steuerungskraft des Rechts hier faktisch massiv beschränkt ist (vgl. Specht 2017a: 1042 u. 1046; Hofmann/Freiling 2020: 335).

Um die*den Einzelne*n zu stärken, wird vorgeschlagen, auf Visualisierung zu setzen (s. auch Art. 12 Abs. 7 DSGVO). Ein »selbstbestimmter, bewussterer Umgang mit personenbezogenen Daten« werde nur dann erfolgen, wenn es endlich gelingen würde, »dem Betroffenen vor Augen zu führen, in welche Datenverarbeitungen er einwilligt und welche Rechte ihm zur Verfügung stehen« (Specht 2017a: 1042). Symbole, die ergänzend zu vertraglichen Klauseln eingesetzt werden sollten, könnten ein geeignetes Mittel darstellen, der fehlenden Kenntnisnahme von Datenschutzerklärungen entgegenzuwirken (vgl. Krüger 2016: 191). Auch Zertifizierungssysteme wären, so Stimmen in der Literatur, ein Schritt zur Stärkung der Betroffenen (vgl. ebd.).

Dessen ungeachtet erweist sich der faktische Zwang zur Einwilligung als Problem. Will der*die Nutzer*in einen bestimmten Dienst nutzen, kommt er*sie häufig nicht umhin, entweder der (überschießenden) Verarbeitung seiner*ihrer Daten zuzustimmen oder das Angebot nicht nutzen zu können. Dem versucht zwar Art. 7 Abs. 4 DSGVO entgegenzuwirken. Demnach ist bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, dem Umstand in größtmöglichem Umfang Rechnung zu tragen, ob u.a. die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind. Es scheint aber vor allem geboten, dass der*die Nutzer*in ohne Mühe differenzierte Einwilligungen erteilen kann. Ihm*ihr sollte es ohne Weiteres möglich sein, bestimmten Verarbeitungen zuzustimmen, anderen nicht. Statt der Möglichkeit, einen Haken unter die Datenschutzerklärung zu setzen, wäre dem*der Betrof-

fenen gedient, wenn er*sie mit mehreren Haken seine*ihre Zustimmung maßgeschneidert geben könnte (vgl. Krüger 2016: 191).

Noch nicht ausgeschöpft erscheinen auch die Möglichkeiten der Klauselkontrolle (zurückhaltend BGH 2008). Intransparenten (s. 307 Abs. 1 S. 2 BGB; s. auch Art. 7 Abs. 2 DSGVO; vgl. Ernst 2017: 113, 2010: 297158; von Westphalen 2017) oder nicht interessengerechten datenschutzrechtlichen Klauseln (s. § 307 Abs. 1 S. 1 BGB) könnte die Wirksamkeit versagt werden. Es ist kein Grund ersichtlich, warum vorformulierte Einwilligungserklärungen nicht oder nur eingeschränkt kontrollfähige Vertragsbedingungen sein sollten (vgl. so auch Krüger 2016: 191f.; soweit die Datenschutzerklärung informativen Charakter hat, s. z.B. Art. 13, 14 DSGVO, scheidet eine AGB-Kontrolle aus, vgl. Wendehorst/von Westphalen 2016: 3748). Es muss möglich sein, die Klausel auch über die Vorgaben des Datenschutzrechts hinaus zu kontrollieren (vgl. aber BGH 2012: Rn. 16, alleiniger Prüfungsmaßstab sollen die Vorschriften des Datenschutzrechts sein; ggf. können auch Vorschriften des UWG zur Unwirksamkeit einer Klausel führen, vgl. BGH 2008). In diesem Sinne verweist Erwägungsgrund 42 DSGVO unter Hinweis auf die Klauselrichtlinie (Richtlinie 93/13/EWG) darauf, dass Klauseln nicht »missbräuchlich« sein dürften (vgl. auch Wendehorst/von Westphalen 2016: 3749).

Während der*die Verbraucher*in in der Lage sein muss, freiwillige, informierte Entscheidungen zu treffen (Information und Transparenz als »Grundpfeiler der Datensouveränität«; vgl. Krüger 2016: 192), begrenzt das Datenschutzrecht die Souveränität des*der Einzelnen aber auch aus einer anderen Richtung. Es stellt sich die Frage, ob das Datenschutzrecht nicht dem*der Betroffenen das Recht nimmt, eigenverantwortlich über seine*ihre Daten zu verfügen, also beispielsweise, vereinfacht gesagt, mit Daten zu bezahlen. Art. 7 Abs. 4 DSGVO (»Kopplungsverbot«) könnte sich insoweit als Hürde erweisen (vgl. Krohm/Müller-Peltzer 2017; Hacker 2019; Dix 2017). Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, muss demnach dem Umstand in größtmöglichem Umfang Rechnung getragen werden, ob u.a. die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind. Mit unterschiedlichen Begründungen wird versucht, dem Geschäftsmodell »Daten gegen Leistung« über eine mehr oder weniger restriktive Auslegung des Art. 7 Abs. 4 DSGVO nicht von vornherein das Wasser abzugraben (vgl. Übersicht bei Kumkar 2020: 328ff.). Es wird darauf hingewiesen, dass es weder mit Art. 8 EU-Grundrechtecharta noch mit dem europäischen Verbrau-

cher*innenleitbild vereinbar wäre, »dem Einzelnen prinzipiell die Fähigkeit abzusprechen, auf Grundlage einer überlegten Entscheidung seine Daten zum Gegenstand eines Austauschverhältnisses zu machen« (Kumkar 2020: 330). Darauf aufbauend wird gefordert, dass über die grundsätzlich freie Widerruflichkeit der Einwilligung (s. Art. 7 Abs. 3 S. 1 DSGVO) disponiert werden können müsse (vgl. Sattler 2017: 1041ff.; zu einem »Datenschuldrecht« vgl. Schmidt-Kessel 2017; vgl. Specht 2017a, 2017b). Einem kategorischen Ausschluss von bindenden Vereinbarungen über personenbezogene Daten wird nach dieser Sichtweise eine Absage erteilt (vgl. Sattler 2017: 1045).

Gemeinsames Schlussfazit: Herausforderungen für die Rechtskonzepte der Souveränität, Integrität und Privatautonomie durch die Digitalisierung

Wir haben gezeigt, dass die klassischen rechtswissenschaftlichen Konzepte der Souveränität, Integrität und Privatautonomie in den Zeiten der Digitalisierung neu herausgefordert werden. Grenzen verschwimmen und eine direkte Übertragung dieser Rechtskonstruktionen aus einer »analogen« Zeit scheitert oftmals an den neuen Gegebenheiten der digitalen Welt. Nicht nur staatliche Souveränität, sondern auch die »individuelle Souveränität« als Basis des Privatrechts wird durch die fortschreitende Digitalisierung herausgefordert. Auf den Punkt gebracht: Privatrechtliche Grundprinzipien werden im Digitalen radikal hinterfragt.

In einer ersten Perspektive wurde gesehen, dass die faktische Grenzenlosigkeit des Internets und damit des weltweiten Datenverkehrs und der entsprechenden Zugriffsmöglichkeiten ein striktes Anknüpfen der Souveränität über »Daten« an deren physischen Speicherort anachronistisch erscheinen lässt. Ein Belegenheitsort der in den Daten enthaltenen Informationen ist technisch-faktisch heute oftmals kaum mehr festzulegen. Mit Ausnahme des – vom Volumen her betrachtet – sehr kleinen Bereichs der Staatsgeheimnisse ist auch das Interesse an der »Herrschaft« über die Informationen und Daten bzw. an der Aufrechterhaltung der digitalen Integrität der Daten kein genuin staatliches, sondern ein solches des einzelnen betroffenen Rechtssubjekts. Künftig kommt es daher weniger auf Fragen der staats- und völkerrechtlichen Souveränität im digitalen Raum, sondern vielmehr auf den grund- und menschenrechtlich verbürgten Schutz der digitalen Integrität der Rechtssubjekte gegenüber inner- und außerstaatlichen Zugriffen auf Daten

und Informationen an. Wir plädieren daher sowohl für rechtspolitische Debatten als auch für den Diskurs um die Auslegung von Rechtsnormen für eine Verschiebung der Perspektive weg von klassischem staatsrechtlichem Souveränitätsdenken hin zur Fokussierung der Gewährleistung und des Ausbaus des grund- und menschenrechtlichen Schutzes der digitalen Integrität der Rechtssubjekte.

Während in einer zweiten Perspektive die weitere Erschütterung privatrechtlicher Grundkonzepte im digitalen Raum anhand verschiedener Stichpunkte zu illustrieren versucht wurde, bleibt am Ende festzuhalten: Die Reaktion des Privatrechts muss dabei eine genuin privatrechtliche sein (marktermöglichender statt marktkompensierender Regulierung). Es gilt auch weiterhin einen Rahmen zu schaffen, in dem individuelle Freiheit größtmöglich verwirklicht werden kann (vgl. Podszun 2020: F 102). Allen voran ist es nicht die Aufgabe des Rechts, sich im Sinne einer Zentralsteuerung selbst an die Stelle der privaten Akteure zu setzen: Statt beispielsweise die Bestimmung von Vertragsinhalten selbst in die Hand zu nehmen, ist es stattdessen die Aufgabe des Privatrechts, dafür zu sorgen, dass ein fairer Rahmen für Vertragsverhandlungen besteht (vgl. Hofmann 2019: 1224, 2020b: 667).

Literaturverzeichnis

Teil I

Bär, Wolfgang (2011): »Transnationaler Zugriff auf Computerdaten«, in: ZIS – Zeitschrift für Internationale Strafrechtsdogmatik 6 (2), S. 53–59.

Bergmann, Jan (2014): »Stichwort: Souveränität«, in: Jan Bergmann (Hg.), Handlexikon der Europäischen Union, Baden-Baden: Nomos.

BGH – Bundesgerichtshof (2007): »5 StR 546/06«, in: NJW – Neue Juristische Wochenschrift 60 (31), S. 2269–2274.

Bode, Thomas A. (2012): Verdeckte strafprozessuale Ermittlungsmaßnahmen, Berlin/Heidelberg: Springer.

Brodowski, Dominik (2021): »§ 110«, in: Georg Borges/Marc Hilber (Hg.), Beck'scher Online-Kommentar IT-Recht, München: C.H. Beck, S. Rn. 12.

Brodowski, Dominik/Eisenmenger, Florian (2014): »Der Zugriff auf Cloud-Speicher und Internetdienste durch Ermittlungsbehörden. Zur sachlichen und zeitlichen Reichweite der ›kleinen Online-Durchsuchung‹ nach § 110 Abs. 3 StPO«, in: ZD – Zeitschrift für Datenschutz 4 (3), S. 119–126.

Bruns, Michael (2019): »§ 110«, in: Rolf Hannich (Hg.), Karlsruher Kommentar zur Strafprozessordnung, München: C.H. Beck, S. Rn. 8a.

Burchard, Christoph (2018a): »Der grenzüberschreitende Zugriff auf Clouddaten im Lichte der Fundamentalprinzipien der internationalen Zusammenarbeit – Teil 1«, in: ZIS – Zeitschrift für Internationale Strafrechtsdogmatik 13 (6), S. 190–203.

Burchard, Christoph (2018b): »Der grenzüberschreitende Zugriff auf Clouddaten im Lichte der Fundamentalprinzipien der internationalen Zusammenarbeit in Strafsachen – Teil 2«, in: ZIS – Zeitschrift für Internationale Strafrechtsdogmatik 13 (7–8), S. 249–267.

BVerfG – Bundesverfassungsgericht (1983) (65): »1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83«, in: BVerfGE, S. 1–71.

BVerfG – Bundesverfassungsgericht (2008) (120): »1 BvR 370/07, 1 BvR 595/07«, in: BVerfGE, S. 274–350.

BVerfG – Bundesverfassungsgericht (2009): »2 BvR 902/06«, in: NJW – Neue Juristische Wochenschrift 62 (34), S. 2431–2439.

BVerfG – Bundesverfassungsgericht (2016) (141): »1 BvR 966/09, 1 BvR 1140/09«, in: BVerfGE, S. 220–378.

BVerfG – Bundesverfassungsgericht (2016): »1 BvR 966, 1140/09«, in: NJW – Neue Juristische Wochenschrift 69 (25), S. 1781–1814.

BVerfG – Bundesverfassungsgericht (2018): »2 BvR 1405/17,2 BvR 1780/17«, in: BeckRS, S. 14189.

BVerfG – Bundesverfassungsgericht (2020a): »1 BvR 16/13«, in: NJW – Neue Juristische Wochenschrift 73 (5), S. 300–314.

BVerfG – Bundesverfassungsgericht (2020b): »1 BvR 276/17«, in: NJW – Neue Juristische Wochenschrift 73 (5), S. 314–328.

BVerfG – Bundesverfassungsgericht (2020c): »1 BvR 2835/17«, in: NJW – Neue Juristische Wochenschrift 73 (31), S. 2235–2269.

BVerfG – Bundesverfassungsgericht (2021): »2 BvR 1845/18, 2 BvR 2100/18«, in: NJW – Neue Juristische Wochenschrift 74 (21), S. 1518–1526.

Council of Europe (2001): Übereinkommen über Computerkriminalität vom 23.11.2001 (= Sammlung Europäischer Verträge Nr. 185). Online unter: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185, abgerufen am 19.07.2022.

Diel-Gligor, Katharina (2021): »Sicherungsinstrumente für die Rechtsstaatlichkeit in der EU«, in: ZRP – Zeitschrift für Rechtspolitik 54 (2), S. 63–66.

Durner, Wolfgang (2021): »Art. 10«, in: Roman Herzog/Rupert Scholz/Matthias Herdegen/Hans Klein (Hg.), Dürig/Herzog/Scholz Grundgesetz Kommentar Band I, München: C.H. Beck, S. Rn. 141ff.

EGMR – Europäischer Gerichtshof für Menschenrechte (2015): »Zakharov gg. Russland 47143/06«, in: NLMR – Newsletter Menschenrechte 24 (6), S. 509–516.

EuGH – Europäischer Gerichtshof (2014): »C-293/12, C-594/12«, in: NJW – Neue Juristische Wochenschrift 67 (30), S. 2169–2173.

Fritzsche, Albrecht (2022): »Konturenbildung im Gestaltungsraum der digitalen Transformation – eine Reflexion der Debatte über ›digitale Souveränität‹ aus betriebswirtschaftlicher Sicht«, in: Georg Glasze/Eva Odzuck/Ronald Staples (Hg.), Was heißt digitale Souveränität? Diskurse, Praktiken und Voraussetzungen »individueller« und »staatlicher Souveränität« im digitalen Zeitalter, Bielefeld: transcript, S. 229–245.

Galen, Margarete von (2020): »Kritische Anmerkungen zur E-Evidence-Verordnung«, in: Elisa Hoven/Hans Kudlich (Hg.), Digitalisierung und Strafverfahren, Baden-Baden: Nomos, S. 127–138.

Glasze, Georg/Odzuck, Eva/Staples, Ronald (2022): »Einleitung: Digitalisierung als Herausforderung – ›Souveränität‹ als Antwort? Konzeptionelle Hintergründe der Forderungen nach ›digitaler Souveränität‹«, in: Georg Glasze/Eva Odzuck/Ronald Staples (Hg.), Was heißt digitale Souveränität? Diskurse, Praktiken und Voraussetzungen »individueller« und »staatlicher Souveränität« im digitalen Zeitalter, Bielefeld: transcript, S. 7–28.

Goger, Thomas/Stock, Jürgen (2017): »Cybercrime – Herausforderung für die internationale Zusammenarbeit«, in: ZRP – Zeitschrift für Rechtspolitik 47 (1), S. 10–14.

Grözinger, Andreas (2019): »Heimliche Zugriffe auf die Cloud – Befugnis zur Plünderung eines unermesslichen Datenschatzes«, in: StV – Strafverteidiger 39 (6), S. 406–412.

Hamel, Patricia (2020): »Schnellerer grenzüberschreitender Zugriff auf elektronische Beweismittel: Die E-evidence Vorschläge der Europäischen Kommission«, in: Elisa Hoven/Hans Kudlich (Hg.), Digitalisierung und Strafverfahren, Baden-Baden: Nomos, S. 103–126.

Hauck, Pierre (2014): Heimliche Strafverfolgung und Schutz der Privatheit: Eine vergleichende und interdisziplinäre Analyse des deutschen und englischen Rechts unter Berücksichtigung der Strafverfolgung in der Europäischen Union und im Völkerstrafrecht, Tübingen: Mohr Siebeck.

Hauschild, Jörn (2014): »§ 110«, in: Christoph Knauer/Hans Kudlich/Hartmut Schneider (Hg.), Münchener Kommentar zur StPO, Band 1: §§1-150, München: C.H. Beck, S. Rn. 18f.

Jansen, Marek (2018): »Microsofts ›Search Warrant‹ Case – oder die Zukunft der europäischen Datensouveränität«, in: ZD – Zeitschrift für Datenschutz 9 (4), S. 149–150.

Jarass, Hans D. (2021): »Art. 8 GrCh«, in: Hans D. Jarass (Hg.), Charta der Grundrechte der Europäischen Union, München: C.H. Beck, S. Rn. 9.

Jellinek, Georg (1922): Allgemeine Staatslehre, Berlin: Springer.

Kalpakis, George/Tsikrika, Theodora/Cunningham, Neil/Iliou, Christos/Vrochidis, Stefanos/Middleton, Jonathan/Kompatsiaris, Ioannis (2016): »OSINT and the Dark Web«, in: Babak Akhgar/P. Saskia Bayerl/Fraser Sampson (Hg.), Open Source Intelligence Investigation, Cham: Springer, S. 111–132.

Köhler, Marcus (2021): »§ 110«, in: Lutz Meyer-Goßner/Bertram Schmitt (Hg.), Strafprozessordnung mit GVG und Nebengesetzen, München: C.H. Beck, S. Rn. 7b.

Krcmar, Helmut (2016): »§ 1 Technische Grundlagen des Cloud Computings«, in: Georg Borges/Geert Meents (Hg.), Rechtshandbuch Cloud Computing, München: C.H. Beck, S. 1–17.

Moechel, Erich (2021): Verhandlungen EU-USA zur Cloud-Überwachung gestartet. FM4 ORF, Issue vom 06.05.2021. Online unter: https://fm4.orf.at/stories/3014416/, abgerufen am 16.07.2022.

Oberlandesgericht Karlsruhe (2020): »Ausl 301 AR 156/19«, in: BeckRS, S. 1720.

Rath, Michael/Spies, Axel (2018): »CLOUD Act: Selbst für Wolken gibt es Grenzen«, in: CCZ – Corporate Compliance Zeitschrift 11 (5), S. 229–230.

Rückert, Christian (2020a): »Herausforderungen der Digitalisierung für das Strafverfahren«, in: Elisa Hoven/Hans Kudlich (Hg.), Digitalisierung und Strafverfahren, Baden-Baden: Nomos, S. 9–38.

Rückert, Christian (2020b): »§ 21 Strafanwendungsrecht«, in: Philipp Maume/Lena Maute/Mathias Fromberger (Hg.), Rechtshandbuch Kryptowerte, München: C.H. Beck, S. 537–546.

Safferling, Christoph (2014): »Der EuGH, die Grundrechtecharta und nationales Recht: Die Fälle Åkerberg Fransson und Melloni«, in: NStZ – Neue Zeitschrift für Strafrecht 34 (10), S. 545–551.

Safferling, Christoph (2021): »Entführung durch ausländischen Geheimdienst auf deutschem Boden«, in: JR – Juristische Rundschau 93 (7), S. 306–331.

Safferling, Christoph/Rückert, Christian (2020): »Schutz von Dissidenten und Abwehr von Cyberspionage – die neue Bedeutung des § 99 StGB«, in: ZStW – Zeitschrift für die gesamte Strafrechtswissenschaft 132 (2), S. 367–369.

Safferling, Christoph/Rückert, Christian (2021): »Europäische Grund- und Menschenrechte im Strafverfahren – ein Paradigmenwechsel?«, in: NJW – Neue Juristische Wochenschrift 74 (5), S. 287–292.

Schmahl, Stefanie (2020): »Grundrechtsbindung der deutschen Staatsgewalt im Ausland«, in: NJW – Neue Juristische Wochenschrift 73 (31), S. 2221–2224.

Schwabenbauer, Thomas (2013): Heimliche Grundrechtseingriffe: Ein Beitrag zu den Möglichkeiten und Grenzen sicherheitsbehördlicher Ausforschung, Tübingen: Mohr Siebeck.

Staffler, Lukas/Jany, Oliver (2020): »Künstliche Intelligenz und Strafrechtspflege – eine Orientierung«, in: ZIS – Zeitschrift für Internationale Strafrechtsdogmatik 15 (4), S. 164–177.

Tanneberger, Steffen (2014): Die Sicherheitsverfassung: Eine systematische Darstellung der Rechtsprechung des Bundesverfassungsgerichts; zugleich ein Beitrag zu einer induktiven Methodenlehre, Tübingen: Mohr Siebeck.

Wicker, Magda (2013a): »Durchsuchung in der Cloud – Nutzung von Cloud-Speichern und der strafprozessuale Zugriff deutscher Ermittlungsbehörden«, in: MMR – Multimedia und Recht 16 (12), S. 765–769.

Wicker, Magda (2013b): »Ermittlungsmöglichkeiten in der Cloud«, in: Jürgen Taeger (Hg.), DSRI-Tagungsband, Oldenburg: OlWIR Oldenburger Verlag für Wirtschaft, Informatik und Recht, S. 981–1001.

Teil II

Alexander, Christian (2019): Wettbewerbsrecht, Köln: Carl Heymanns.

BGH – Bundesgerichtshof (2008): »Urt. v. 16.7.2008 – VIII ZR 348/06«, in: NJW – Neue Juristische Wochenschrift 61 (42), S. 3055.

BGH – Bundesgerichtshof (2012): »Urt. v. 11.11.2009 – VIII ZR 12/08«, in: NJW – Neue Juristische Wochenschrift 65 (12), S. 864.

Böhm, Franz (1966): »Privatrechtsgesellschaft und Marktwirtschaft«, in: Ordo – Jahrbuch für die Ordnung von Wirtschaft und Gesellschaft 17, S. 75–151.

Bornkamm, Joachim/Feddersen, Jörn (2021): »§ 5 Irreführende geschäftliche Handlungen«, in: Helmut Köhler/Joachim Bornkamm/Jörn Feddersen (Hg.), Gesetz gegen den unlauteren Wettbewerb: UWG, München: C.H. Beck, S. 750–1074.

Brehm, Wolfgang (2008): Allgemeiner Teil des BGB, Stuttgart: Boorberg.

Brox, Hans/Walker, Wolf-Dietrich (2020): Allgemeiner Teil des BGB, München: Vahlen.

Busch, Christoph (2019): »Mehr Fairness und Transparenz in der Plattformökonomie?«, in: GRUR – Gewerblicher Rechtsschutz und Urheberrecht 121 (8), S. 788–796.

Busch, Christoph/Dannemann, Gerhard/Schulte-Nölke, Hans (2020): »Bausteine für ein europäisches Recht der Plattformökonomie«, in: MMR – Multimedia und Recht 23 (10), S. 667–675.

BVerfG – Bundesverfassungsgericht (1984): »Urt. v. 15.12.1983 – 1 BvR209/83«, in: NJW – Neue Juristische Wochenschrift 37 (8), S. 419.

BVerfG – Bundesverfassungsgericht (1994): »Beschl. v. 19.10.1993 – 1 BvR 567/89«, in: NJW – Neue Juristische Wochenschrift 47 (1), S. 36.

BVerfG – Bundesverfassungsgericht (2018): »Beschl. v. 11.4.2018 – 1 BvR 3080/09«, in: NJW – Neue Juristische Wochenschrift 71 (23), S. 1667 – Stadionverbot.

Deutscher Bundestag (2009): Bundestag-Drucksache 17/315 vom 18.12.2009. Online unter: https://dserver.bundestag.de/brd/2017/0315-17.pdf, abgerufen am 19.07.2022.

Dix, Alexander (2017): »Daten als Bezahlung – zum Verhältnis zwischen Zivilrecht und Datenschutzrecht«, in: ZEuP – Zeitschrift für europäisches Privatrecht 25 (1), S. 1–5.

Englerth, Markus/Towfigh, Emanuel V. (2010): »§ 8 – Verhaltensökonomik«, in: Emanuel V. Towfigh/Niels Petersen (Hg.), Ökonomische Methoden im Recht. Eine Einführung für Juristen, Tübingen: Mohr Siebeck, S. 237–276.

Ernst, Stefan (2010): BGH: Ausgestaltung von Kundenbindungssystemen – Happy Digits. LMK, Kommentierte BGH-Rechtsprechung, Lindenmaier-Möhring (Fachdienst Zivilrecht), 297158.

Ernst, Stefan (2017): »Die Einwilligung nach der Datenschutzgrundverordnung«, in: ZD – Zeitschrift für Datenschutz 7 (3), S. 110–113.

EuGH – Europäischer Gerichtshof (2019): »Urt. v. 3.10.2019 – C-18/18 – Eva Glawischnig-Piesczek/Facebook Ireland Ltd.«, in: GRUR – Gewerblicher Rechtsschutz und Urheberrecht 121 (11), S. 1208.

Fezer, Karl-Heinz (2017): »Dateneigentum der Bürger«, in: ZD – Zeitschrift für Datenschutz 7 (3), S. 99–104.

Flume, Werner (1975): Allgemeiner Teil des Bürgerlichen Rechts. Zweiter Band: Das Rechtsgeschäft, Berlin/Heidelberg: Springer.

Geiger, Christoph (2004): »Der urheberrechtliche Interessenausgleich in der Informationsgesellschaft. Zur Rechtsnatur der Beschränkungen des Urheberrechts«, in: GRUR Int. – Gewerblicher Rechtsschutz und Urheberrecht, Internationaler Teil (10), S. 815–820.

Grigoleit, Hans Christoph (2008): »Anforderungen des Privatrechts an die Rechtstheorie«, in: Matthias Jestaedt/Oliver Lepsius (Hg.), Rechtswissenschaftstheorie, Tübingen: Mohr Siebeck, S. 51–78.

Grünberger, Michael (2017): »Internetplattformen – Aktuelle Herausforderungen der digitalen Ökonomie an das Urheber- und Medienrecht«, in: ZUM – Zeitschrift für Urheber- und Medienrecht 61 (2), S. 89–92.

Grünberger, Michael (2018): »Verträge über digitale Güter«, in: AcP – Archiv für die civilistische Praxis 218, S. 213–296.

Hacker, Philipp (2019): »Daten als Gegenleistung: Rechtsgeschäfte im Spannungsfeld von DSGVO und allgemeinem Vertragsrecht«, in: ZfPW – Zeitschrift für die gesamte Privatrechtswissenschaft 5 (2), S. 148–197.

Hellgardt, Alexander (2016): Regulierung und Privatrecht: Staatliche Verhaltenssteuerung mittels Privatrecht und ihre Bedeutung für Rechtswissenschaft, Gesetzgebung und Rechtsanwendung, Tübingen: Mohr Siebeck.

Hofmann, Franz (2016): »Der maßgeschneiderte Preis. Dynamische und individuelle Preise aus lauterkeitsrechtlicher Sicht«, in: WRP – Wettbewerb in Recht und Praxis 13 (9), S. 1074–1081.

Hofmann, Franz (2017): »Das Allgemeininteresse an der Verfügbarkeit von Internet im Spannungsverhältnis zum Schutz von Urheberrecht«, in: GPR – Zeitschrift für das Privatrecht der Europäischen Union 14 (4), S. 176–182.

Hofmann, Franz (2019): Fünfzehn Thesen zur Plattformhaftung nach Art. 17 DSM-RL«, in: GRUR – Gewerblicher Rechtsschutz und Urheberrecht 121 (12), S. 1219–1229.

Hofmann, Franz (2020a): »›Absolute Rechte‹ an Daten – immaterialgüterrechtliche Perspektive«, in: Tereza Pertot (Hg.), Rechte an Daten, Tübingen: Mohr Siebeck, S. 9–33.

Hofmann, Franz (2020b): »Plattformregulierung im Lichte des Unionsrechts«, in: ZUM – Zeitschrift für Urheber- und Medienrecht 64 (10), S. 665–670.

Hofmann, Franz (2020c): »Einseitige und übereinstimmende Erledigungserklärungen vor unzuständigem Gericht«, in: NJW – Neue Juristische Wochenschrift 73 (16), S. 1117–1119.

Hofmann, Franz (2020d): »Standpunkt: Recht auf ›Unrecht‹«, in: NJW-Aktuell – Neue Juristische Wochenschrift Aktuell (36), S. 15.

Hofmann, Franz (2021): »Das neue Urheberrechts-Diensteanbieter-Gesetz«, in: NJW – Neue Juristische Wochenschrift 74 (27), S. 1905–1910.

Hofmann, Franz/Freiling, Felix (2020): »Personalisierte Preise und das Datenschutzrecht«, in: ZD – Zeitschrift für Datenschutz 10 (7), S. 331–335.

Köhler, Helmut (2017): BGB. Allgemeiner Teil, München: C.H. Beck.

Körber, Torsten (2016): »›Ist Wissen Marktmacht?‹ Überlegungen zum Verhältnis von Datenschutz, ›Datenmacht‹ und Kartellrecht – Teil 1«, in: NZKart – Neue Zeitschrift für Kartellrecht 4 (7), S. 303–309.

Krohm, Niclas/Müller-Peltzer, Philipp (2017): »Auswirkungen des Koppelungsverbots auf die Praxistauglichkeit der Einwilligung«, in: ZD – Zeitschrift für Datenschutz 7 (12), S. 551–555.

Krüger, Philipp-L. (2016): »Datensouveränität und Digitalisierung«, in: ZRP – Zeitschrift für Rechtspolitik 49 (7), S. 190–192.

Kühling, Jürgen/Martini, Mario (2016): »Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht?«, in: EuZW – Europäische Zeitschrift für Wirtschaftsrecht 27 (12), S. 448–453.

Kumkar, Lea K. (2020): »Herausforderungen eines Gewährleistungsrechts im digitalen Zeitalter«, in: ZfPW – Zeitschrift für die gesamte Privatrechtswissenschaft 6 (3), S. 306–333.

Leistner, Matthias/Roder, Verena (2016): »Die Rechtsprechung des EuGH zum Unionsurheberrecht aus methodischer Sicht – zugleich ein Beitrag zur Fortentwicklung des europäischen Privatrechts im Mehrebenensystem«, in: ZfPW – Zeitschrift für die gesamte Privatrechtswissenschaft 2 (2), S. 129–172.

Louven, Sebastian (2018): »Datenmacht und Zugang zu Daten«, in: NZKart – Neue Zeitschrift für Kartellrecht 6 (5), S. 217–222.

Medicus, Dieter/Lorenz, Stephan (2015): Schuldrecht I. Allgemeiner Teil, München: C.H. Beck.

Paal, Boris P./Kumkar, Lea K. (2021): »Wettbewerbsschutz in der Digitalwirtschaft«, in: NJW – Neue Juristische Wochenschrift 74 (12), S. 809–815.

Paulus, Christoph G./Zenker, Wolfgang (2001): »Grenzen der Privatautonomie«, in: JUS – Juristische Schulung 41 (1), S. 1–8.

Petersen, Jens (2011): »Die Privatautonomie und ihre Grenzen«, in: JURA – Juristische Ausbildung 33 (3), S. 184–186.

Podszun, Rupprecht (2020): Gutachten Teil F zum 73. Deutschen Juristentag. Empfiehlt sich eine stärkere Regulierung von Online-Plattformen und anderen Digitalunternehmen?, München: C.H. Beck.

Raiser, Ludwig (1961): »Der Stand der Lehre vom subjektiven Recht im Deutschen Zivilrecht«, in: JZ – Juristen Zeitung 16, S. 465–473.

Raue, Benjamin/Steinebach, Martin (2020): »Uploadfilter – Funktionsweisen, Einsatzmöglichkeiten und Parametrisierung«, in: ZUM – Zeitschrift für Urheber- und Medienrecht 64 (5), S. 355–364.

Riesenhuber, Karl (2009): »§ 1 Privatrechtsgesellschaft: Leistungsfähigkeit und Wirkkraft im deutschen und Europäischen Recht. Entwicklung, Stand und Verfassung des Privatrechts«, in: Karl Riesenhuber (Hg.), Privatrechtsgesellschaft. Entwicklung, Stand und Verfassung des Privatrechts, Tübingen: Mohr Siebeck, S. 1–32.

Sattler, Andreas (2017): »Personenbezogene Daten als Leistungsgegenstand«, in: JZ – Juristen Zeitung 72 (21), S. 1036–1046.

Sauer, Stefan/Staples, Ronald/Steinbach, Vincent (2022): »Der relationale Charakter von ›digitaler Souveränität‹. Zum Umgang mit dem ›Autonomie/Heteronomie‹-Dilemma in sich transformierenden Arbeitswelten«, in: Georg Glasze/Eva Odzuck/Ronald Staples (Hg.), Was heißt digitale Souveränität? Diskurse, Praktiken und Voraussetzungen »individueller« und »staatlicher Souveränität« im digitalen Zeitalter, Bielefeld: transcript, S. 287–315.

Schmidt-Kessel, Martin (2017): »Unentgeltlich oder entgeltlich? – Der vertragliche Austausch von digitalen Inhalten gegen personenbezogene Daten«, in: ZfPW – Zeitschrift für die gesamte Privatrechtswissenschaft 3 (1), S. 84–108.

Schuppert, Gunnar (2019): Eigentum neu denken. Ein Rechtsinstitut zwischen Wandel und Resilienz, Baden-Baden: Nomos.

Schweitzer, Heike (2019a): »Digitale Plattformen als private Gesetzgeber: Ein Perspektivwechsel für die europäische ›Plattform-Regulierung‹«, in: ZEuP – Zeitschrift für Europäisches Privatrecht 27 (1), S. 1–12.

Schweitzer, Heike (2019b): »Datenzugang in der Datenökonomie: Eckpfeiler einer neuen Informationsordnung«, in: GRUR – Gewerblicher Rechtsschutz und Urheberrecht 121 (6), S. 569–580.

Specht, Louisa (2017a): »Das Verhältnis möglicher Datenrechte zum Datenschutzrecht«, in: GRUR Int. – Gewerblicher Rechtsschutz und Urheberrecht, Internationaler Teil (12), S. 1040–1047.

Specht, Louisa (2017b): »Daten als Gegenleistung – Verlangt die Digitalisierung nach einem neuen Vertragstypus?«, in: JZ – Juristen Zeitung 72 (15–16), S. 763–770.

Tonner, Klaus (2017): »Verbraucherschutz in der Plattform-Ökonomie«, in: VuR – Verbraucher und Recht 32 (5), S. 161–162.

Tuhr, Andreas von (1957): Der Allgemeine Teil des Deutschen Bürgerlichen Rechts. Erster Band: Allgemeine Lehren und Personenrecht, Berlin: Duncker & Humblot.

Veil, Winfried (2018): »Einwilligung oder berechtigtes Interesse? – Datenverarbeitung zwischen Skylla und Charybdis«, in: NJW – Neue Juristische Wochenschrift 71 (46), S. 3337–3343.

Wagner, Gerhard (2017): »Produkthaftung für autonome Systeme«, in: AcP – Archiv für die civilistische Praxis 217 (6), S. 707–765.

Wagner, Gerhard/Eidenmüller, Horst (2019): »In der Falle der Algorithmen? Abschöpfen von Konsumentenrente, Ausnutzen von Verhaltensanomalien und Manipulation von Präferenzen: Die Regulierung der dunklen Seite personalisierter Transaktionen«, in: ZfPW – Zeitschrift für die gesamte Privatrechtswissenschaft 5 (2), S. 220–246.

Wendehorst, Christiane (2019): »§§ 312–312k«, in: Franz J. Säcker/Roland Rixecker/Hartmut Oetker/Bettina Limperg (Hg.), Münchener Kommentar zum BGB, Band 3: Schuldrecht – Allgemeiner Teil II, München: C.H. Beck, S. 156–317.

Wendehorst, Christiane/Westphalen, Friedrich von (2016): »Das Verhältnis zwischen Datenschutz-Grundverordnung und AGB-Recht«, NJW – Neue Juristische Wochenschrift 69 (52), S. 3745–3749.

Westphalen, Friedrich von (2017): »Nutzungsbedingungen von Facebook – Kollision mit europäischem und deutschem AGB-Recht«, in: VuR – Verbraucher und Recht 32 (9), S. 323–331.

Wiebe, Andreas (1992): »Reverse Engineering und Geheimnisschutz von Computerprogrammen«, in: CR – Computer und Recht 8 (3), S. 134–141.

Zech, Herbert (2012): Information als Schutzgegenstand, Tübingen: Mohr Siebeck.

Zech, Herbert (2015a): »›Industrie 4.0‹ – Rechtsrahmen für eine Datenwirtschaft im digitalen Binnenmarkt«, in: GRUR – Gewerblicher Rechtsschutz und Urheberrecht 117 (12), S. 1151–1159.

Zech, Herbert (2015b): »Daten als Wirtschaftsgut – Überlegungen zu einem ›Recht des Datenerzeugers‹«, in: CR – Computer und Recht 31 (3), S. 137–146.

»Digitale Souveränität«: Zielperspektive einer Bildung in Zeiten tiefgreifender Mediatisierung?

Jane Müller, Rudolf Kammerl

Abstract *Der Beitrag untersucht Fragen zur »digitalen Souveränität«, die sich aus einer medienpädagogischen Perspektive auf der Mikroebene stellen. Zunächst benennt er dazu Herausforderungen einer tiefgreifend mediatisierten Gesellschaft für das Bildungssystem. Darauf aufbauend diskutiert der Beitrag Begriffsbestimmungen und Forderungen nach einer »individuellen Souveränität«. Er problematisiert eine Engführung auf insbesondere technische Fertigkeiten. Demgegenüber schlägt er vor, »digitale Souveränität« vor dem Hintergrund endogener und exogener Faktoren relational zu fassen. Resümierend formuliert der Beitrag die (Mit-)Gestaltung der digital geprägten Welt als Bildungsziel und zeigt Implikationen für Forschung, Bildungspolitik und -praxis auf.*

Bei der Gestaltung des gesellschaftlichen Zusammenlebens sollte auch im digitalen Wandel gelten, dass in Demokratien das Volk der Souverän ist. Die Selbst- und Mitbestimmung der Bürger*innen legitimiert gesellschaftlichen Wandel und ist in Demokratien verfassungsrechtlich verankert. Die staatliche »digitale Souveränität« muss deshalb auch auf individueller Ebene sicherstellen, dass Selbst- und Mitbestimmung Anwendung finden. Daran schließen sich die Fragen an, ob Bürger*innen überhaupt zu »Souveränität« im Umgang mit digitalen Medien in der Lage sind und was darunter konkret zu verstehen ist. Die derzeit zu beobachtende Übertragung des Begriffs »digitale Souveränität« auf den individuellen Umgang mit Medien bietet Chancen, geht aber auch mit Schwierigkeiten einher. Problematisch ist sie immer dann, wenn die Begriffsverwendung auf individuelle Kompetenzen und Anpassungsfähigkeiten verkürzt wird oder Aufgabenstellungen an das Bildungssystem und pädagogische Fachkräfte adressiert werden, die auf anderen Ebenen besser zu bearbeiten wären. Daher fasst dieser Beitrag »digitale Souveränität« relational. Sie kann in einem performativen Herstellungsprozess jeweils (nur) situativ und temporär ausgehandelt werden. Die jeweils

vorfindbaren Freiheitsgrade und die Verteilung der Handlungsmacht in Bezug auf die Umsetzung konkreter Medienpraktiken charakterisieren dabei die Verteilung von »digitaler Souveränität«. Der so definierte Analysezugang unterstreicht, dass neben individuellen auch soziale, technische und rechtliche Bedingungen in die Analyse einfließen müssen. Ziel des Beitrags ist es, mit dieser eigenen Definition den bisherigen Fachdiskurs zu erweitern und im Anschluss an praxeologische Forschungsansätze die Notwendigkeit und den Mehrwert eines relationalen Zugangs zur »digitalen Souveränität« von Individuen herauszuarbeiten.

1. Mediatisierung als gesellschaftlicher Transformationsprozess

Kommunikation wird in allen Lebensbereichen immer stärker durch zunächst technische und sodann digitale Medien mitbestimmt. Krotz (2007) bezeichnet diesen Metaprozess als Mediatisierung, der in Verbindung mit anderen Transformationsprozessen zu einem umfassenden gesellschaftlichen Wandel führt. Es ändern sich nicht nur quantitativ die Mediennutzungszeiten, auch was und wie mit welchen Medien kommuniziert wird, verändert sich qualitativ. »Permanently online, permanently connected« (Vorderer 2015: 259), wandeln sich u.a. das Beziehungshandeln und die Identitätsentwicklung. Erreichbarkeit und Reaktionszeiten werden gegenüber räumlicher Nähe relevanter, und die strategische Darstellung des eigenen Selbst im Netz zählt zu den Aufgaben der Identitätsentwicklung. Für die Individuen ändern sich Kommunikationsformen und -inhalte sowie die an der Kommunikation beteiligten Akteur*innen.

Diese Entwicklungen auf den unterschiedlichen Ebenen der Kommunikationsstrukturen lassen sich weniger als technischer Prozess, sondern vielmehr als sozialer Wandel (digitaler Wandel) beschreiben und werden in den Sozialwissenschaften als Zusammenspiel von Medien-, Kommunikations- und gesellschaftlichem Wandel unter dem Begriff der Mediatisierung untersucht (vgl. Krotz 2001; Couldry/Hepp 2013; Hepp 2018). Hepp (ebd.) identifiziert fünf zentrale Trends, die eine tiefgreifende Mediatisierung kennzeichnen: die Ausdifferenzierung der Medientechnologie, deren wachsende Konnektivität, die Omnipräsenz digitaler (Mobil-)Kommunikation, eine beschleunigte Innovationsdichte und die Datafizierung jedweder Medienpraktiken. Die Veränderungen auf der Ebene technologischer Entwicklungen und gesellschaftlicher Gestaltung des Mediensystems (vgl. Luhmann 1996)

lassen sich als historischer Wandel der Medienumgebung beschreiben. Waren lange Zeit Massenmedien Mittler zwischen Staat und Gesellschaft, haben sie durch Individualisierung der Medienpraktiken zunehmend an Meinungsmacht verloren. Die tiefgreifende Mediatisierung spiegelt sich zudem in den zentralen Bildungs- und Sozialisationsinstanzen wider und wird konkret sichtbar in veränderten Medien und Medienpraktiken in Familien, Schulen und Peergroups (vgl. Kammerl et al. 2020).

Für Kinder und Jugendliche gilt besonders, dass sie im digitalen Wandel zunehmend mit den Chancen und Risiken digitaler Mediennutzung konfrontiert sind. Einerseits wird herausgestellt, dass »digitale Kompetenzen […] immer häufiger Grundlage erfolgreicher Arbeits- und Bildungsbiografien« sind (BMFSFJ 2017: 299). Andererseits werden die Risiken gefährdender Inhalte und Kontakte sowie die kommerziellen Interessen der Anbietenden problematisiert. Darüber hinaus werden die intensivierte Sammlung und Auswertung individueller Nutzungsdaten als Gefährdung der informationellen Selbstbestimmung interpretiert. Grundlegend stellt sich die Frage, wie Selbstbestimmung als ein Grundpfeiler von Konzepten der Menschenwürde im digitalen Zeitalter konzipiert und realisiert werden kann und wie diese Konzepte umgesetzt werden können. Gleichzeitig stellt sich die Frage, wie die Medien- und Informationskompetenz der*s Einzelnen individuell (im Sinne einer bildungsbiografisch zu entwickelnden kompetenten und reflexiven Mediennutzung) entwickelt sowie strukturell (im Sinne der Pluralität und Qualität entsprechender Bildungs- und Hilfsangebote) medienpädagogisch gefördert werden kann.

2. Herausforderungen für das Bildungssystem

Infolge von Mediatisierung und Digitalisierung entstehen neue Herausforderungen und Aufgabenstellungen für das Bildungssystem, die aus unterschiedlichen fachwissenschaftlichen und didaktischen Perspektiven diskutiert werden. Fokussiert auf den Erziehungs- und Bildungsauftrag, sind vor allem die strukturfunktionalistische und die anthropologische Argumentationslinie (vgl. Duncker 2007) bedeutsam. Ausgehend von dieser Unterscheidung können als zentrale Aufgaben schulischer Bildung einerseits die Vorbereitung der Kinder auf ihre Rolle in der Gesellschaft (strukturfunktionalistische Linie) und andererseits die Unterstützung einer individuellen Persönlichkeitsentwicklung (anthropologische Linie) gesehen werden. Diese anthropologische

Linie ist durch das Spannungsfeld gekennzeichnet, in dem die aktive Kulturaneignung durch Heranwachsende (Enkulturation) und das Recht auf Individualität (Individuierung) sich gegenüberstehen. Darüber hinaus wird die Entwicklung von Kindern zu Erwachsenen als eine Entwicklung von der Hilfsbedürftigkeit zur Eigenständigkeit konzeptualisiert und gesellschaftlich organisiert. Kinder sind angewiesen auf Erziehung und Bildung. Sie sind hierfür in Abgrenzung zur Arbeits- und Lebenswelt der Erwachsenen in einem eigenen Schonraum zu separieren (vgl. Honig 1999: 221). Erst durch Bildungsprozesse werden Heranwachsende zu einer selbstbestimmten und selbstverantworteten Lebensführung ermächtigt.

Gerade mit Blick auf Kinder und jüngere Jugendliche werden deshalb im Rahmen zunehmender Mediatisierung Aspekte des Jugendmedienschutzes relevant. Ein funktionierender Jugendmedienschutz scheint jedoch kaum gewährleistet. So zählt etwa der Gefährdungsatlas der Bundesprüfstelle für jugendgefährdende Medien eine große Vielzahl von Risiken auf (vgl. Brüggen et al. 2019)[1]. Demgegenüber werden aber im Anschluss an die Kinderrechtsbewegung auch (Teilhabe-)Rechte betont. Kinder und Jugendliche wachsen in vielfältig mit digitalen Medien ausgestatteten Haushalten auf. Ein Umgang mit digitalen Medienangeboten ist zur Befriedigung alltäglicher Bedürfnisse von Kindern und Jugendlichen notwendig. So fordert das UN-Kinderrechtskomitee u.a. den Zugang zu kindgerechten Onlineangeboten als Kinderrecht ein (vgl. UN 2021).

In diesem Spannungsfeld zeigt sich, dass sich der Erziehungs- und Bildungsauftrag auf die aktuelle Lebenslage von Kindern und Jugendlichen beziehen und gleichzeitig auf die zukünftige Rolle der Individuen in einer zunehmend von digitalen Medien geprägten Gesellschaft ausgerichtet sein muss.

Die Beschlüsse der Kultusministerkonferenz (KMK 2012, 2016) und der Digitalpakt von BMBF und KMK (2017) spiegeln die bildungspolitischen Reaktionen hierauf wider. Im Zentrum steht dabei die Förderung individueller Kompetenzen im Umgang mit digitalen Medien, die für eine aktive, selbstbestimmte Teilhabe in einer digitalen Welt erforderlich sind. Mit dem Digitalpakt für Schulen und den Länderprogrammen werden derzeit in großem Stil Schulen mit digitalen Medien ausgestattet, und es sollen schulische Medienbildungskonzepte entwickelt werden, die auf eine Förderung der Kompetenzbereiche

1 Der Gefährdungsatlas unterscheidet über 30 verschiedene Arten von Gefährdungen und verdeutlicht, dass auch Jugendliche sich selbst in vielfältiger Weise strafbar machen können.

»Suchen und Verarbeiten«, »Kommunizieren und Kooperieren«, »Produzieren und Präsentieren«, »Schützen und sicher agieren«, »Problemlösen und Handeln« sowie »Analysieren und Reflektieren« abzielen. In den Schulen ist die Umsetzung als »integrativer Teil der Fachcurricula aller Fächer« (Tulodziecki/Grafe/Herzig 2019: 197ff.) vorgesehen.

Während diese »digitalen Kompetenzen« in der Diskussion hohe Beachtung fanden, spielt auf Ebene der Zielfragen der Begriff der »digitalen Souveränität«[2] bislang eine eher untergeordnete Rolle: Zentrale Positionspapiere mit explizitem Bezug zur Souveränität waren *Souveränität und Verantwortung in der vernetzten Medienwelt,* eine Stellungnahme des Bundesjugendkuratoriums (vgl. BJK 2013), und (breiter rezipiert) das Gutachten des Aktionsrats Bildung *Digitale Souveränität und Bildung* (ARB 2018). Sie verdeutlichen, dass Souveränität auf Handlungsmöglichkeiten der Individuen zielt. Der Aktionsrat Bildung versteht unter »digitaler Souveränität« die Möglichkeit,

> »digitale Medien selbstbestimmt und unter eigener Kontrolle zu nutzen und sich an die ständig wechselnden Anforderungen in einer digitalisierten Welt anzupassen. Digital souveränes Handeln ist einerseits an individuelle Voraussetzungen gebunden, nämlich eine hinreichende Medienkompetenz der Person, und andererseits an die Bereitstellung entsprechender Technologien und Produkte.« (ARB 2018: 12)

3. Medienbildung, Medienkompetenz und »digitale Souveränität« im erziehungswissenschaftlichen Fachdiskurs

Der Kern der individuellen Souveränität, also die Möglichkeit zu selbstbestimmtem Handeln unter gegebenen gesellschaftlichen Rahmenbedingungen, wird im erziehungswissenschaftlichen und medienpädagogischen Fachdiskurs vorrangig unter dem Bildungsbegriff diskutiert:

2 Er wird insgesamt – so zeigt der vorliegende Sammelband deutlich – über die verschiedenen Fachdisziplinen hinaus kontrovers und mit je unterschiedlichem Zugang und/oder Fokus diskutiert. In der Rechtswissenschaft beispielsweise wird die Souveränität des Staates der Privatautonomie des Individuums gegenübergestellt (s. hierzu insbesondere die Ausführungen von Rückert/Safferling/Hofmann 2022 in diesem Band).

> »Bildung wird […] verstanden als Befähigung zu vernünftiger Selbstbestimmung, die die Emanzipation von Fremdbestimmung voraussetzt oder einschließt als Befähigung zur Autonomie, zur Freiheit eigenen Denkens und eigener moralischer Entscheidungen. Eben deshalb ist denn auch Selbsttätigkeit die zentrale Vollzugsform des Bildungsprozesses.« (Klafki 2007: 19)

In der Bildungstheorie sind sowohl der transitive (jemanden nach einem vorab bestimmten Bilde bilden, das sog. »Handwerkermodell«) als auch der reflexive bzw. klassische Bildungsbegriff (sich selbst bilden) bekannt. Während der transitive Bildungsbegriff vor allem auf Bildung in formalen Kontexten mit ihren räumlichen und zeitlichen Abgrenzungen zu ihrer Umwelt fokussiert und eine im engeren Sinne schulpädagogische Auffassung des Bildungsbegriffs widerspiegelt, ist beim reflexiven bzw. klassischen Bildungsbegriff, der in der aktuellen Bildungstheorie dominiert, diese Limitierung im Sinne einer kontextübergreifenden und lebenslangen Weiterentwicklung des reflexiven Verhältnisses zu sich selbst, zum Anderen und der Welt nicht gängig. Anthropologisch betrachtet ist das Verhältnis zum sozialen Anderen und der Welt stets schon medial vermittelt. Da reflexive Prozesse auf dem repräsentationalen Denken, also dem Gebrauch von Zeichen, beruht, schließt Bildung Medienkompetenz notwendigerweise als Voraussetzung mit ein (vgl. Spanhel 2010a: 46f.).

Begünstigend für die Verbreitung des Begriffs »Medienbildung« war eine gewisse Renaissance des allgemeinen Bildungsbegriffs: Wurde Mitte der 1960er-Jahre versucht, den Bildungsbegriff als Leitbegriff zu vermeiden und durch »vermeintlich theoretische Äquivalente« (Hansmann 1988: 21) zu ersetzen, so können gegenwärtig Bemühungen um Rekonstruktion und Revision des Bildungsbegriffs festgestellt werden. Es werden Anschlüsse an die Tradition der Bildungstheorie gesucht. Dabei lässt sich für den medienpädagogischen Fachdiskurs zeigen, dass diese Bemühungen direkt in die Entwicklung einer Theorie der Medienbildung eingegangen sind. So wurde von Marotzki, aufbauend auf den Entwurf einer allgemeinen strukturalen Bildungstheorie, eine Theorie der Medienbildung vorgelegt (vgl. Marotzki 2004; Jörissen/Marotzki 2009).

Eine ganz andere Traditionslinie weist der Begriff der schulischen Medienbildung auf. Im formalen Bildungskontext folgt der Begriff »Medienbildung« meist dem schulpädagogischen Verständnis. Wenn Medien als Gegenstand des Unterrichts überhaupt aufgegriffen wurden, dann im Sinne einer Film- oder Fernseherziehung oder einer Pädagogik der Massenmedien. Computer und Internet wurden lange unabhängig davon als informationstechnische

Grundbildung thematisiert. Dementsprechend wurde laut Tulodziecki der Begriff der Medienbildung »eher aus pragmatischen, denn aus bildungstheoretischen Gründen eingeführt« (Tulodziecki 2011: 27), um diese beiden Handlungsfelder zusammenzuführen. Die Diskussion um dessen theoretische Präzisierung entwickelte sich erst in den folgenden Jahren, z.B. durch die Arbeiten von Marotzki (2004), Schorb (2009) und Spanhel (2010b).

Im medienpädagogischen Fachdiskurs wird Medienbildung meist als lebenslanger Bildungsprozess verstanden, der in unterschiedlichen Kontexten stattfindet und in dessen Rahmen durch eine aktive und reflektierende Auseinandersetzung mit Medien und deren Folgen zunehmend Medienkompetenz entwickelt wird. »Medienkompetenz« ist der Zielbegriff, »Medienbildung« der Begriff zur Beschreibung des dazugehörigen Entwicklungsprozesses (vgl. Tulodziecki 2011). Dieses Grundverständnis findet sich auch in unterschiedlichen Studien und Positionspapieren wieder. So wird in der Erklärung der Kultusministerkonferenz (KMK 2012: 3) schulische Medienbildung verstanden als ein »dauerhafter, pädagogisch strukturierter und begleiteter Prozess der konstruktiven und kritischen Auseinandersetzung mit der Medienwelt. […] Sie zielt auf den Erwerb und die fortlaufende Erweiterung von Medienkompetenz […].«

Der in dem medienpädagogischen Fachdiskurs neben Medienbildung mindestens ebenso zentrale Begriff der Medienkompetenz kann auf Dieter Baackes Adaption des Konzeptes »Kommunikative Kompetenz« (vgl. Habermas 1971) zurückgeführt werden. Ausgehend von der potenziellen Fähigkeit jedes Menschen, situations- und aussagenadäquat zu kommunizieren, rückte Baacke die Kompetenzen in den Mittelpunkt, die nötig sind, um in von Massenmedien geprägten Demokratien zu partizipieren (vgl. Baacke 1975). Mit der Konzeptionierung von Massenmedien als »vierte Gewalt« in Demokratien wurden mündige, kritikfähige Rezipierende als notwendig erachtet. Entsprechend standen in der Medienpädagogik die Befähigung zur Kritik der Massenkommunikation und der Erwerb solcher Kompetenzen, die nötig sind, um eigene Interessen mithilfe von Medien auszudrücken, besonders im Vordergrund. Als »Medienkompetenz« wird im Fachdiskurs der Teil kommunikativer Kompetenz und sozialer Handlungsfähigkeit verstanden, den Kinder und Jugendliche für die Bewältigung zentraler Entwicklungsaufgaben und für eine souveräne Lebensführung in einer mediatisierten Gesellschaft erwerben müssen. Hierzu gehören: (1) das Wissen und die Reflexion über die Strukturen, Angebote und Funktionen der jeweils aktuellen Medienwelt; (2) Kompetenzen zum selbstbestimmten Gebrauch von Medien als Mittel und

Wege der Artikulation und Partizipation; und (3) die Befähigung zu fortwährender eigen- und sozialverantwortlicher Positionierung zur jeweils aktuellen Medienwelt sowie zum eigenen Medienhandeln und dem Medienhandeln anderer in dieser mediatisierten Welt (vgl. Eickelmann/Aufenanger/Herzig 2014: 8).

> »Medienkompetenz wird dabei verstanden als integrierter Bestandteil von kommunikativer Kompetenz und von Handlungskompetenz. Sie bildet eine wesentliche Voraussetzung für eine souveräne Lebensführung, die zunehmend davon geprägt ist, mit und über Medien das eigene Leben zu gestalten.« (Schorb/Wagner 2013: 18)

Im fachlichen Diskurs wird kontrovers diskutiert, ob die etablierten Konzepte der Medienbildung und der Medienkompetenz die Komplexität der tiefgreifenden Mediatisierung und der Digitalisierung noch ausreichend erfassen. Hierzu finden sich insbesondere zwei Forderungen: Erstens bedarf es einer Aktualisierung der Konzepte, um digitale Technologien und ihre Charakteristika – wie digitale bzw. informatische Aspekte (vgl. Dander 2014; Grimm/Keber/Zöllner 2015; Autorengruppe [AG] Dagstuhl-Erklärung 2016; Pangrazio/Selwyn 2018; Autorengruppe [AG] Frankfurt-Dreieck 2019) angemessen zu berücksichtigen. Mit Begriffen wie »Digitale Bildung« und »Bildung in der digitalen Welt« wird dieser Anspruch neuerer Konzepte markiert. Hierzu gibt es aber auch eine kritische Auseinandersetzung, insbesondere zu Digitaler Bildung (vgl. Niesyto 2021).

Zweitens wird gefordert, das kommunikationstheoretische Konzept der Medienkompetenz in ein durch die empirische Bildungsforschung validiertes Kompetenzmodell zu überführen. Tatsächliche Kompetenzmessungen bei Kindern und Jugendlichen finden derzeit noch selten statt (etwa Bos et al. 2014; Sowka et al. 2015; Eickelmann et al. 2019). Studien zur Medienbildung/-kompetenz basieren stattdessen vielfach auf Selbsteinschätzungen (s. Rott 2020) oder beschränken sich auf Teilaspekte (vgl. Gapski 2001). Bestehende Modellierungen sind zum einen der Kritik ausgesetzt, dass sie nicht die Breite und Reflexivität der Medienkompetenz im Sinne des ursprünglichen Konzeptes abbilden und so ein verkürztes Verständnis von Medienkompetenz repräsentieren. Zum anderen zeigen sich Schwierigkeiten bei der Berücksichtigung der Lebenswelten von Kindern und Jugendlichen sowie deren heterogenen Medienumgebungen (s.u.).

Vor dem Hintergrund dieser – hier verkürzt dargestellten – Diskurslinien wird der Nutzen des Souveränitätsbegriffs als möglicher neuer Fachbegriff

ambivalent betrachtet. Ein Blick auf gegenwärtige Begriffsverwendungen in der aktuellen Literatur zeigt, dass Souveränität von Individuen vor allem in Bezug auf Selbstbestimmung, Bildung und Kompetenz diskutiert wird.

»Digitale Souveränität« erfreut sich in den letzten Jahren in politischen und wirtschaftsorientierten Strategiepapieren, aber auch zunehmend in wissenschaftlichen Auseinandersetzungen großer Beliebtheit. Lepping und Palzkill (2017) schlagen vor, verschiedene Ebenen »digitaler Souveränität« zu unterscheiden, und zwar die von Gesellschaft, Organisationen und Individuen. Christmann-Budian und Geffers (2017) verdeutlichen in diesem Zusammenhang, dass »digitale Souveränität« von Individuen auf der Grundlage anderer Voraussetzungen entstehe und damit auch anderen Risiken ausgesetzt sei als die »digitale Souveränität« von Staaten oder Unternehmen (vgl. ebd.: 119). Dennoch ist die Perspektive von Individuen nur gelegentlich Gegenstand der (wissenschaftlichen) Auseinandersetzung (vgl. Stubbe 2017: 43). Individuen geraten hierbei als Nutzer*innen (Stichwort *user empowerment*), Verbraucher*innen, Bürger*innen oder (zukünftige) Arbeitnehmer*innen in den Blick. Mit besonderem Bezug auf die Perspektive Jugendlicher existieren zwei einander gegenüberstehende Verwendungsweisen des Konzepts der »digitalen Souveränität«.

Auf der einen Seite finden sich Veröffentlichungen, die »digitale Souveränität« ausschließlich oder hauptsächlich als individuell zu lösende Aufgabe rahmen. Hierzu gehört etwa die Einschätzung des Aktionsrates Bildung (ARB). Dieser versteht unter »digitaler Souveränität« die Möglichkeit, »digitale Medien selbstbestimmt und unter eigener Kontrolle zu nutzen und sich an die ständig wechselnden Anforderungen in einer digitalisierten Welt anzupassen« (ARB 2018: 12). Sie sei geknüpft an individuelle Voraussetzungen und die »Bereitstellung entsprechender Technologien und Produkte« (ebd.). Die angesprochene Anpassung wird dabei als Aneignung neuer Anwendungskompetenzen im Rahmen informeller Lernprozesse umgesetzt (ebd.: 61; die kontinuierliche Weiterentwicklung digitaler Kompetenzen fordert auch Krings 2016). Es geht dem ARB beim Thema »digitale Souveränität« um die Gestaltung der digitalen Transformation, um gesellschaftliche Teilhabe, um den Erhalt von Wettbewerbsfähigkeit und somit auch um den Erhalt von Wohlstand (vgl. ARB 2018: 7). Auch Lena-Sophie Müller (2016) kann zu dieser Gruppe gerechnet werden. Sie setzt sich mit der Frage auseinander, ob und wie es möglich wäre, für das Agieren im digitalen Raum ein »Bauchgefühl« zu entwickeln, und unterstreicht hierfür die Notwendigkeit, eine Technik-, Meinungsbildungs- und

Sozialkompetenz auszubilden sowie »ein gesundes Rechts- und ein versiertes Datenbewusstsein im Netz« (ebd.: 270) zu entwickeln.

> »Die Untersuchungen der Initiative D21 belegen seit mehreren Jahren, dass ›digitale Souveränität‹ strukturell maßgeblich durch das Bildungsniveau und die erworbene Kompetenz bestimmt wird. Angesichts der fortschreitenden Digitalisierung aller Lebensbereiche darf digitale gesellschaftliche Teilhabe aber keine Frage von Bildung, Alter, Wohnort, Einkommen und Geschlecht sein.« (Ebd.: 279)

Neben einer Schwerpunktsetzung auf individuelle Verantwortung und Fähigkeiten sind die entsprechenden Publikationen vielfach eher politisch oder wirtschaftlich argumentierende Strategiepapiere als wissenschafts-theoretische Annäherungen, die eine marktwirtschaftliche Eignung von Menschen zum Ziel haben (vgl. auch SVRV 2017).

Auf der anderen Seite gibt es wissenschaftsnähere Publikationen, die der Notwendigkeit Rechnung tragen, neben individuellen auch weitere Faktoren bei der Betrachtung »digitaler Souveränität« von Nutzer*innen zu berücksichtigen. Stubbe (2017: 44) schlägt vor, den sozialen Aspekt »digitaler Souveränität« auch unter dem Gesichtspunkt der Teilhabegerechtigkeit einzubeziehen und dabei neben einem kompetenten auch einen verantwortungsvollen »Umgang mit Technik sowie mit ihren Auswirkungen und Chancen« (ebd.) als wesentliches Element »digitaler Souveränität« aufzunehmen. Zentral ist dabei Stubbes Forderung, dass Einzelne nur dort Verantwortung übernehmen könnten, wo ihnen die rechtlichen Rahmenbedingungen auch Spielräume dafür zur Verfügung stellen (vgl. ebd.: 57). Er macht deutlich, dass die »digitale Souveränität« nicht dasselbe abbilde wie etwa der Begriff der Medienkompetenz (vgl. ebd.: 55f.). Vielmehr könne diese nur im Zusammenhang von digitaler Welt und sozialem Leben erfasst werden – zwei Bereichen, die, folgt man Stubbe, untrennbar miteinander verbunden sind. Auch Groebel (2016) unterstreicht in seinem Beitrag den sozialen Bezug »digitaler Souveränität« von Individuen (ebd.: 399). Er definiert psychologische Einflussfaktoren auf die »digitale Souveränität« Einzelner und bildet diese in einer »Digitalsouveränitäts-Matrix« (ebd.: 408) ab. Dabei zeigt er auf, inwiefern Emotionen, Kognitionen, Soziales, Werte und das Handeln eines Menschen dessen »digitale Souveränität« verändern können. Goldacker definiert »digitale Souveränität« als »die Summe aller Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können.« (Goldacker 2017: 3). Sie betont dabei diverse Abhän-

gigkeiten der »digitalen Souveränität« von Nutzer*innen, etwa von der »digitalen Souveränität« des Staates (vgl. ebd.: 9). Auch Brüggen (2015) verweist in der Auseinandersetzung mit der Frage nach souveräner Lebensgestaltung in einer digital geprägten Welt auf die Notwendigkeit, »bei der Suche nach Lösungen den Fokus über die individuelle Selbstverantwortung aus[zu]weiten« (ebd.: 57). Diese zweite Gruppe an Konzepualisierungen verweist auf das Potenzial, Souveränität im Kontext digitaler Medien und Infrastrukturen relational zu fassen. Dabei erfordert die Allgegenwart einer tiefgreifenden Mediatisierung den Einbezug einer Vielzahl von rahmenden Bedingungen.

4. »Digitale Souveränität« als relationales Konzept

Inwiefern überhaupt eine selbstbestimmte Nutzung digitaler Medien möglich sein kann, wird u.a. mit dem Konzept der »digitalen Souveränität« diskutiert. Im Anschluss an die vorangegangene Darstellung können souveräne Medienpraktiken relational betrachtet werden. Die Relationalität verweist dabei auf:

- individuelle Voraussetzungen (z.B. kognitive und moralische Entwicklung, Medienrepertoire und -kompetenz)
- personenexogene Faktoren (Technologien und Produkte, rechtliche, ökonomische, soziale und organisatorische Rahmenbedingungen)

Im Folgenden soll insbesondere auf Aspekte eingegangen werden, die verdeutlichen, wie »digitale Souveränität« in Relation zu personenexogenen Faktoren steht.

Medienbildung und Medienkompetenz werden auf die individuelle Handlungsfähigkeit bezogen. Diese ist jedoch in Zeiten tiefgreifender Mediatisierung in immer komplexeren Gefügen mit exogenen Faktoren verwoben. Der Ansatz der kommunikativen Figurationen (vgl. Hepp/Hasebrink 2014) illustriert dies in geeigneter Weise (Kammerl et al. 2020) und dient deshalb in diesem Beitrag als Bezugstheorie zur Auseinandersetzung mit individueller »digitaler Souveränität«. Ihm zufolge ist das Zusammenleben der Menschen in einer Gesellschaft charakterisiert durch die Einbindung in unterschiedliche kommunikative Figurationen. Diese umfassen die Interdependenzgeflechte verschiedener Akteur*innen spezifischer sozialer Domänen (etwa Familie, Schule, Freundeskreis). Indem das Konzept entsprechende Konstellationen von Akteur*innen fokussiert, erlaubt es den Einbezug von Praktiken ein-

zelner Akteur*innen und der Herstellung von Gesellschaft. Damit hebt es die traditionelle Unterscheidung von Individuum und Gesellschaft auf und erkennt an, dass beide nur zusammen gedacht und beschrieben werden können. Vor dem Hintergrund sozialer und technologischer Entwicklungen sowie aufgrund »fluktuierender Machtbalancen« (Elias: 1971: 143) und affektiver Bindungen (Valenzen) zwischen den beteiligten Akteur*innen sind Beziehungsnetzwerke kontinuierlichen Veränderungsprozessen unterworfen. Insofern können kommunikative Figurationen nicht als starre Gebilde gesehen werden, sondern müssen stets sowohl in ihrer Prozesshaftigkeit als auch ebenenübergreifend, also unter Einbeziehung individueller und geteilter Aspekte, betrachtet werden.

Während die sich wandelnde Medienumgebung Technologien, Anwendungen, Medien- bzw. Technikunternehmen sowie deren gesellschaftliche Regulierung beschreibt, bezieht sich das sich ebenfalls verändernde Medienensemble auf das unmittelbare ökologische Zentrum[3] eines Individuums und dessen Medienbiografie. In Familien oder auch in Schulen stehen den Mitgliedern dieser sozialen Domänen Medienangebote zur Verfügung, die nach sozialen Regeln und Rollen räumlich verteilt und unterschiedlich zugänglich gemacht werden. Die Medienpraktiken folgen also nicht allein den Merkmalen der technologischen Möglichkeiten, sondern sind sozial mitbestimmt. Darüber hinaus nimmt der Ansatz der kommunikativen Figuration auf das individuelle Medienrepertoire Bezug. Dieses umfasst alle Medienangebote, die ein Individuum regelmäßig in seine Alltagspraktiken einbezieht, und die Art und Weise, wie es unterschiedliche Medien kombiniert. Das Medienrepertoire bezeichnet also ein relativ stabiles, individuelles und medienübergreifendes Muster der Medienpraktiken, das die Individuen – orientiert an übergreifenden Prinzipien wie z.B. Nützlichkeit, Involvement oder Effektivität – entwickeln (vgl. Hasebrink/Hölig 2017). In der kommunikationswissenschaftlichen Forschung diente der Repertoireansatz ursprünglich dazu, Rezeptionsmuster von Nachrichten und Informationsquellen zu untersuchen (vgl. Kim 2016), und wurde inzwischen um weitere (digitale) Medienangebote und medienbiografische Perspektiven erweitert (vgl. Ytre-Arne 2019). Paus-Hasebrink und

3 Nach dem Ansatz der Ökologie der menschlichen Entwicklung (vgl. Bronfenbrenner 1981) ist die unmittelbare physische und soziale Umwelt eines Kindes (Mikrosystem) besonders bedeutsam für dessen Entwicklung. Wechselwirkungen der unmittelbaren Umwelt werden im Mesosystem, größere soziale Systeme im Exo- und Makrosystem berücksichtigt.

Hasebrink (2014) schlagen vor, dabei die Gesamtheit aller medialen und nicht medialen kommunikativen Handlungen eines Individuums in den Blick zu nehmen und den Ansatz des Medienrepertoires auf ein Kommunikationsrepertoire zu erweitern.

Figurationen sind klar umgrenzt, stehen aber miteinander in Beziehung. Kommunikative Praktiken prägen das soziale Miteinander in den Figurationen. Sie sind auf ein figurationsspezifisches Medienensemble bezogen, welches sie ausgehend von der Medienumgebung (grundsätzlich zur Verfügung stehende Medienangebote) zusammenstellen und an einem thematischen Rahmen orientieren. Eine Person erstellt sich ein individuelles Medienrepertoire wiederum als einen Auszug der Medienensembles der verschiedenen kommunikativen Figurationen, denen sie angehört (Paus-Hasebrink/Hasebrink 2014). Eine Analyse der »digitalen Souveränität« von Individuen muss deshalb das Medienrepertoire untersuchen, das Individuen in der Auseinandersetzung mit den Medienensembles und Akteur*innenkonstellationen ihrer Lebenswelt herausbilden und kontinuierlich weiterentwickeln.

Die Prozesshaftigkeit des Ansatzes kommunikativer Figurationen lässt sich auf zwei Ebenen konkretisieren. Erstens kann mit der Einbettung in das Konzept ein dynamischer Bildungsprozess in den Blick genommen werden, der sich durch fluktuierende Machtbalancen und sich wandelnde Valenzen innerhalb sozialer Domänen fassen lässt. Zweitens vermag der Ansatz gerade den Wandel des Verhältnisses formaler und informeller Kontexte adäquat zu beschreiben. Diese sind weder als deutlich getrennt noch als gänzlich entgrenzt und vermengt zu verstehen. Mit Elias (1971) lässt sich tiefgreifende Mediatisierung als ein zunehmender Integrationsprozess beschreiben: Die Beziehungsgeflechte werden infolge der Mediatisierung dichter, differenzierter und verfestigen sich gleichzeitig.

Bezogen auf Jugendliche bedeutet das: Die Medienpraktiken der Jugendlichen sind in soziale Kontexte eingebunden, in denen Eltern als Rollenvorbilder dienen (vgl. Knop/Hefner 2018) und die eigene hohe/geringe Medienkompetenz weitergeben (vgl. Livingstone 2017), ein Medienensemble vorgeben und mit medienerzieherischen Praktiken den Gebrauch des individuellen Medienrepertoires regulieren (vgl. Kammerl et al. 2020; Knop/Hefner 2018; Shin/Kang 2016; Wagner et al. 2013). Kammerl et al. (2020) fanden heraus, dass z. B. Macht, Regeln oder Bindungen zwischen Menschen diese sozialen Kontexte prägen und damit kommunikative Praktiken beeinflussen. Später generieren dann Freund*innen/Peers über Nutzungsentscheidungen sozialen Druck be-

zogen auf die Gestaltung individueller Medienrepertoires und entscheiden so letztlich über soziale Anerkennung oder Ausgrenzung der Heranwachsenden (vgl. Marwick/boyd 2014; Gapski 2015; Gebel/Wütscher 2015; Agosto/Abbas 2017; Brüggen et al. 2019). Viele junge Menschen glauben, dass sie nur die Wahl haben, sich entweder diesem Druck zu beugen oder Gefahr zu laufen, sozial isoliert zu werden. Sozioökonomischer Status, Bildungshintergrund und Ressourcen der Familien determinieren darüber hinaus die Fähigkeiten, welche Jugendliche im Umgang mit (digitalen) Medien entwickeln, da sich dadurch erklärt, welche Medienausstattung zur Verfügung steht, welche medienbezogene Verhaltensmuster als Vorbilder zur Verfügung stehen und welche Hilfestellungen dazu die Familienangehörigen anbieten können (vgl. Hargittai 2010; boyd/Hargittai 2013; Kutscher 2014; Brüggen et al. 2019; Eickelmann et al. 2019; Zilka 2019).

Die durch Familien/Peers vorgegebenen Medienensembles sind Auszüge der Medienumgebung, welche technisch ausgestaltet ist. Jugendlichen stehen dabei immer bedienfreundlichere *user interfaces* zur Verfügung, die dahinter ablaufenden Prozesse werden für sie jedoch unverständlicher (vgl. Dander/Aßmann 2015; Matzner/Richter 2017). Benenson, Freiling und Meyer-Wegener verweisen in diesem Zusammenhang darauf, dass es Nutzer*innen vielfach schwerfällt, »mögliche Bedrohungen für die Sicherheit und den Schutz der Privatsphäre realistisch wahrzunehmen« (2022: 62; in diesem Band). Darüber hinaus würden auch die tatsächlichen Möglichkeiten zur Kontrolle über eigene Endgeräte immer weiter eingeschränkt (ebd.: 67ff.). Auch ohne bewusst etwas über sich selbst zu veröffentlichen, produzieren sie online permanent Daten und hinterlassen einen »digitalen Fußabdruck« (Livingstone 2017: 28). Daten werden kontinuierlich aggregiert und algorithmisch analysiert, um Nutzungsprofile, automatisierte Empfehlungen und personalisierte Newsfeeds oder Werbung zu generieren (vgl. Wagner/Gebel/Lampert 2013; Mascheroni 2018; Brüggen et al. 2019). Jugendliche sind also kontinuierlich der Gefahr der Manipulation ausgesetzt, wodurch eine gewisse Hilflosigkeit entsteht (vgl. Wagner/Gebel/Lampert 2013; De Mooy 2017). Dennoch setzt sich die Informatik nur selten mit Fragen des *user empowerment* auseinander (etwa Schäwel 2018; s. Bräunlich et al. 2020).

Die Gestaltung der Medienumgebung ist darüber hinaus rechtlich determiniert. Anbieterseitig ist die Umsetzung geltenden Rechts vor allem ökonomisch motiviert (vgl. Livingstone et al. 2012). Rückert, Safferling und Hofmann (2022; im gleichen Band) unterstreichen in diesem Zusammenhang die Gefahr einer schleichenden Entmündigung der Nutzer*innen, und Hof-

mann (2019) beschreibt eine Privatisierung der Rechtsdurchsetzung, etwa indem allgemeine Geschäftsbedingungen unverständlich sind (vgl. Creswick et al. 2019) oder die Nutzung durch Jugendliche ausschließen, obwohl diese zur Hauptnutzungsgruppe eines Angebots gehören (vgl. Brüggen et al. 2019). Internetnutzer*innen fühlen sich zudem angesichts der Datenerhebung durch Unternehmen und Staaten zunehmend hilflos (vgl. De Mooy 2017; Stoilova/Nandagiri/Livingstone 2021). Eine garantierte Sicherheit von Onlineaktivitäten mit personenbezogenen Daten ist jedoch von grundlegender Bedeutung, damit Jugendliche auf digitale Technologien vertrauen können. Geltendes Recht und die darauf bezogene Rechtsprechung hinken zudem technologischen Entwicklungen hinterher (vgl. ebd.; Cap 2017; Gräf/Lahmann/Otto 2018). Nach wie vor sind sie an Angeboten und Inhalten statt an Medienpraktiken Jugendlicher ausgerichtet (vgl. Brüggen et al. 2019; Bulger et al. 2017) und orientieren sich an Sorgen und Ängsten von Eltern/Erwachsenen (vgl. ebd.; Drotner 1999; Staksrud 2013; Livingstone 2017), wodurch Risiken für Jugendliche zwar minimiert, aber auch ihre Chancen beschränkt werden können (vgl. u.a. Bulger et al. 2017; Livingstone 2017; Brüggen et al. 2019).

Der Forschungsstand illustriert, dass die Handlungsfähigkeit Jugendlicher auf die Ebene des eigenen Medienrepertoires beschränkt ist und dieses durch eine Vielzahl externer Faktoren beeinflusst wird, die wiederum umfassend miteinander verwoben sind. Er zeigt, dass diese Einflussfaktoren bisher weder systematisch zueinander in Beziehung gesetzt noch in ihrem Zusammenspiel empirisch untersucht wurden, und deckt somit insbesondere für die Perspektive der Medienpraktiken Jugendlicher deutliche Lücken auf. Um Gestaltungsspielräume im Umgang mit und Abhängigkeit von digitalen Medien verstehen und beeinflussen zu können, müssen dementsprechend externe Einflüsse in ihrer Relationalität zu individuellen Faktoren berücksichtigt werden. Hierfür eignet sich das Konzept »digitaler Souveränität«, da es im Umgang mit digitalen Medien individuelle, soziale, technische und rechtliche Perspektiven zueinander in Beziehung setzt.

5. Ausblick auf Forschung und Bildungspraxis

Der Medienrepertoireansatz ermöglicht ein relationales Verständnis von »digitaler Souveränität«, indem er die Verschränkung des Individuums mit den ihm zur Verfügung stehenden Medienensembles seiner kommunikativen Figurationen und der sich wandelnden Medienumgebung erlaubt. Den

Ausgangspunkt für Forschungsprojekte zur »digitalen Souveränität« von Heranwachsenden stellen dabei konkrete Medienpraktiken dar, die vor dem Hintergrund der jeweils spezifisch gegebenen Konstellation der Akteur*innen und unter Einbezug von Machtbalancen und Valenzen analysiert werden. Dies schließt die zentralen sozialen Domänen (etwa Familie, Schule, Peergroup) ein und berücksichtigt die soziale Lage der Individuen. Für die Forschung gilt es, Medienrepertoires und Medienpraktiken nicht losgelöst von ihrem sozialen Kontext zu untersuchen und zu bewerten. Ausgehend von einem relationalen Verständnis werden von dieser Ebene aus Praktiken einzelner Akteur*innen und die Gesellschaft als Ganzes berücksichtigt. Damit sollen Individuum und Gesellschaft zusammen gedacht und untersucht werden. Die »digitale Souveränität« der Individuen kann nur in digital souveränen Gesellschaften entwickelt werden.

Damit lassen sich aus medienpädagogischer und erziehungswissenschaftlicher Perspektive Schlussfolgerungen für die Zielkategorie »digitale Souveränität« ziehen. Statt – wie in der Definition des Aktionsrates Bildung zum Ausdruck gebracht – einer *Anpassung* an die Anforderungen einer zunehmend von Digitalisierung geprägten Welt ist deren *(Mit-)Gestaltung* als Bildungsziel zu fassen. In demokratischen Entscheidungsprozessen über die Gestaltung der Digitalisierung sollte deshalb die Beteiligung der heranwachsenden Generation sichergestellt werden. Bildung muss über eine reine Einführung in die digitale Gesellschaft oder eine Anpassung an diese hinausgehen. Wenn in der Tradition der klassischen Bildungstheorie der Zweck des Bildungssystems allein darin gesehen werden kann, dass die nachwachsenden Generationen ihre Fähigkeit zur Selbstbestimmung entwickeln, dann ist entsprechend zu prüfen, welche Kompetenzen gefordert sind, um in einer von digitalen Medien geprägten Gesellschaft partizipieren und diese gestalten zu können. Nach Einschätzung der Autor*innen sollte die Förderung »digitaler Souveränität« daran anschließend auf zwei Ebenen ansetzen.

Auf der Ebene endogener Bedingungen geraten insbesondere Kompetenz und Selbstbestimmung derjenigen in den Blick, die Medien in Gebrauch nehmen. Deshalb stehen für die Bildungspraxis unseres Ermessens folgende Fokusse im Vordergrund:

1. Während Heranwachsende sich im Rahmen des Sozialisationsprozesses vor allem instrumentelle Fertigkeiten selbst aneignen, sind sie bei der Entwicklung ihrer Fähigkeit zur (kritischen) Reflexion der mediatisierten Gesellschaft und eigener Medienpraktiken auf Unterstützung angewie-

sen. Jugendliche können zwar schnell die Verwendung von kostenlosen Onlinediensten erlernen, die Geschäftsmodelle der Anbietenden verstehen sie aber nicht (unbedingt) gleichermaßen, und auch die geltenden rechtlichen Regelungen werden nicht en passant erworben, sondern müssen vermittelt werden. Aus beiden Perspektiven heraus spielt das Wissen um die Datenspuren, die eigene Medienpraktiken hinterlassen, eine zentrale Rolle. Deutlich wird damit die Bedeutung einer Kompetenz zur Reflexion von Medienangeboten, -strukturen und eigener wie fremder Medienpraktiken. Es ist deshalb notwendig, dass in pädagogischen Prozessen diese unsichtbaren Zusammenhänge erfahrbar und hinterfragbar gemacht werden.

2. In der Verwendung digitaler Medien bleiben Heranwachsende zudem meist in der Rolle der Konsument*innen und Nutzer*innen stehen. Statt sich auf Rezeption und Liken zu beschränken, muss auch eine Befähigung zur Artikulation eigener Standpunkte und deren Aufbereitung in einer ansprechenden Form stattfinden. Die Dynamik des digitalen Wandels verdeutlicht, dass sich Interaktions-, Informations- und Kommunikationsmöglichkeiten rasch weiterentwickeln. Heranwachsende sollten Gestaltungsmöglichkeiten erkennen lernen und selbst die Erfahrung machen, neue Anwendungen entwickeln zu können. Die Fähigkeit zur Unterscheidung von Scheinbeteiligung und Partizipation wird dabei ebenso wie die Differenzierung zwischen Fake News und vertrauenswürdigen Informationen immer bedeutsamer. Angesprochen sind damit nicht nur die Kompetenzen der Jugendlichen, sondern auch deren Selbstbestimmung: So muss sich ihre Kreativität nicht auf die Nutzung bestehender Kanäle beschränken, sondern kann darüber hinaus auch innerhalb vorhandener Kanäle eigene Wege gehen.

Die Befähigung zur Selbstbestimmung kann jedoch nicht allein als individueller Prozess verstanden werden. Die bisherigen Ausführungen unterstreichen demgegenüber die Bedeutung einer zweiten Ebene: der exogenen Bedingungen. Dabei steht neben der Selbstbestimmung auch die Frage nach der Sicherheit jugendlicher Medienpraktiken im Fokus.

3. Da eine Demokratie sicherstellen muss, dass sich nachkommende Generationen an der kollektiven Selbstbestimmung beteiligen, müssen Heranwachsende ermutigt und befähigt werden, sich in den politischen Diskurs einzubringen (beginnend in ihrem medienökologischen Zentrum). Dies

betrifft zunächst die Festlegung von Regeln im Umgang mit digitalen Medien zu Hause, in der Schule und in der Aushandlung mit den Peers. Wenn die Heranwachsenden, deren Eltern und die Lehrkräfte mehr über die Funktionsweisen digitaler Medien wissen und deren Einstellungen zielgerichteter nutzen können, könnten sie ihre Verwendung besser selbst regulieren. Deshalb muss eine Kompetenzförderung zunächst an dem konkret genutzten Medienensemble der Individuen ansetzen. Kollektive Selbstbestimmung bezieht sich aber auch auf das Themenfeld der Netzpolitik im weiteren Sinne. Netzgestützte Partizipationsmöglichkeiten und politische Diskurse im Netz sind dabei Gegenstände medienpädagogischer Arbeit mit Jugendlichen. Pädagogisch betrachtet eignen sich insbesondere auch Themen, welche die Lebenswelt der Adoleszenten unmittelbar betreffen, wie z.B. die Reform des Urheberrechts oder die Diskussion um die staatliche Beschränkung der Nutzungszeiten von Onlinegames nach chinesischem Vorbild.

4. Auch Fragen des Datenschutzes oder des Jugendmedienschutzes können nicht individualistisch auf den Kompetenzerwerb Einzelner verkürzt werden. Die Sicherheit jugendlicher Medienpraktiken wird maßgeblich durch exogene Faktoren beeinflusst: Insbesondere zentrale Schutzbestimmungen erfordern rechtliche und politische Maßnahmen. Daneben wäre auch eine (Selbst-)Verpflichtung der Anbietenden zur Einhaltung von Mindeststandards für jugendliche Medienpraktiken denkbar und sinnvoll (Möglichkeit, Accounts nur einem beschränkten Nutzer*innenkreis zugänglich zu machen; Blockier- und Meldefunktion; Beobachtung von Kriminalität auf den Plattformen u.v.a.m.).

Welche Implikationen ergeben sich daraus für die Bildungspraxis und den bildungspolitischen Diskurs? Eine verkürzte Forderung nach einer individuell zu entwickelnden Souveränität ist nicht nur unrealistisch, sondern droht zu einer Instrumentalisierung von Bildung zu führen. Problematiken, die primär auf staatlicher oder organisationaler Ebene zu lösen sind, können nicht erfolgreich auf individueller Ebene durch Lern- und/oder Bildungsprozesse bearbeitet werden. Stattdessen sollten Bildungsaufgaben an das Bildungssystem adressiert werden, die dort mit pädagogischen Mitteln bearbeitet werden können: Förderung von Reflexionsfähigkeit, Aktivierung von Produktivität und Kreativität sowie Befähigung zu einer diskursiven Beteiligung an der Kultivierung der digitalen Welt. Ansatzpunkte (medien-)pädagogischer Arbeit können dabei nicht nur Heranwachsende selbst und ihre eigenen Medien-

praktiken sein, sondern sollten ebenso Eltern und weiteres pädagogisches Personal umfassen.

Digitale Medien beeinflussen bereits vielfältig die Entwicklung von Kindern und Jugendlichen. Diese gesellschaftlich zugelassene Einflussnahme durch Medien muss reguliert und im Rahmen gesellschaftlicher Enkulturationshilfen in eine pädagogische Beeinflussung überführt werden, damit auch der nächsten Generation eine selbstbestimmte Lebensführung ermöglicht wird. Ausgehend von der These, dass der digitale Wandel Neuland ist, gibt es noch wenige kulturelle Traditionen, auf die dabei zurückgegriffen werden kann. Pädagogische Arbeit kann sich gerade hier nicht in der Tradierung von kulturell Bewährtem erschöpfen. Vielmehr gilt, dass Enkulturationshilfe bedeutet, kulturelle Produktivität und Kreativität der Heranwachsenden zu aktivieren und somit kulturelle Praxen neu zu erschaffen. Das Bildungssystem kann diesen Prozess unterstützen, indem es einerseits kritische Reflexionsfähigkeit fördert und andererseits einen produktiven und kreativen Umgang mit der Medienwelt eröffnet. Die bildungstheoretische Fundierung einer »Bildung in der digitalen Gesellschaft« spiegelt diese Perspektive wider und verdeutlicht, dass gerade im Bildungssystem pädagogische Begründungszusammenhänge für die Gestaltung des digitalen Wandels handlungsleitend sein sollten (vgl. Kammerl 2019).

Literaturverzeichnis

Agosto, Denise E./Abbas, June (2017): »›Don't be dumb—that's the rule I try to live by‹: A closer look at older teens' online privacy and safety attitudes«, in: New Media & Society 19, S. 347–365.

ARB – Aktionsrat Bildung (2018): Digitale Souveränität und Bildung. Gutachten, Münster: Waxmann.

Autorengruppe (AG) Dagstuhl-Erklärung (2016): Dagstuhl-Erklärung. Bildung in der digitalen vernetzten Welt. Eine gemeinsame Erklärung der Teilnehmerinnen und Teilnehmer des Seminars auf Schloss Dagstuhl – Leibniz-Zentrum für Informatik GmbH. Online unter: https://gi.de/fileadmin/GI/Hauptseite/Themen/Dagstuhl-Erkla__rung_2016-03-23.pdf, abgerufen am 12.01.2020.

Autorengruppe (AG) Frankfurt-Dreieck (2019): *Frankfurt-Dreieck* zur Bildung in der digital vernetzten Welt. Ein interdisziplinäres Modell. Online unter:

https://dagstuhl.gi.de/fileadmin/GI/Allgemein/PDF/Frankfurt-Dreieck-zur-Bildung-in-der-digitalen-Welt.pdf, abgerufen am 12.01.2020.

Baacke, Dieter (1975): Kommunikation und Kompetenz. Grundlegung einer Didaktik der Kommunikation und ihrer Medien, München: Juventa.

Benenson, Zinaida/Freiling, Felix/Meyer-Wegener, Klaus (2022): »Soziotechnische Einflussfaktoren auf die ›digitale Souveränität‹ des Individuums«, in: Georg Glasze/Eva Odzuck/Ronald Staples (Hg), Was heißt digitale Souveränität? Diskurse, Praktiken und Voraussetzungen »individueller« und »staatlicher Souveränität« im digitalen Zeitalter, Bielefeld: transcript, S. 61–87.

BJK – Bundesjugendkuratorium (2013): Souveränität und Verantwortung in der vernetzten Medienwelt. Anforderungen an eine kinder- und jugendorientierte Netzpolitik. Online unter: https://bundesjugendkuratorium.de/presse/souveraenitaet-und-verantwortung-in-der-vernetzten-medienwelt.html, abgerufen am 29.07.2022.

BMBF/KMK – Bundesministerium für Bildung und Forschung/Kultusministerkonferenz (2017): DigitalPakt Schule von Bund und Ländern. Gemeinsame Erklärung. Online unter: https://www.dstgb.de/aktuelles/archiv/archiv-2017/DStGB_zu_den_Eckpunkten_der_Bund-Laender_Vereinbarung_DigitalPaktSchule_/Ergebnis_Eckpunkte_St-AG_230517.pdf?cid=7p2, abgerufen am 29.07.2022.

BMFSFJ – Bundesministerium für Familie, Senioren, Frauen und Jugend (Hg.) (2017): Bericht über die Lebenssituation junger Menschen und die Leistungen der Kinder- und Jugendhilfe in Deutschland – 15. Kinder- und Jugendbericht, Berlin vom 01.02.2017. Online unter: https://www.bmfsfj.de/resource/blob/115438/d7ed644e1b7fac4f926619145990 3c62/15-kinder-und-jugendbericht-bundestagsdrucksache-data.pdf, abgerufen am 19.04.2021.

Bos, Wilfried/Eickelmann, Birgit/Gerick, Julia/Goldhammer, Frank/Schaumburg, Heike/Schwippert, Knut/Senkbeil, Martin/Schulz-Zander, Renate/Wendt, Heike (2014): ICILS 2013. Computer- und informationsbezogene Kompetenzen von Schülerinnen und Schülern in der 8. Jahrgangsstufe im internationalen Vergleich, Münster: Waxmann.

boyd, danah/Hargittai, Eszter (2013): »Connected and concerned: Variation in parents' online safety concerns«, in: Policy & Internet 5, S. 245–269.

Bräunlich, Katharina/Dienlin, Tobias/Eichenhofer, Johannes/Helm, Paula/Trepte, Sabine/Grimm, Rüdiger/Seubert, Sandra/Gusy, Christoph (2020):

»Linking loose ends: An interdisciplinary privacy and communication model«, in: New Media & Society, o.S.

Bronfenbrenner,Urie (1981): Die Ökologie der menschlichen Entwicklung. Natürliche und geplante Experimente, Stuttgart: Klett-Cotta.

Brüggen, Niels (2015): »Gedanken zur Neuausrichtung der Medienkompetenzförderung angesichts Big Data«, in: Harald Gapski (Hg.), Big Data und Medienbildung. Zwischen Kontrollverlust, Selbstverteidigung und Souveränität in der digitalen Welt (= Schriftenreihe zur digitalen Gesellschaft NRW, Band 3), Düsseldorf/München: kopaed, S. 51–62.

Brüggen, Niels/Dreyer, Stephan/Gebel, Christa/Lauber, Achim/Müller, Raphaela/Stecher, Sina (2019): Gefährdungsatlas. Digitales Aufwachsen. Vom Kind aus denken. Zukunftssicher handeln. Online unter: https://www.bzkj.de/resource/blob/176416/2c81e8af0ea7cff94d1b688f360ba1d2/gefaehrdungsatlas-data.pdf, abgerufen am 05.08.2020.

Bulger, Monica/Burton, Patrick/O'Neill, Brian/Staksrud, Elisabeth (2017): »Where policy and practice collide: Comparing United States, South African and European Union approaches to protecting children online«, in: New Media & Society 19, S. 750–764.

Cap, Clemens H. (2017): »Verpflichtung der Hersteller zur Mitwirkung bei informationeller Selbstbestimmung«, in: Michael Friedewald/Jörn Lamla/Alexander Roßnagel (Hg.), Informationelle Selbstbestimmung im digitalen Wandel, Wiesbaden: Springer Vieweg, S. 249–264.

Christmann-Budian, Stephanie/Geffers, Johannes (2017): »Wie Zuhause so im Cyberspace? Internationale Perspektiven auf digitale Souveränität«, in: Volker Wittpahl (Hg.), Digitale Souveränität. Bürger, Unternehmen, Staat (= iit-Themenband), Berlin/Heidelberg: Springer Vieweg, S. 117–150.

Couldry, Nick/Hepp, Andreas (2013): »Conceptualizing Mediatization: Contexts, Traditions, Arguments«, in: Communication Theory 23, S. 191–202.

Creswick, Helen/Dowthwaite, Liz/Koene, Ansgar/Perez Vallejos, Elvira/Portillo, Virginia/Cano, Monica/Woodard, Christopher (2019): »›… They don't really listen to people‹«, in: Journal of Information, Communication and Ethics in Society 17, S. 167–182.

Dander, Valentin (2014): »Von der ›Macht der Daten‹ zur ›Gemachtheit von Daten‹. Praktische Datenkritik als Gegenstand der Medienpädagogik«, in: Mediale Kontrolle unter Beobachtung, Datenkritik 3 (1), S. 1–21, https://doi.org/10.25969/mediarep/13783.

Dander, Valentin/Aßmann, Sandra (2015): »Medienpädagogik und (Big) Data: Konsequenzen für die erziehungswissenschaftliche Medienforschung

und -praxis«, in: Harald Gapski (Hg.), Big Data und Medienbildung. Zwischen Kontrollverlust, Selbstverteidigung und Souveränität in der digitalen Welt (= Schriftenreihe zur digitalen Gesellschaft NRW, Band 3), Düsseldorf/München: kopaed, S. 33–50.

De Mooy, Michelle (2017): Rethinking Privacy Self-Management and Data Sovereignty in the Age of Big Data. Considerations for Future Policy Regimes in the United States and the European Union. Online unter: https://www.bertelsmann-stiftung.de/de/publikationen/publikation/did/rethinking-privacy-self-management-and-data-sovereignty-in-the-age-of-big-data, abgerufen am 01.08.2020.

Drotner, Kirsten (1999): »Dangerous media? Panic discourses and dilemmas of modernity«, in: Paedagogica historica 35, S. 593–619.

Duncker, Ludwig (2007): Die Grundschule. Schultheoretische Zugänge und didaktische Horizonte (= Grundlagentexte Pädagogik), Weinheim/München: Juventa.

Eickelmann, Birgit/Aufenanger, Stefan/Herzig, Bardo (2014): Medienbildung entlang der Bildungskette. Ein Rahmungskonzept für eine subjektorientierte Förderung von Medienkompetenz im Bildungsverlauf von Kindern und Jugendlichen, Bonn. Herausgegeben von der Deutschen Telekom Stiftung. Online unter: https://www.telekom-stiftung.de/sites/default/files/files/media/publications/buch_medienbildung.bildungskette_end.pdf abgerufen am 19.04.2021.

Eickelmann, Birgit/Bos, Wilfried/Gerick, Julia/Goldhammer, Frank/Schaumburg, Heike/Schwippert, Knut/Senkbeil, Martin/Vahrenhold, Jan (Hg.) (2019): ICILS 2018 #Deutschland – Computer- und informationsbezogene Kompetenzen von Schülerinnen und Schülern im zweiten internationalen Vergleich und Kompetenzen im Bereich Computational Thinking, Münster: Waxmann.

Elias, Norbert (1971): Was ist Soziologie? (= Grundfragen der Soziologie, Band 1), München: Juventa.

Gapski, Harald (2001): Medienkompetenz. Eine Bestandsaufnahme und Vorüberlegungen zu einem systemtheoretischen Rahmenkonzept, Wiesbaden: VS Verlag für Sozialwissenschaften.

Gapski, Harald (Hg.) (2015): Big Data und Medienbildung. Zwischen Kontrollverlust, Selbstverteidigung und Souveränität in der digitalen Welt (= Schriftenreihe zur digitalen Gesellschaft NRW, Band 3), Düsseldorf/München: kopaed.

Gebel, Christa/Wütscher, Swenja (2015): Social Media und die Förderung von Werte- und Medienkompetenz Jugendlicher. Expertise zu den Potenzialen der Medienarbeit mit Social Media. JFF – Institut für Medienpädagogik in Forschung und Praxis, München. Online unter: https://www.ich-wir-ihr.de/wp-content/uploads/2015/08/Expertise_Jugend-Werte-Medien_Gebel_Wuetscher.pdf, abgerufen am 01.08.2020.

Goldacker, Gabriele (2017): Digitale Souveränität. Online unter: https://www.oeffentliche-it.de/documents/10181/14412/Digitale+Souver%C3%A4nit%C3%A4t, abgerufen am 01.08.2020.

Gräf, Eike/Lahmann, Henning/Otto, Philipp (2018): Die Stärkung der digitalen Souveränität. Wege der Annäherung an ein Ideal im Wandel. Diskussionspapier von iRights.Lab. Online unter: https://www.divsi.de/wp-content/uploads/2018/05/DIVSI-Themenpapier-Digitale-Souveraenitaet.pdf, abgerufen am 12.01.2020.

Grimm, Petra/Keber, Tobias O./Zöllner, Oliver (Hg.) (2015): Anonymität und Transparenz in der digitalen Gesellschaft (= Medienethik, Band 15), Stuttgart: Franz Steiner Verlag.

Groebel, Jo (2016): »Zur Psychologie der digitalen Souveränität: Bedürfnis, Gewöhnung, Engagement«, in: Mike Friedrichsen/Peter-J. Bisa (Hg.), Digitale Souveränität. Vertrauen in der Netzwerkgesellschaft, Wiesbaden: Springer VS, S. 399–413.

Habermas, Jürgen (1971): »Vorbereitende Bemerkungen zu einer Theorie der kommunikativen Kompetenz«, in: Jürgen Habermas/Niklas Luhmann (Hg.), Theorie der Gesellschaft oder Sozialtechnologie – Was leistet die Systemforschung?, Frankfurt a.M.: Suhrkamp, S. 101–141.

Hansmann, Otto (1988): »Kritik der sogenannten ›theoretischen Äquivalente‹ von ›Bildung‹«, in: Otto Hansmann/Winfried Marotzki (Hg.), Diskurs Bildungstheorie. 1. Systematische Markierungen, Weinheim: Deutscher Studienverlag, S. 21–54.

Hargittai, Eszter (2010): »Digital na(t)ives? Variation in internet skills and uses among members of the ›Net Generation‹«, in: Sociological Inquiry 80, S. 92–113.

Hasebrink, Uwe/Hölig, Sascha (2017): »Deconstructing audiences in converging media environments«, in: Sergio Sparviero/Corinna Peil/Gabriele Balbi (Hg.), Media convergence and deconvergence, Cham: Springer International Publishing, S. 113–133.

Hepp, Andreas (2018): »Von der Mediatisierung zur tiefgreifenden Mediatisierung«, in: Jo Reichertz/Richard Bettmann (Hg.), Kommunikation – Medien – Konstruktion, Wiesbaden: Springer VS, S. 27–45.

Hepp, Andreas/Hasebrink, Uwe (2014): »Kommunikative Figurationen – ein Ansatz zur Analyse der Transformation mediatisierter Gesellschaften und Kulturen«, in: Birgit Stark/Oliver Quiring/Nikolaus Jackob (Hg.), Von der Gutenberg-Galaxis zur Google-Galaxis: Alte und neue Grenzvermessungen nach 50 Jahren DGPuK (= Schriftenreihe der Deutschen Gesellschaft für Publizistik- und Kommunikationswissenschaft, Band 41), Konstanz/München: UVK Verlagsgesellschaft, S. 343–360.

Hofmann, Franz (2019): »Fünfzehn Thesen zur Plattformhaftung nach Art. 17 DSM-RL«, in: GRUR – Gewerblicher Rechtsschutz und Urheberrecht 121 (12), S. 1219–1229.

Honig, Michael-Sebastian (1999): Entwurf einer Theorie der Kindheit, Frankfurt a.M.: Suhrkamp.

Jörissen, Benjamin/Marotzki, Winfried (2009): Medienbildung – eine Einführung. Theorie – Methoden – Analysen (= UTB Erziehungswissenschaft, Medienbildung, Band 3189), Bad Heilbrunn: Klinkhardt.

Kammerl, Rudolf (2019): »Bildung im digitalen Wandel«, in: DDS – Die Deutsche Schule 111, S. 422–434.

Kammerl, Rudolf/Müller, Jane/Lampert, Claudia/Rechlitz, Marcel/Potzel, Katrin (2020): »Kommunikative Figurationen – ein theoretisches Konzept zur Beschreibung von Sozialisationsprozessen und deren Wandel in mediatisierten Gesellschaften?«, in: Isabell van Ackeren/Helmut Bremer/Fabian Kessl/Hans-Christoph Koller/Nicolle Pfaff/Carolin Rotter/Esther Dominique Klein/Ulrich Salaschek (Hg.), Bewegungen. Beiträge zum 26. Kongress der Deutschen Gesellschaft für Erziehungswissenschaft, Opladen: Verlag Barbara Budrich, S. 377–388.

Kim, Su Jung (2016): »A repertoire approach to cross-platform media use behaviour«, in: new media & society 18 (3), S. 353–372.

Klafki, Wolfgang (2007): Neue Studien zur Bildungstheorie und Didaktik. Zeitgemäße Allgemeinbildung und kritisch-konstruktive Didaktik, Weinheim/Basel: Beltz.

KMK – Kultusministerkonferenz (2012): Medienbildung in der Schule. Beschluss der Kultusministerkonferenz vom 8. März 2012. Online unter: https://www.kmk.org/fileadmin/veroeffentlichungen_beschluesse/2012/2012_03_08_Medienbildung.pdf, abgerufen am 01.07.2022.

KMK – Kultusministerkonferenz (2016): Bildung in der digitalen Welt. Strategie der Kultusministerkonferenz. Beschluss der Kultusministerkonferenz vom 08.12.2016. Online unter: https://www.kmk.org/fileadmin/Dateien/pdf/PresseUndAktuelles/2017/Strategie_neu_2017_datum_1.pdf, abgerufen am 12.01.2020.

Knop, Karin/Hefner, Dorothée (2018): »Feind oder Freund in meiner Hosentasche? – Zur Rolle von Individuum, Peergroup und Eltern für die (dys)funktionale Handynutzung«, in: Praxis der Kinderpsychologie und Kinderpsychiatrie 67, S. 204–216.

Krings, Günter (2016): »Digitale Souveränität«, in: Mike Friedrichsen/Peter-J. Bisa (Hg.), Digitale Souveränität. Vertrauen in der Netzwerkgesellschaft, Wiesbaden: Springer VS, S. 351–357.

Krotz, Friedrich (2001): Die Mediatisierung kommunikativen Handelns. Der Wandel von Alltag und sozialen Beziehungen, Kultur und Gesellschaft durch die Medien, Wiesbaden: Westdeutscher Verlag.

Krotz, Friedrich (2007): Mediatisierung. Fallstudien zum Wandel von Kommunikation (= Medien – Kultur – Kommunikation), Wiesbaden: VS Verlag für Sozialwissenschaften.

Kutscher, Nadia (2014): »Soziale Ungleichheit«, in: Angela Tillmann/Sandra Fleischer/Kai-Uwe Hugger (Hg.), Handbuch Kinder und Medien, Wiesbaden: Springer VS, S. 101–112.

Lepping, Joachim/Palzkill, Matthias (2017): »Die Chance der digitalen Souveränität«, in: Volker Wittpahl (Hg.), Digitalisierung. Bildung, Technik, Innovation (= iit-Themenband), Berlin/Heidelberg: Springer Vieweg, S. 17–26.

Livingstone, Sonia (2017): »Children's and young people's lives online«, in: Jon Brown (Hg.), Online risk to children. Impact, protection and prevention, Newark: John Wiley, S. 23–36.

Livingstone, Sonia/Ólafsson, Kjartan/O'Neill, Brian/Donoso, Veronica (2012): Towards a better internet for children: Findings and recommendations from EU Kids Online to inform the CEO coalition. EU Kids Online, London. Online unter: http://eprints.lse.ac.uk/44213/1/Towards%20a%20better%20internet%20for%20children%28LSERO%29.pdf, abgerufen am 05.08.2020.

Luhmann, Niklas (1996): Die Realität der Massenmedien, Wiesbaden: VS Verlag für Sozialwissenschaften.

Marotzki, Winfried (2004): »Von der Medienkompetenz zur Medienbildung«, in: Rainer Brödel (Hg.), Weiterbildung als Netzwerk des Lernens. Differenzierung der Erwachsenenbildung, Bielefeld: Bertelsmann, S. 63–74.

Marwick, Alice E./boyd, danah (2014): »Networked privacy: How teenagers negotiate context in social media«, in: New Media & Society 16, S. 1051–1067.

Mascheroni, Giovanna (2018): »Researching datafied children as data citizens«, in: Journal of Children and Media, S. 1–7.

Matzner, Tobias/Richter, Philipp (2017): »Die Zukunft der informationellen Selbstbestimmung«, in: Michael Friedewald/Jörn Lamla/Alexander Roßnagel (Hg.), Informationelle Selbstbestimmung im digitalen Wandel, Wiesbaden: Springer Vieweg, S. 319–323.

Müller, Lena-Sophie (2016): »Das digitale Bauchgefühl«, in: Mike Friedrichsen/Peter-J. Bisa (Hg.), Digitale Souveränität. Vertrauen in der Netzwerkgesellschaft, Wiesbaden: Springer VS, S. 267–286.

Niesyto, Horst (2021): »›Digitale Bildung‹ wird zu einer Einflugschneise für die IT-Wirtschaft«, in: merz – medien + erziehung 65 (1), S. 23–29.

Pangrazio, Luci/Selwyn, Neil (2018): »›It's not like it's life or death or whatever‹: Young people's understandings of social media data«, in: Social Media + Society 4, https://doi.org/10.1177/2056305118787808.

Paus-Hasebrink, Ingrid/Hasebrink, Uwe (2014): »Kommunikative Praxen im Wandel«, in: MedienJournal 38, S. 4–14.

Rott, Karin J. (2020): Medienkritikfähigkeit messbar machen. Analyse medienbezogener Fähigkeiten bei Eltern von 10- bis 15-Jährigen (= Erwachsenenbildung und lebensbegleitendes Lernen – Forschung & Praxis, Band 36), Bielefeld: Bertelsmann.

Rückert, Christian/Safferling, Christoph/Hofmann, Franz (2022): »Souveränität, Integrität und Selbstbestimmung – Herausforderungen von Rechtskonzepten in der digitalen Transformation«, in: Georg Glasze/Eva Odzuck/Ronald Staples (Hg), Was heißt digitale Souveränität? Diskurse, Praktiken und Voraussetzungen »individueller« und »staatlicher Souveränität« im digitalen Zeitalter, Bielefeld: transcript, S. 159–199.

Schäwel, Johanna (2018): How to raise users' awareness of online privacy. An empirical and theoretical approach for examining the impact of persuasive privacy support measures on users' self-disclosure on online social networking sites. Dissertation, Universität Duisburg-Essen, https://doi.org/10.17185/DUEPUBLICO/70691.

Schorb, Bernd (2009): »Gebildet und kompetent«, in: merz – medien + erziehung 53 (5), S. 50–56.

Schorb, Bernd/Wagner, Ulrike (2013): »Medienkompetenz – Befähigung zur souveränen Lebensführung in einer mediatisierten Gesellschaft«, in: Bun-

desministerium für Familie, Senioren, Frauen und Jugend (Hg.), Medienkompetenzförderung für Kinder und Jugendliche. Eine Bestandsaufnahme, Berlin, S. 18–23.

Shin, Wonsun/Kang, Hyunjin (2016): »Adolescents' privacy concerns and information disclosure online: The role of parents and the internet«, in: Computers in Human Behavior 54, S. 114–123.

Sowka, Alexandra/Klimmt, Christoph/Hefner, Dorothée/Mergel, Fenja/Possler, Daniel (2015): »Die Messung von Medienkompetenz. Ein Testverfahren für die Dimension ›Medienkritikfähigkeit‹ und die Zielgruppe ›Jugendliche‹«, in: Medien & Kommunikationswissenschaft 63, S. 62–82.

Spanhel, Dieter (2010a): »Bildung in der Mediengesellschaft«, in: Ben Bachmair (Hg.), Medienbildung in neuen Kulturräumen, Wiesbaden: VS Verlag für Sozialwissenschaften, S. 45–58, https://doi.org/10.1007/978-3-531-92133-4_3.

Spanhel, Dieter (2010b): »Medienbildung statt Medienkompetenz?«, in: merz – medien + erziehung 54 (1), S. 49–54.

Staksrud, Elisabeth (2013): »Online grooming legislation: Knee-jerk regulation?«, in: European Journal of Communication 28, S. 152–167.

Stoilova, Mariya/Nandagiri, Rishita/Livingstone, Sonia (2021): »Children's understanding of personal data and privacy online – a systematic evidence mapping«, in: Information, Communication & Society 24, S. 557–575.

Stubbe, Julian (2017): »Von digitaler zu soziodigitaler Souveränität«, in: Volker Wittpahl (Hg.), Digitale Souveränität. Bürger, Unternehmen, Staat (= iit-Themenband), Berlin/Heidelberg: Springer Vieweg, S. 43–59.

SVRV – Sachverständigenrat für Verbraucherfragen beim Bundesministerium der Justiz und für Verbraucherschutz (2017): Digitale Souveränität. Gutachten des Sachverständigenrats für Verbraucherfragen, Berlin. Online unter: www.svr-verbraucherfragen.de/wp-content/uploads/Gutachten_Digitale_Souveränität_.pdf, abgerufen am 01.08.2020.

Tulodziecki, Gerhard (2011): »Zur Entstehung und Entwicklung zentraler Begriffe bei der pädagogischen Auseinandersetzung mit Medien«, in: Heinz Moser/Petra Grell/Horst Niesyto (Hg.), Medienbildung und Medienkompetenz. Beiträge zu Schlüsselbegriffen der Medienpädagogik, München: kopaed, S. 11–40.

Tulodziecki, Gerhard/Grafe, Silke/Herzig, Bardo (2019): Medienbildung in Schule und Unterricht. Grundlagen und Beispiele, Stuttgart: UTB.

UN – United Nations (Hg.) (2021): General comment No. 25 on children's rights in relation to the digital environment. Online unter: https://children

s-rights.digital/hintergrund/index.cfm/topic.280/key.1661, abgerufen am 31.07.2022.

Vorderer, Peter (2015): »Der mediatisierte Lebenswandel«, in: Publizistik 60, S. 259–276.

Wagner, Ulrike/Brüggen, Niels/Gerlicher, Peter/Schemmerling, Mareike/Gebel, Christa (2013): Identitätsarbeit und sozialraumbezogenes Medienhandeln in Sozialen Netzwerkdiensten. Vierte Teilstudie der 5. Konvergenzstudie »Das Internet als Rezeptions- und Präsentationsplattform Jugendlicher«. Zusammenfassung der Teilstudie, München. Online unter: https://www.jff.de/fileadmin/user_upload/jff/projekte/konvergenzstudien/JFF_Kurzfassung_Teilstudie_Identitaetsarbeit.pdf, abgerufen am 05.08.2020.

Wagner, Ulrike/Gebel, Christa/Lampert, Claudia (Hg.) (2013): Zwischen Anspruch und Alltagsbewältigung. Medienerziehung in der Familie (= Schriftenreihe Medienforschung der Landesanstalt für Medien Nordrhein-Westfalen, Band 72), Berlin: Vistas-Verlag.

Ytre-Arne, Brita (2019): »Media use in changing everyday life: How biographical disruption could destabilize media repertoires and public connection«, in: European Journal of Communication 34, S. 488–502.

Zilka, Gila C. (2019): »The digital divide: implications for the eSafety of children and adolescents«, in: International Journal of Technology Enhanced Learning 11, S. 20.

Konturenbildung im Gestaltungsraum der digitalen Transformation

Eine Reflexion der Debatte über »digitale Souveränität« aus betriebswirtschaftlicher Sicht

Albrecht Fritzsche

Abstract *Die digitale Transformation der Gesellschaft schafft eine Vielfalt neuer Gestaltungsoptionen für Wertschöpfungsprozesse. Im Diskurs über »digitale Souveränität« entstehen durch Vorstellungen territorialer Abgrenzung und Inanspruchnahme von Kontrolle hilfreiche Orientierungspunkte zur Beherrschung dieser Gestaltungsoptionen. Sie erlauben die Bildung von Konturen im Gestaltungsraum der digitalen Transformation, an denen verschiedenste Argumente ansetzen können. Die Aufmerksamkeit des vorliegenden Beitrags gilt diesem Prozess der Konturenbildung. Der Beitrag zeigt auf, dass Konturenbildung in einem Gestaltungsraum, dessen Inhalt aufgrund seiner Mächtigkeit und Komplexität nicht transparent ist, noch auf andere Weise hinterfragt werden kann, als dies heute zumeist der Fall ist. Insbesondere beim Umgang mit dem Ressourcenbegriff wäre eine tiefergehende Reflexion nötig, um verkürzte Schlussfolgerungen zu vermeiden. Am Beispiel aktueller Entwicklungen in der Wirtschaft wird aufgezeigt, dass Strukturbildung vielerorts in Richtungen vorangetrieben wird, die über territoriale Zuordnungen von Autorität und Entscheidungsgewalt an einzelne Personen oder Institutionen kaum erfassbar scheint. Im weiteren Verlauf des Diskurses über »digitale Souveränität« wäre demnach die Frage zu stellen, ob und wie diese Szenarien thematisiert werden können.*

1. Die Orientierungsleistung des Konzepts der Souveränität

Smartphones und andere Geräte, die unentwegt Daten sammeln, verarbeiten und über weltweite Netzwerke miteinander austauschen, sind während der

vergangenen Jahre in alle Bereiche des menschlichen Lebensalltags vorgedrungen. Mit dieser digitalen Transformation der Gesellschaft gehen radikale Strukturveränderungen einher, die in der jüngeren Literatur auf vielfältige Arten und Weisen angesprochen werden. Wenn dabei von Souveränität die Rede ist, dann geht es keineswegs immer nur um politische Autorität oder Entscheidungsgewalt in einem physisch greifbaren Territorium, wie es »akademische« Definitionen von Souveränität nahelegen (z.B. Philpott 1995; Humphrey 2004). Vielmehr diskutieren die entsprechenden Texte Probleme, die Raum und Autorität auch anderweitig interpretieren (Couture/Toupin 2019), nämlich im Hinblick auf die Reichweite, Verantwortung und Kontrolle des eigenen Handelns, bezogen auf Staaten genauso wie auf spezielle gesellschaftliche Institutionen, ethnische Gruppen oder einzelne Personen in privaten oder beruflichen Kontexten (s. die Einleitung von Glasze/Odzuck/Staples 2022 in diesem Band sowie die Kapitel von Dammann/Glasze 2022 und Tretter 2022). Neben »digitaler Souveränität« wird dabei auch von technischer Souveränität, Datensouveränität, Cybersouveränität oder Internetsouveränität und anderem gesprochen, um besondere Herausforderungen im Umgang mit moderner Informationstechnologie zu kennzeichnen (vgl. Hummel et al. 2021).

Angesichts dieser Vielfalt von Bezugnahmen auf Souveränität muss man wohl davon ausgehen, dass dieser Begriff eine Orientierungsleistung erbringt, die im gegenwärtigen Diskurs besonders nachgefragt wird. Dies ist aber keineswegs selbstverständlich, denn die oben genannte »akademische« Definition von Souveränität hat mit Technologie und binären Daten ja zunächst einmal gar nichts zu tun. Im Gegensatz zum deutschen Sprachraum existiert anderswo auch kaum ein umgangssprachlicher Begriff von Souveränität, wie man ihn hierzulande kennt. Im Deutschen lassen sich alle Menschen als »souverän« bezeichnen, die eine Situation meistern können, die in der Lage sind, »die Bälle in der Luft zu behalten« und sich nicht von den über sie hereinbrechenden Anforderungen aus der Ruhe bringen lassen. In anderen Sprachen ist das nicht der Fall, und der laufende internationale Diskurs erreicht auch keineswegs die Bandbreite, die eine deutsche Begriffsbestimmung von Souveränität zulassen würde (s. dazu auch den Beitrag von Glasze/Odzuck/Staples 2022 in diesem Band sowie von Dammann/Glasze 2022 und Tretter 2022). Glaubt man etwa Floridi (2020), so geht es bei »digitaler Souveränität« um Kontrolle. Kontrolle ist aber nicht einfach so gleichzusetzen mit der Fähigkeit, eine Situation zu meistern. Sie setzt einen Bezugspunkt voraus, etwas, über das man Kontrolle hat und das diesbezüglich unterscheidbar ist von etwas anderem. So lässt sich

dann auch zuordnen, wer über was »das Sagen« hat. Ohne ein zumindest intuitives Verständnis von Autorität und territorialer Eingrenzung kommt man dabei nicht aus. Der Begriff der Souveränität scheint nun genau das im gegenwärtigen Diskurs zu liefern.

Allzu leicht wird dabei aber vergessen, dass Kontrolle keineswegs überall herstellbar ist und dass nicht einmal die Bezugsobjekte, die zu kontrollieren wären, klar erfassbar sein müssen. Beispiele dafür lassen sich vermutlich vielerorts finden, insbesondere aber auch in der modernen Betriebswirtschaft. Aus diesem Grund setzt sich das vorliegende Kapitel mit der Orientierungsleistung des Begriffs der Souveränität aus Sicht der Betriebswirtschaftslehre auseinander. Es untersucht, welche Möglichkeiten ein Diskurs über Souveränität im Kontext der digitalen Transformation bietet und an welchen Stellen der Diskurs an seine Grenzen stößt.

Die Betriebswirtschaftslehre und ihre Teildisziplinen haben sich bisher kaum mit »digitaler Souveränität« auseinandergesetzt. Umso mehr befassen sie sich aber mit Fragen der Erschließung und Verwertung von Daten im Kontext der digitalen Transformation der Gesellschaft, auf die im Diskurs über »digitale Souveränität« immer wieder verwiesen wird. Die folgenden Ausführungen sollen dazu beitragen, solche Verweise besser zu verstehen und von der Formulierung konkreter Argumente hinsichtlich der Territorialisierung von Autorität und Entscheidungsgewalt abzugrenzen. Es geht also weniger darum, einen bestimmten Standpunkt im Diskurs zu beziehen, als vielmehr um die Klärung der Bedingungen, unter denen der Diskurs stattfindet, um den Gefahren verkürzter Darstellungen entgegenzuwirken.

Als theoretische Grundlage der Untersuchung werden verschiedene Überlegungen aus den Wirtschaftswissenschaften herangezogen, die nur noch zum Teil mit räumlichen Intuitionen vereinbart werden können. Im Rahmen eines Buchkapitels, das sich an ein breites Publikum richtet, lassen sich dabei natürlich nicht alle Gedankengänge bis ins Detail ausbreiten. Deshalb werden nur einige Stichpunkte aus der Forschung herausgegriffen, die von besonderer Bedeutung für die Untersuchung der Orientierungsleistung des Souveränitätsbegriffs im vorliegenden Kontext sind. Dies betrifft insbesondere die Differenzierung zwischen der Wahrnehmung von Ressourcen, Besitzansprüchen, territorialen Regelungen und möglichen Alternativen im Umgang mit Ressourcen, die anknüpfungsfähig an Überlegungen in anderen Disziplinen sind.

2. Explodierende Gestaltungsoptionen und die Orientierung im Unbestimmten

Die Betriebswirtschaftslehre hat sehr früh begonnen, sich mit der digitalen Transformation der Gesellschaft und ihren Folgen für die Bestimmung und Abgrenzung einzelner Handlungsbereiche auseinanderzusetzen. Dies erklärt sich dadurch, dass viele Phänomene, die gegenwärtig in der Gesellschaft allgemein zu beobachten sind, bereits vor längerer Zeit im engen Kontext der verarbeitenden Industrie vorweggenommen wurden (s. dazu auch Gölzer/Fritzsche 2017). Noch vor der Erfindung des Smartphones ermöglichte der Ausbau leistungsfähiger Kommunikationssysteme die Aufteilung und Verlagerung von Fertigungsprozessen über geographische und organisationale Grenzen hinweg, ohne merkliche Verluste an Effizienz oder Effektivität hinnehmen zu müssen. Dementsprechend wandte sich die Aufmerksamkeit der Forschung recht bald dem Management weltweiter Lieferketten und ähnlichen Aktivitäten zu, in denen verschiedene Unternehmen eng abgestimmt miteinander zusammenarbeiten (vgl. z.B. Stadtler/Kilger/Meyr 2015).

Mithilfe moderner Informationstechnologie wurde die Integration der Unternehmensaktivitäten weiter vorangetrieben und die Fähigkeit zur Adaption an veränderliche Marktbedingungen erhöht. Angesichts dieser Entwicklungen sprachen einzelne Quellen schon im späten 20. Jahrhundert von der Zersetzung territorialer Autorität bis hin zur Auflösung der Unternehmung selbst (vgl. Picot/Reichwald 1994). Das Schema, nach dem sich die digitale Transformation gegenwärtig vollzieht, ist also im Grunde genommen gar nicht so neu. Was sich in den letzten Jahren verändert hat, sind die Flexibilität der technischen Systemlandschaft und ihr Anwendungsbereich, der heute weit über die Grenzen der verarbeitenden Industrie hinausragt und Ansprüche auf eine umfassende Erschließung des menschlichen Lebensalltags laut werden lässt.

In der betriebswirtschaftlichen Fachliteratur hat sich diese Entwicklung dergestalt niedergeschlagen, dass neben einzelnen Unternehmen und ihren Liefernetzwerken auch noch weitergehende Strukturen thematisiert werden. So befasst sich die Forschung derzeit intensiv mit ökonomischen Ökosystemen, die alle Institutionen einschließen, die zur erfolgreichen Abwicklung von Wertschöpfungsprozessen nötig sind (vgl. Jacobides/Cennamo/Gawer 2018). Außerdem wird diskutiert, wie das Leistungsspektrum der Industrie weiter ausgedehnt werden kann, um individuelle Bedürfnisse im Lebensalltag einzelner Menschen anzusprechen (vgl. Vargo/Maglio/Akaka 2008). Punk-

tuelle Transaktionen beim einmaligen Kauf eines Produkts gelten dabei nur noch als momentane Ausprägungen einer längerfristigen Geschäftsbeziehung zwischen den jeweils Beteiligten, deren Rentabilität von ihrer Dauer und Ausdifferenzierung im Lauf der Zeit abhängt.

Wie im Falle des Managements von Lieferketten wird dies alles heute deshalb interessant, weil digitale Technologien es erlauben, strukturbildende Prozesse absichtsvoll in verschiedene Richtungen voranzutreiben. Mit anderen Worten: Die entsprechenden Strukturen entwickeln sich nicht einfach so von selbst, ohne dass es den Beteiligten möglich wäre, darauf Einfluss zu nehmen. Digitale Technologien erlauben es vielmehr, auf verschiedenste Weise zielgerichtet in diese Entwicklung einzugreifen. Diese Gestaltungsoptionen können nicht ignoriert werden. Die Beteiligten müssen sich überlegen, wie sie damit umgehen wollen. Das Problem besteht nun darin, dass die Möglichkeiten zur weiteren Entwicklung, die von diesen Gestaltungsoptionen aufgeworfen werden, derart vielfältig sind, dass das daraus resultierende Potenzial für die Weiterentwicklung des Wirtschaftsbetriebs selbst kaum vorherzusagen ist. Entscheidungen über den Einsatz digitaler Technologien führen nicht nur dazu, dass sich neue Märkte entwickeln oder dass bestimmte Prozesse effizienter umzusetzen sind und damit die Wettbewerbsfähigkeit des Wirtschaftsbetriebs erhöhen. Sie führen auch dazu, dass sich die Beteiligten anders als Handelnde konstituieren. So kann es eben sein, dass unternehmerische Entscheidungen durch die Auflösung institutioneller Grenzen nur noch gemeinsam getroffen werden können, dass die Risiken bei der Entwicklung neuer Geschäftsmodelle nicht mehr einzelnen ökonomisch Handelnden zugeordnet werden können, sondern stets auf mehrere Häupter verteilt werden, und so weiter.

Aus Sicht der Betriebswirtschaftslehre, so wäre daraus abzuleiten, hat der Gestaltungsraum der digitalen Transformation für sich allein betrachtet überhaupt noch keine greifbare Kontur. Gestaltungsoptionen sind als solche nur in Teilen erkennbar und ihre tatsächlichen Folgen nicht abzusehen. Es besteht also durchaus Bedarf an einer Orientierungshilfe, die zuallererst aber nicht den Zweck hätte, Gestaltungsoptionen bewertbar zu machen, sondern sie überhaupt formulieren zu können. Sie wäre vergleichbar mit einer Kontrastfolie, die über dem Gestaltungsraum der digitalen Transformation ausgebreitet wird, um dessen Inhalte erfassbar zu machen.

Ein bewährtes Konzept wie Souveränität kann diesem Zweck dienen. Der laufende Diskurs über »digitale Souveränität« gibt einen Eindruck davon, welche Konturen im Gestaltungsraum der digitalen Transformation durch die da-

mit entstehende Kontrastfolie zu sehen sind. Aber er gibt kaum Aufschluss über das, was dabei ausgeblendet wird. Es bleibt unklar, welche weiteren Gestaltungsoptionen bestehen könnten, wenn eine andere Kontrastfolie gewählt würde, und nach welchen Kriterien Vergleiche zwischen solchen verschiedenen Kontrastfolien angestellt werden müssten. Dies soll im Folgenden weiter beleuchtet werden.

3. Konturenbildung im Gestaltungsraum als vorgelagerter Prozess

Datensouveränität, technische Souveränität, Cybersouveränität, Internetsouveränität und so weiter betreffen sehr unterschiedliche Gestaltungsobjekte. Die Inanspruchnahme territorialer Autorität als Schema, das es möglich macht, Probleme zu formulieren und davon ausgehend über Lösungen nachzudenken, ist also vielfältig einsetzbar. Fraglich ist allerdings, unter welchen Bedingungen man sich auf die Verwendung dieses Schemas einlassen sollte. Dies mag auf den ersten Blick nun so klingen, als ginge es um die Nützlichkeit des Schemas als Werkzeug zur Bearbeitung eines Problems. Genau das ist aber nicht der Fall. Nützlichkeit hat ja nur etwas damit zu tun, welche Vor- und Nachteile die Anwendung eines Werkzeugs hat. Wenn der Gestaltungsraum der digitalen Transformation tatsächlich so intransparent ist, wie oben beschrieben, und wenn die zu treffenden Entscheidungen dazu führen, dass sich die Beteiligten in ihren Rollen immer wieder neu konstituieren, dann muss die Aufmerksamkeit nicht dem Einsatz des Werkzeugs, sondern der Angemessenheit der Konturenbildung im Gestaltungsraum durch die Bezugnahme auf Souveränität gelten. Egal welche Positionen im Diskurs über »digitale Souveränität« eingenommen werden, wäre also zu fragen, wie die Argumente, die uns dieser Diskurs zu formulieren erlaubt, die digitale Transformation vor unseren Augen erscheinen lassen und welche Einsichten dadurch ermöglicht oder verunmöglicht werden.

Ganz neu ist das alles nicht. Es gab schon immer Krisensituationen, die derartig verworren und vertrackt waren, dass Handlungsoptionen nicht klar erkennbar und in ihren Folgen für alle Beteiligten nicht abschätzbar waren. Mitteleuropa befand sich im 16. und 17. Jahrhundert zweifellos in einer solchen Krise. Gerade zu dieser Zeit wurde das Konzept der Souveränität nun maßgeblich geprägt (s. dazu knapp die Einleitung von Glasze/Odzuck/Staples 2022 sowie vgl. z.B. Philpott 1995). Ein frühes Beispiel für die Bezugnahme auf territoriale Autorität, dessen Angemessenheit aus heutiger Sicht fragwür-

dig erscheint, sind wohl die Regelungen aus dem *Augsburger Religionsfrieden*, die mit dem Leitsatz »*cuius regio, eius religio*« assoziiert werden. Dass Konflikte zwischen Menschen, die verschiedenen religiösen Bekenntnissen anhängen, überhaupt etwas mit geographischen Grenzen zu tun haben müssen, ist ja keineswegs selbstverständlich. Mag die getroffene Regelung auch durchaus einen gewissen Nutzen gehabt haben, mutet die zugrunde liegende Idee, so über die gegebene Krisensituation nachzudenken, seltsam an, wenn sie mit genügend historischem Abstand betrachtet wird. Ähnliches könnte in Zukunft auch für unseren heutigen Umgang mit dem Konzept der Souveränität im Kontext digitaler Technologien gelten.

Demzufolge scheint es geboten, sehr genau darauf zu achten, wie und warum Bezüge zwischen digitalen Technologien und territorialer Autorität aufgebaut werden. Es mag oft naheliegen, bestimmte Grenzen zwischen unterschiedlichen Sphären von Kontrolle, Verantwortung und Verfügung zu ziehen, um sich Personen und Institutionen überhaupt erst als Handelnde vorstellen zu können. Die Tatsache, dass diese Vorstellungen eine Argumentationsgrundlage für weitere Entscheidungen und Bewertungen schaffen, bedeutet aber nicht, dass es zu diesem Vorgehen nicht auch Alternativen geben könnte, durch die ein ganz anderes Nachdenken über die digitale Transformation in Gang gesetzt würde.

Ein bekanntes Gestaltungsproblem, an dem dies illustriert werden kann, ist die Regulierung der Weiterverarbeitung von Daten. Viele Lösungsvorschläge für dieses Gestaltungsproblem basieren auf der Vorstellung, dass sich auf Datenquellen territoriale Claims abstecken lassen. Weit verbreitet ist die Metapher von Daten als neuem Öl, die schon kurz nach der Jahrtausendwende erste Verwendung fand (s. Hirsch 2013). Auch anderweitig werden Daten oft mit Bodenschätzen verglichen, die mit neuen Technologien gehoben und verwertet werden könnten (vgl. z.B. Gröhe 2018; Weyers et al. 2018). Solche Vergleiche eröffnen auch Möglichkeiten für eine zielgerichtete Kritik der Sammlung von Daten, basierend auf negativen Erfahrungen mit der Erschließung von Bodenschätzen (vgl. Nolin 2019). Besonders deutlich wird dies dort, wo Datenkolonialismus als unrechtmäßige Besitzergreifung angeprangert wird, mit der einzelne Länder oder Unternehmen ihren Machtbereich ausweiten (vgl. z.B. Dander 2019; Zimmer 2019).

Infolge dieser Konturbildung im Gestaltungsraum der digitalen Transformation können nun ganz unterschiedliche Argumente entwickelt werden. Auf der einen Seite sprechen die Stimmen des Fortschritts mit ihrem Pioniergeist: Land wird erschlossen; wildes Terrain wird urbar gemacht. Mit der Verwer-

tung von Daten gehen Heilsversprechen einher. Informationstechnologie soll dazu beitragen, das Leben besser zu gestalten, Effizienz und Effektivität des eigenen Handelns zu erhöhen und große Menschheitsprojekte wie Gesundheit, Sicherheit, Gerechtigkeit umzusetzen. Auf der anderen Seite sprechen die Betroffenen von den Folgen des Wandels. Sie nutzen Motive, die aus Geschichten vom Untergang alter Gesellschaftsformen bekannt sind, von kultureller Verarmung und Abhängigkeit. Ein freier Zugriff auf Daten zur beliebigen Weiterverarbeitung wird assoziiert mit einem Eindringen fremder Mächte in den eigenen Lebensbereich, wodurch die eigene Identität bedroht wird und Entwicklungsmöglichkeiten verloren gehen.

Man kann dies als territoriale Interpretationen positiver und negativer Freiheitsbegriffe ansehen. Positiv wird die Verwertung von Daten als Ermöglichung selbstbestimmten Handelns interpretiert. Der Mensch verwirklicht ungenutztes Potenzial. Er emanzipiert sich von Beschränkungen, die ihm die Natur auferlegt hat. Negativ wird die Ausbeutung von Daten als Verletzung einer vorhandenen Ordnung gesehen. Die Aufmerksamkeit ist auf Eingriffe in die Verfügungsgewalt des Menschen über die eigenen Daten gerichtet, die nicht notwendigerweise darin zum Tragen kommen, dass die Daten anderweitig verwendet werden, sondern darin, dass sie der Verwertung gänzlich entzogen sind. Aus der Technikphilosophie sind diese Überlegungen bereits lange bekannt (s. Kapp 1978; auch Gehlen 1957). Dabei wurde auch schon darauf verwiesen, dass beide Standpunkte technisch geprägte Überlegungen schon voraussetzen (etwa in Hubig 2015). Es ist ja erst dann möglich, über Verwertung zu sprechen, wenn bereits eine Vorstellung davon vorhanden ist, was eine solche Verwertung bedeutet. Dies aber erfordert einen technischen Blick auf die Sachlage, der wiederum auf bestimmten kulturellen Erfahrungen beruht.

So naheliegend es auch sein mag, den Diskurs in dieser Richtung voranzutreiben, sollte man sich doch im Klaren darüber sein, wie viel dabei schon vorausgesetzt und stillschweigend als gegeben akzeptiert wird. Wenn die Auseinandersetzung nur darum kreist, wer über Datenschätze verfügen kann, dann geraten die technischen und ökonomischen Deutungsprozesse, die einer solchen Art des Nachdenkens über digitale Technologien vorangehen, völlig außer Acht. Für die Betroffenen stellt sich gar nicht mehr die Frage, ob und wie sie etwas als wichtige Ressource auffassen wollen. Es geht nur noch darum, ob sie oder jemand anderes diese Ressource kontrollieren. Man kann dies mit der Situation vergleichen, in der sich die Bevölkerung eines Landes befindet, das durch fremde Mächte kolonisiert wurde. Die Machtverhältnisse im Land

mögen sich zu einem späteren Zeitpunkt durchaus wieder verändern lassen. Für die Einsicht in das Vorhandensein von Bodenschätzen, den Ausbau der Infrastruktur zu ihrer Verwertung und die daraus resultierenden territorialen Interessen gilt dies nicht. Die Deutungsmuster, die sich hier einmal ausgebildet haben, bleiben über viel längere Zeit wirksam. Umso wichtiger erscheint es also, die Bedingungen der Entstehung solcher Deutungsmuster genauer zu untersuchen, um mögliche Alternativen nicht zu übersehen.

4. Veränderliche Ausprägungen wirtschaftlicher Bezugsgrößen

Um dem Prozess der Konturenbildung im Gestaltungsraum der digitalen Transformation auf die Spur zu kommen, sind grundlegende Überlegungen zur Modellierung menschlichen Handelns kaum zu vermeiden. Im hier beschriebenen Fall wird die Spurensuche früher oder später zu dem Begriff der Knappheit führen. Knappheit erklärt, warum es überhaupt zur Erschließung neuer Ressourcen und Erhebung von territorialen Besitzansprüchen kommt. Durch die Erschließung von Ressourcen wird Knappheit reduziert. Besitzansprüche erlauben es, dass Ressourcen als Güter behandelt werden können. Die Privatisierung von Gütern wird meistens dadurch gerechtfertigt, dass sie den effizienten Umgang mit knappen Gütern fördert. Öffentliche Güter oder Allmendegüter sind stets der Gefahr übermäßiger Beanspruchung ausgesetzt. Bei privaten Gütern ist das nicht der Fall. Sie schaffen die Voraussetzung für Gütertausch nach den Gesetzen von Angebot und Nachfrage, die unter geeigneten Bedingungen zu einer gleichmäßigen Befriedigung der Bedürfnisse aller Beteiligten führt.

Narrative von Souveränität weisen vielfältige Bezüge zu Erfahrungen von Knappheit auf, die durch territoriale Zuordnungen entweder gemindert oder verstärkt wurden. Einflussgebiete werden ausgedehnt, um wichtige Ressourcen zu erschließen oder unter eigene Kontrolle zu bringen; umgekehrt werden Grenzen gezogen, um genau dies zu vermeiden, den Zugriff auf die eigenen Ressourcen abzusichern und sie damit auch handelbar zu machen. Dies gilt nicht nur auf nationalstaatlicher Ebene, sondern überall dort, wo in irgendeiner Form Privatheit thematisiert wird – bis hin zur Intimsphäre einzelner Personen, die nicht nur Identität stiftet, sondern auch die Möglichkeit zur Interaktion auf Augenhöhe mit anderen Personen schafft, welche aus wirtschaftlicher Sicht wiederum in den Kontext des Tauschhandels gestellt werden könnte.

Es darf nicht übersehen werden, dass Erfahrungen von Knappheit in ganz unterschiedlicher Hinsicht gestaltenden Interventionen unterworfen sind. Dies beginnt bei der Wahrnehmung von Bedürfnissen als Voraussetzung solcher Erfahrungen. Wenn es jemandem an etwas mangelt, ist es noch lange nicht selbstverständlich, dass dies als Einschränkung wahrgenommen wird. Für eine Person mag es völlig unerheblich sein, ob sie Zugang zu einer Bibliothek belletristischer Bücher hat, für eine andere aber umso wichtiger. Ebenso ist es denkbar, dass die erste Person kein schnelles Internet braucht, während die zweite darauf angewiesen ist. Verantwortlich dafür sind verschiedene Lebensumstände und Prägungen auf bestimmte Werthaltungen.

Umgekehrt lassen sich Problemsituationen oft durch verschiedene Ursachen erklären, die nicht auf den Mangel derselben Ressource zurückzuführen sind. Infolgedessen werden weitere Kriterien hinzugezogen, mit denen die Aufmerksamkeit auf bestimmte Ressourcen gelenkt werden kann. Konventionen hinsichtlich von Kleidung und Schmuck als Zeichen für die Zugehörigkeit zu sozialen Gruppen können dies illustrieren. Selbst in Szenarien, die eher durch Überfluss gekennzeichnet sind als durch Mangel, lässt sich auf diese Weise Knappheit erfahrbar machen. (Besonders interessant sind hierbei auch Böhmes [2016] Überlegungen zum Ästhetischen Kapitalismus.)

In jedem dieser Fälle werden Kausalbeziehungen aufgebaut, mit denen sich das Vorhandensein bestimmter Ressourcen als notwendige Voraussetzung für die Erreichung eines Ziels darstellen lässt. Durch die Formalisierung von Handlungsschemata können Ressourcen dabei auch abstrakt konstruiert werden. Ein historisches Beispiel, mit dem viele Problemstellungen der heutigen Informationsgesellschaft bereits vorweggenommen wurden, ist die Regulierung der Nutzung geistigen Eigentums durch Patente. Hiermit entstand eine künstliche Ressource, die es in dieser Form vorher nicht gegeben hatte und die bereits so gestaltet wurde, dass sie die Einführung neuer Besitzansprüche nahelegte. Das Patentwesen machte Wissen über technische Neuentwicklungen einerseits zu einem knappen Gut, andererseits aber auch zu einem handelbaren Gut, womit die Erschließung neuen Wissens an Attraktivität gewann und Innovation gefördert wurde. Ähnlich verhält es sich mit CO_2-Emissionsrechten, die allerdings weniger zur Erschließung neuer Ressourcenbestände beitragen, sondern eher den Umgang mit vorhandenen Ressourcen durch künstliche Verknappung effizienter machen sollen.

Erfahrungen von Knappheit lassen sich also nicht isoliert betrachten, sondern erfordern ein tieferes Verständnis der Handlungen, deren Erfolg durch die Verfügbarkeit von Ressourcen abgesichert werden soll. Dabei ist zu be-

rücksichtigen, dass diese Lebensvollzüge keineswegs stabil bleiben. Nicht zuletzt durch den technischen Fortschritt sind Bildung, Ernährung, Arbeit, Familien und Freizeitverhalten etc. ja stetigen Veränderungen unterworfen, mit weitreichenden Konsequenzen für die Wahrnehmung von Bedürfnissen, die Erfahrungen von Knappheit zugrunde liegen. Infolgedessen entwickelt sich auch der Blick auf Ressourcen beständig weiter und lenkt die Aufmerksamkeit auf Möglichkeiten und Beschränkungen des Zugriffs, die vor Jahren vielleicht noch gar keine Rolle gespielt haben. Dies führt nun auch dazu, dass unsere Vorstellungen von territorialer Autorität oder Entscheidungsgewalt immer wieder angepasst werden müssen. Vor der Erschließung des Luftraums als Verkehrsweg war es unerheblich, welche territorialen Ansprüche dort erhoben wurden; heute ist dies aus verschiedensten Gründen wichtig. Der Eintrag von Kontaktdaten im Telefonbuch stellte über viele Jahre ebenfalls kaum ein Problem dar, bis diese Daten systematisch erschlossen und kommerziell verwendet wurden, was entsprechende Gegenreaktionen hinsichtlich der Verfügbarkeit der Daten nach sich zog. Umgekehrt wurden Beschränkungen im Personen- und Warenverkehr während der vergangenen Jahre eher abgebaut. Auch die eigene Privatsphäre wird je nach Zeit und kulturellem Hintergrund ganz anders definiert, was sich insbesondere am Umgang mit persönlichen Fotos und Videos zeigt.

Eine Auseinandersetzung mit territorialen Ansprüchen in absoluter Form hat deshalb nur eine sehr begrenzte Reichweite. Um weitergehende Einsichten zu gewinnen, ist es wichtig, sich klarzumachen, auf welche Ressourcen sich solche Ansprüche beziehen und welche Handlungen mit diesen Ressourcen angestrebt werden. Dabei muss man bedenken, dass immer wieder neue Ressourcen als relevant identifiziert werden und neue Verwertungsmuster entstehen, die bisher keine Rolle spielten. Wenn heute ganz pauschal über den beschränkten Zugang zu Daten diskutiert wird, so spricht dies für eine große Unsicherheit im Hinblick auf das Verständnis von Ressourcen und ihre Verwertungsmöglichkeiten. Erst seit wenigen Jahren werden vermehrt Anstrengungen unternommen, um die Nutzung von Daten zu bestimmten Zwecken näher zu spezifizieren. Ein Beispiel dafür sind die Erläuterungen zur Verwendung von Cookies beim Aufruf von Webseiten auf dem Territorium der Europäischen Union. Man kann dies als wichtigen Schritt auf dem Weg zu einer handlungsorientierten Auseinandersetzung mit Ressourcen in der Datenwirtschaft werten. An der Art, wie die Zustimmung zum Setzen von Cookies auf Webseiten eingefordert wird, lässt sich gleichzeitig aber auch erkennen, wie oberflächlich diese Auseinandersetzung derzeit noch erfolgt.

5. Neue Konturen im Gestaltungsraum durch ein weiteres Verständnis von Ressourcen

Anhand der vorangehenden Überlegungen ist es möglich, die Wahrnehmung von Ressourcen, daraus resultierende Besitzansprüche und ihre territoriale Umsetzung nach dem Prinzip der Souveränität voneinander zu unterscheiden. Davon ausgehend wäre nun auch noch die Frage zu erörtern, ob es nicht auch einen anderen Weg des Umgangs mit Ressourcen gibt, der ohne Territorialisierung auskommt. Angesichts der Tatsache, dass die digitale Transformation immanent mit der Verbreitung von Netzwerken einhergeht, in denen verschiedenste Beteiligte integriert sind, könnte ein solcher Weg von besonderem Interesse sein.

Tatsächlich wurden in den Wirtschaftswissenschaften während der vergangenen Jahre umfangreiche Überlegungen zum Thema Ressourcen angestellt, auf die man an dieser Stelle zurückgreifen kann (s. etwa Prahalad/Hamel 1990; Prahalad/Ramaswamy 2000; auch Vargo/Lusch 2004, 2008). Ging es der Forschung im 20. Jahrhundert meist nur um die Frage, wie Ressourcen in der betrieblichen Praxis eingesetzt werden sollten, hat sich der Horizont des Interesses in neuerer Zeit deutlich erweitert. Dies ist vor allem darauf zurückzuführen, dass die Bedeutung materiell nicht greifbarer Größen in diesem Zusammenhang stark zugenommen hat. Zugang zu materiellen Ressourcen ist zwar weiterhin eine notwendige Voraussetzung, um betrieblich tätig werden zu können. Der Unternehmenserfolg hängt aber auch von anderen Faktoren ab, die in konventionellen Auflistungen des Betriebsvermögens kaum darstellbar sind. Zu diesen Faktoren gehören Wissensbestände im Unternehmen, Verfügungsrechte über Erfindungen und Marken, Infrastrukturen an den jeweiligen Standorten und existierende Handelsbeziehungen. Ebenso tragen aber auch Faktoren wie die Motivation der Belegschaft, die Attraktivität einer Marke, der Umgangston im Unternehmen, seine Verankerung in der lokalen Kultur und das Nutzungsverhalten mit Kundinnen und Kunden zum Unternehmenserfolg bei. In einer Bilanz findet dies alles so gut wie keinen Niederschlag. Dennoch wird es bei der Bewertung von Unternehmen an der Börse umfangreich berücksichtigt und trägt wesentlich dazu bei, dass der Marktwert stark vom Buchwert eines Unternehmens abweichen kann. Besonders deutlich wird das heutzutage bei Unternehmen der sogenannten Plattformökonomie, die selbst nur in sehr geringem Ausmaß über klassische Wirtschaftsgüter verfügen, aber eine riesige Zahl von Geschäftstreibenden miteinander vernetzen.

Über den Güterbegriff sind viele solche Ressourcen nicht mehr zu erschließen. So lässt sich die Motivation der Belegschaft eines Unternehmens kaum von dem Unternehmen selbst trennen. Obendrein mag das Unternehmen viel Geld investiert haben, um diese Motivation zu verbessern. Dennoch handelt es sich hier weder um ein privates noch um ein öffentliches Gut. (Blendet man das Unternehmen selbst aus und betrachtet nur individuelle Personen, so könnte vielleicht von einem Klubgut die Rede sein, also einem Gut, für das keine Rivalität herrscht, aber von dem andere ausgeschlossen werden können. Dies hilft bei der Diskussion des Unternehmens als handelnder Institution jedoch auch nicht weiter.) Noch schwieriger ist die Lage, wenn das Verhalten oder die Ansichten potenzieller Kundinnen und Kunden berücksichtigt werden müssen, die gar nicht explizit an das Unternehmen gebunden sind. Bezugspunkt oder Träger der Ressource ist also ein Kollektiv unbestimmter Größe. Spätestens hier scheitert damit auch jeder Versuch einer Territorialisierung. Bestenfalls lässt sich von einem Zentrum und einer unscharfen Peripherie sprechen, wie man sie auch anderenorts bei gemeinschaftlichem Handeln beobachten kann.

Trotz alledem bleibt das Unternehmen eindeutiger Bezugspunkt der Ressourcen. Es hat auch Einfluss auf die Entwicklung der Ressourcen und das damit verbundene Verhalten der beteiligten Personen. Dabei muss es jedoch auf Praktiken zurückgreifen, die ohne deutliche Herrschaftsansprüche auskommen, insbesondere den Aufbau und die Aufrechterhaltung eines Diskurses über unternehmensbezogene Themen, die für die Kollektive interessant sind. Ein Beispiel findet sich im Innovationsmanagement, wo viele Unternehmen begonnen haben, sich laufend mit potenziellen Kundinnen und Kunden über Produktideen auszutauschen, und ihnen die Möglichkeit geben, sich aktiv an einzelnen Schritten der Produktentwicklung zu beteiligen. Dies ist für alle Beteiligten interessant, da Produkte und Bedarfe am Markt besser aufeinander abgestimmt und neue Ideen schneller aufgegriffen werden können. Aufgabe des Unternehmens ist die Anleitung und Moderation des Austauschs und die Umsetzung der jeweiligen Ideen. Durch die Übernahme dieser Aufgabe hat das Unternehmen eine besondere Autorität. Auch wenn klare juristische Regelungen meistens fehlen, scheint es durchaus möglich, dies als eine Form von Souveränität des Handelns anzusehen, die allerdings im Hinblick auf ihren territorialen Bezug ganz anders verstanden werden muss, weil klare Grenzen zwischen Autorität und Entscheidungsgewalt verschiedener Beteiligter nicht mehr zu ziehen sind. Die Polarität zwischen besitzen/handeln und nicht besitzen/nicht handeln wird in eine Art Kontinuum aufgelöst.

6. Wege zu einer breiteren Reflexion über »digitale Souveränität«

Das Konzept der Souveränität spielt ohne Zweifel eine wichtige Rolle als Kontrastfolie im laufenden Diskurs über die digitale Transformation der Gesellschaft. Dies gilt auch und gerade dort, wo es nicht um politische Autorität und Entscheidungsgewalt geht, sondern um Selbstbestimmung und Handlungsfähigkeit von einzelnen Individuen, sozialen Gruppen und Institutionen verschiedenster Art. Souveränität schafft einen Bezugspunkt, um Interaktion und Teilhabe im Angesicht des technischen Wandelns zielführend zu gestalten. Die Ausführungen in diesem Kapitel können diese Orientierungsleistung »digitaler Souveränität« nicht infrage stellen. Sie können aber dazu beitragen, diese Leistung besser zu verstehen und ihre Reichweite einzuschätzen.

Mit dem Begriff der Ressource geht ein Interpretationsvorgang einher, durch den etwas instrumentell erfassbar wird in seiner Funktion bei der Umsetzung bestimmter Handlungen. In den vorangehenden Abschnitten wurde skizziert, wie sich dieser Interpretationsvorgang auf die Formulierung von Besitz- und Verwertungsansprüchen auswirkt, die eben nicht absolut formuliert werden können, sondern nur im Hinblick auf etwas, das getan werden kann. Dies überträgt sich ebenso auf die Einführung territorialer Grenzen, deren Offenheit oder Geschlossenheit auch nur in Bezug auf bestimmte Bewegungs- und Übertragungsvorgänge zu definieren ist und immer wieder an neue Bedürfnisse angepasst werden muss.

Im vorliegenden Kapitel wurden wirtschaftswissenschaftliche Überlegungen genutzt, um solche Zusammenhänge aufzudecken. Auf anderem Wege hätte sich wohl das Gleiche erreichen lassen. Was Wirtschaft in diesem Zusammenhang besonders interessant macht, ist jedoch die Tatsache, dass Organisationsentwicklung, Innovation und vor allem Unternehmertum im Sinne von Schumpeters (1961) kreativer Zerstörung genau darauf ausgerichtet sind, Neuinterpretationen von Ressourcen vorzunehmen und Wertschöpfungsströme weiterzuentwickeln. Nicht zuletzt deshalb haben die Wirtschaftswissenschaften sich in den letzten Jahren auch zunehmend mit Erfolgsfaktoren auseinandergesetzt, die sich Besitzansprüchen entziehen und kaum territorial geregelt werden können. Es besteht Grund zur Annahme, dass in digitalen Netzwerken solche Erfolgsfaktoren zunehmend an Bedeutung gewinnen, da sie weitere Möglichkeiten zum informellen Informationsaustausch fördern.

Hier scheinen die größten Herausforderungen der Konturbildung im Gestaltungsraum der digitalen Transformation zu liegen. Wird eine klar

geregelte Territorialität an zu vielen Stellen erzwungen, so gerät allzu leicht außer Acht, dass es auch Interaktionsformen gibt, die ohne solche Regelungen auskommen. Gerade hier gäbe es jedoch noch eine Menge zu lernen über mögliche Gestaltungsprozesse mithilfe moderner Informationstechnologie, ihre Vor- und Nachteile genauso wie die Gefahren des Missbrauchs von Autorität. Forschungen in diesem Bereich könnten interessante Impulse für die Weiterentwicklung des Konzepts »digitaler Souveränität« geben.

Literaturverzeichnis

Böhme, Gernot (2016): Ästhetischer Kapitalismus, Berlin: Suhrkamp.

Couture, Stephane/Toupin, Sophie (2019): »What does the notion of ›sovereignty‹ mean when referring to the digital?«, in: New Media & Society 21 (10), S. 2305–2322.

Dammann, Finn/Glasze, Georg (2022): »›Wir müssen als Deutsche und Europäer unsere digitale Souveränität zurückgewinnen!‹ Historische Rekonstruktion und internationale Kontextualisierung der Diskurse einer ›digitalen Souveränität‹ in Deutschland«, in: Georg Glasze/Eva Odzuck/Ronald Staples (Hg.), Was heißt digitale Souveränität? Diskurse, Praktiken und Voraussetzungen »individueller« und »staatlicher Souveränität« im digitalen Zeitalter, Bielefeld: transcript, S. 29–60.

Dander, Valentin (2019): »Datenpolitiken ›von unten‹ zwischen Aktivismus und politischer Medienbildung«, in: Martina Bachor/Theo Hug/Günther Pallaver (Hg.), Data Politics: Zum Umgang mit Daten im digitalen Zeitalter, Innsbruck: Innsbruck University Press, S. 93–111.

Floridi, Luciano (2020): »The fight for digital sovereignty: What it is, and why it matters, especially for the EU«, in: Philosophy & Technology 33 (3), S. 369–378.

Gehlen, Arnold (1957): Die Seele im technischen Zeitalter. Sozialpsychologische Probleme in der industriellen Gesellschaft (= Rowohlts deutsche Enzyklopädie), Reinbek: Rowohlt.

Glasze, Georg/Odzuck, Eva/Staples, Ronald (2022): »Einleitung: Digitalisierung als Herausforderung – Souveränität als Antwort? Konzeptionelle Hintergründe der Forderungen nach ›digitaler Souveränität‹«, in: Georg Glasze/Eva Odzuck/Ronald Staples (Hg.), Was heißt digitale Souveränität? Diskurse, Praktiken und Voraussetzungen »individueller« und »staatlicher Souveränität« im digitalen Zeitalter, Bielefeld: transcript, S. 7–28.

Gölzer, Philipp/Fritzsche, Albrecht (2017): »Data-driven operations management: Organisational implications of the digital transformation in industrial practice«, in: Production Planning & Control 28 (16), S. 1332–1343.

Gröhe, Hermann (2018): »Zwischen Datenschutz und Datenschatz – Worauf es bei der Digitalisierung des Gesundheitswesens ankommt«, in: Christian Bär/Thomas Grädler/Robert Mayr (Hg.), Digitalisierung im Spannungsfeld von Politik, Wirtschaft, Wissenschaft und Recht, Berlin/Heidelberg: Springer Gabler, S. 117–125.

Hirsch, Dennis D. (2013): »The glass house effect: Big Data, the new oil, and the power of analogy«, in: Maine Law Review 66, S. 373.

Hubig, Christoph (2015): Die Kunst des Möglichen I. Technikphilosophie als Reflexion der Medialität, Bielefeld: transcript.

Hummel, Patrik/Braun, Matthias/Tretter, Max/Dabrock, Peter (2021): »Data sovereignty: A review«, in: Big Data & Society 8 (1), https://doi.org/10.1177/2053951720982012.

Humphrey, Caroline (2004): »Sovereignty«, in: David Nugent/Joan Vincent (Hg.), A Companion to the anthropology of politics (= Blackwell Companions to Anthropology), Malden/Oxford/Carlton: Blackwell, S. 418–436.

Jacobides, Michael G./Cennamo, Carmelo/Gawer, Annabelle (2018): »Towards a theory of ecosystems«, in: Strategic Management Journal 39 (8), S. 2255–2276.

Kapp, Ernst (1978): Grundlinien einer Philosophie der Technik, Reprint des Originals von 1877, Düsseldorf: Stern.

Nolin, Jan M. (2019): »Data as oil, infrastructure or asset? Three metaphors of data as economic value«, in: Journal of Information, Communication and Ethics in Society 18 (1), S. 28–43.

Philpott, Daniel (1995): »Sovereignty: An introduction and brief history«, in: Journal of International Affairs 48 (2), S. 353–368.

Picot, Arnold/Reichwald, Ralf (1994): »Auflösung der Unternehmung? Vom Einfluß der IuK-Technik auf Organisationsstrukturen und Kooperationsformen«, in: Zeitschrift für Betriebswirtschaft 64 (5), S. 547–570.

Prahalad, Coimbatore K./Hamel, Gary (1990): »The core competence of the corporation«, in: Harvard Business Review 68 (3), S. 79–91.

Prahalad, Coimbatore K./Ramaswamy, Venkatram (2000): »Co-opting customer competence«, in: Harvard Business Review 78 (1), S. 79–90.

Schumpeter, Joseph A. (1961): Konjunkturzyklen. Eine theoretische, historische und statistische Analyse des kapitalistischen Prozesses (= Grundriss der Sozialwissenschaft, Band 1), Göttingen: Vandenhoek & Ruprecht.

Stadtler, Hartmut/Kilger, Christoph/Meyr, Herbert (2015): Supply chain management and advanced planning: Concepts, models, software, and case studies, Berlin/Heidelberg: Springer.

Tretter, Max (2022): »›Digitale Souveränität‹ als Kontrolle. Ihre zentralen Formen und ihr Verhältnis zueinander, in: Georg Glasze/Eva Odzuck/Ronald Staples (Hg.), Was heißt digitale Souveränität? Diskurse, Praktiken und Voraussetzungen »individueller« und »staatlicher Souveränität« im digitalen Zeitalter, Bielefeld: transcript, S. 89–125.

Vargo, Stephen L./Maglio, Paul P./Akaka, Melissa A. (2008): »On value and value co-creation: A service systems and service logic perspective«, in: European Management Journal 26 (3), S. 145–152.

Vargo, Stephen L./Lusch, Robert F. (2004): »Evolving to a new dominant logic for marketing«, in: Journal of Marketing 68, S. 1–17.

Vargo, Stephen L./Lusch, Robert F. (2008): »Service-dominant logic: Continuing the evolution«, in: Journal of the Academy of Marketing Science 36 (1), S. 1–10.

Weyers, Simone/Wahl, Stefanie/Dragano, Nico/Müller-Thur, Kathrin (2018): »Ist der Datenschatz schon gehoben? Eine Übersichtsarbeit zur Nutzung der Schuleingangsuntersuchung für die Gesundheitswissenschaften«, in: Prävention und Gesundheitsförderung 13 (3), S. 261–268.

Zimmer, Wolf (2019): Ansturm der Algorithmen: Die Verwechslung von Urteilskraft mit Berechenbarkeit, Berlin/Heidelberg: Springer Vieweg.

»Digitale Souveränität« in der medienvermittelten öffentlichen Kommunikation

Die Beziehung zwischen Rezipient*in und Gatekeeper

Katharina Leyrer, Svenja Hagenhoff

Abstract *Der Digitalisierung werden im Zusammenhang mit öffentlicher Kommunikation im Diskurs zwei Effekte zugeschrieben: Während einerseits ein Mehr an Selbstbestimmung und Teilhabe vermutet wird, sehen pessimistische Darstellungen und Zuschreibungen zugleich eine Gefahr für die Souveränität der Nutzer*innen und für das zivilisierte gesellschaftliche Miteinander. Problematisch ist, dass dabei unscharf bleibt, was genau die Digitalisierung verändert und auf welchen Zustand und Zeitpunkt referenziert wird. Solange eine systematische Ausarbeitung dieser Veränderungsqualität fehlt, erzeugen die Diskurse um Digitalisierung in der öffentlichen Kommunikation keinen substanziellen erkenntnistheoretischen Mehrwert. Vielmehr bedarf es systematischer Untersuchungen, die kriteriengeleitet zeigen, wie sich die Digitalisierung konkret auf die Souveränitätszustände verschiedener Akteur*innen in der öffentlichen Kommunikation auswirkt. Dieser Beitrag entwickelt daher auf Basis der Network-Gatekeeping-Theorie Kriterien, mit denen beschrieben werden kann, wie sich die Souveränitätszustände von Nutzer*innen in Relation zu Informationsintermediären durch die Digitalisierung verändern. Diese werden beispielhaft auf Bibliotheken und Suchmaschinen angewandt.*

1. Einleitung: Digitalisierung und öffentliche Kommunikation

An der öffentlichen Kommunikation nehmen wir täglich teil, indem wir beispielsweise Radio hören, ein Buch lesen, einen Instagram-Feed durchscrollen, einen Twitter-Post verfassen oder einen Blogartikel schreiben. Auch dieser Beitrag ist Teil der öffentlichen Kommunikation, indem wir als Verfasserinnen Inhalte kommunizieren, die Sie als Leser*in gerade rezipieren.

1.1 Was ist öffentliche Kommunikation?

Öffentliche Kommunikation hat die Aufgabe, die Mitglieder einer modernen Gesellschaft mit Informationen (i.W.S.: Meinung, Inhalt, Daten) zu versorgen, um erwünschte Effekte in Bezug auf politische, kulturelle und ökonomische Beteiligung zu erreichen. Öffentlichkeit ist dabei ein prinzipiell für jeden zugänglicher Kommunikationsraum (vgl. Gerhards/Neidhardt 1990: 16; Jarren 2008: 330), wobei *zugänglich* sich grundsätzlich auf den Akt des Rezipierens (passive Teilhabe) und den des Sprechens (aktive Teilhabe) bezieht (vgl. Hindelang 2019: 10). Moderne öffentliche Kommunikation ist medial vermittelt: Medien als technische Artefakte ermöglichen zeit- und raumüberbrückende Kommunikation, als kulturelle Artefakte erweitern sie die Welt des Individuums erheblich, da sie Vorhandenes (re-)interpretieren, Neues kreieren und als Sinnproduzenten fungieren (vgl. Schmid 2018: 50).

Medial vermittelte öffentliche Kommunikation selbst ist ein komplexes, organisiertes System. Es besteht aus Akteur*innen, die Prozesse und Technologien der Produktion und Distribution von Informationen interessengeleitet gestalten und bereitstellen, und dieses in der Regel in erwerbswirtschaftlicher Form – gemeinwohlorientierte Mediensysteme sind weltweit die Ausnahme – sowie begleitet von unterschiedlich motivierter und divergent ausgeprägter Institutionalisierung (vgl. Hagenhoff 2020: 5ff.). Jarren (2008: 330 u. 332f.) spezifiziert mit Blick auf etablierte Massenmedien, dass diese organisationalen Akteur*innen bekannt sowie gesellschaftlich mitkontrolliert sind; sie arbeiten unter bestimmten sozialen Bedingungen, ihr Tun ist auf Dauer ausgelegt und wird von Träger*innen von Leistungsrollen (vgl. Gerhards/Neidhardt 1990: 24) regelhaft und normengleitet ausgeführt.

1.2 Wie wirkt sich die Digitalisierung auf öffentliche Kommunikation aus?

Der Digitalisierung werden dabei im Zusammenhang mit öffentlicher Kommunikation – gemeint ist dann die Kommunikation mithilfe von Onlinemedien – im Diskurs zwei Effekte zugeschrieben: In sehr optimistischen Darstellungen und Zuschreibungen wird ein Mehr an Selbstbestimmung sowie ein Mehr an Teilhabe und damit eine Stärkung demokratischer Prozesse vermutet (vgl. z.B. Heine 2011; Landeszentrale für politische Bildung BW 2020; Samuelis 2020). Hierzu soll vor allem beitragen, dass die Kommunikation über Onlinemedien zumindest potenziell stärker wechselseitig angelegt

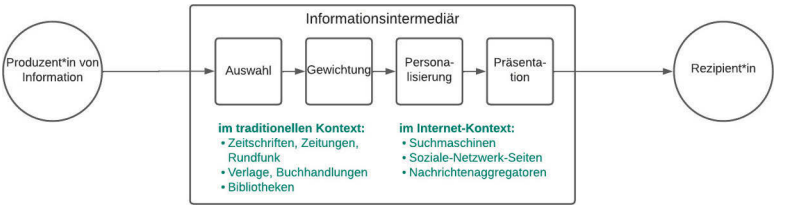
ist, die Hörer*innen- und Sprecher*innen-Rollen gleichverteilt sind und damit der oben erwähnte Zugang zum Kommunikationssystem vollumfänglich realisiert werden kann (vgl. Hindelang 2019: 10f. u. 46). In pessimistischen Darstellungen und Zuschreibungen gelten die mithilfe von Onlinemedien praktizierten Formen von Kommunikation sowie auch das Verhalten der Anbieter[1] relevanter Dienste als gefährlich für das zivilisierte gesellschaftliche Miteinander und für die Demokratie (vgl. z.B. Schweiger 2017; Boehme-Neßler 2019; Bender 2021). Als besonders kritisch wird gesehen, dass Aktivitäten (s. Abb. 1), die bisher durch menschliche Träger*innen von Leistungsrollen (Journalist*in, Bibliothekar*in, Buchhändler*in) vorgenommenen wurden, auf automatisierte, intransparent datenauswertende Routinen verlagert werden.

Die nachstehende Abbildung zeigt eine vereinfachte[2] Prozessierung von Information von den Kommunikator*innen zu den Rezipient*innen. In diesem Prozess des Informationstransports entstehen verschiedene »Points of Control« (Hindelang 2019: 296) in Form von Prozessschritten, Institutionen und technischer Infrastruktur, die eine Teilhabe an der öffentlichen Kommunikation grundsätzlich ermöglichen, unterbinden oder auf diese Teilhabe qualitativ einwirken. Sogenannte »Informationsintermediäre« agieren dabei als Vermittler zwischen Produzierenden und Rezipierenden von Information und nehmen Einfluss auf den Informationsfluss, indem sie Inhalte auswählen, gewichten, personalisieren und präsentieren. Beispiele für Informationsintermediäre sind Zeitschriften, Zeitungen und Rundfunkangebote, aber auch Buchhandlungen und Bibliotheken im traditionellen Kommunikationskontext; im Internetkontext spielen v.a. Suchmaschinen, Soziale-Netzwerk-Seiten und Nachrichtenaggregatoren eine Rolle (vgl. Leyrer 2018).

1 Vor allem die »schrecklichen Fünf« (Manjoo 2016, i.O. »Tech's Frightful 5«): Google, Amazon, Facebook, Apple, Microsoft (GAFAM).

2 Differenzierter bei Bozdag 2013: 214, siehe auch Leyrer 2018.

*Abbildung 1: Informationsprozessierung von den Kommunikator*innen zu den Rezipient*innen.*



Ein zentraler Kritikpunkt an Informationsintermediären besteht darin, dass sie als mächtige Gatekeeper beeinflussen, *welche* Inhalte Nutzer*innen *wie* angezeigt bekommen. Dass sie dabei nicht neutral sein können, formulierte Bagdikian bereits in den 1970er-Jahren:

> »So the gatekeeper, though he seems to perform like one, is not a valueless machine operating in a social vacuum. His decisions, resulting in the printing of most stories seen by the public, reflect his personal as well as his professional values, and all the surrounding pressures that converge on him.« (Ebd. 1971: 106)

Auch wenn sich Bagdikian hier auf traditionelle Gatekeeper bezieht, stehen aktuell vor allem Internet-Informationsintermediäre in der Kritik (vgl. hierzu Leyrer 2018). Mit der Metapher der Filterblase wird der Befürchtung Ausdruck verliehen, dass Nutzer*innen von Suchmaschinen und Soziale-Netzwerk-Seiten nur noch Inhalte angezeigt bekommen, die ihren eigenen Interessen und Meinungen entsprechen, da ein Algorithmus andere Inhalte auf Basis des bisherigen Nutzungsverhaltens und gespeicherter Vorlieben aussortiert. Die als positiv konnotierte Vielfalt an Informationen gelangt somit gar nicht zum*zur Nutzer*in. Als besonders problematisch gilt dabei, dass Nutzer*innen nicht erfahren, welche Inhalte ihnen vorenthalten werden (vgl. Pariser 2011). Alles in allem gilt der*die Nutzer*in der Internet-Intermediäre als passiv ausgeliefert und damit als entmündigt und nicht souverän. Empirisch lassen sich solche Filterblasen jedoch nicht eindeutig nachweisen (eine Übersicht bei Leyrer 2018; Stark/Magin/Jürgens 2021). Darüber hinaus fehlen empirische Analysen, die die Rezipient*innen-Souveränität im Internetkontext über Filterblasen-Effekte hinaus untersuchen.

2. Was ist »digitale Souveränität« in der öffentlichen Kommunikation?

Der Souveränitätsbegriff wird im Forschungsfeld der öffentlichen Kommunikation bisher selten verwendet. Auch fehlt es an Arbeiten, die einen theoretisch fundierten Überblick geben, wie sich Selbstbestimmung oder Souveränität in der medial vermittelten öffentlichen Kommunikation fassen lässt. Es muss also zunächst geschärft werden, was unter Souveränität als spezifischem Untersuchungsgegenstand in der öffentlichen Kommunikation verstanden wird (vgl. Hagenhoff 2020; zu Geschichte und Konzept des Souveränitätsbegriffs allgemein s. die Einleitung in diesem Band von Glasze/Odzuck/Staples 2022).

2.1 Zum Begriff

Wenn auch nicht mit dem Begriff der »digitalen Souveränität«, so gibt es dennoch verschiedene konzeptionelle Annäherungen an die Selbstbestimmung und Autonomie von Rezipient*innen im Internetkontext (zum Diskurs zu »digitaler Souveränität« als Autonomie individueller Nutzer*innen s. auch Glasze/Dammann 2022 in diesem Band): Hindelang (2019: 18) spricht von »kommunikative[r] Selbstbestimmung des Einzelnen«, die im Internetkontext zunimmt, da die individuellen Rezipient*innen hier mehr Möglichkeiten haben, auszuwählen, welche Informationen sie rezipieren möchten. Sie müssen sich weniger als im Kontext traditioneller Medienangebote »den Konditionen und Beschränkungen Dritter für [ihre] kommunikativen Handlungen aussetzen« (ebd.: 6).

Seemann geht darüber noch hinaus: Für ihn wird die *Filtersouveränität* der Nutzer*innen im digitalen Kontext, verglichen mit dem Kontext traditioneller Medienangebote, nicht nur im Sinne der positiven Informationsfreiheit gesteigert – also dadurch, dass sich die Nutzer*innen aus einem breiteren Angebot von Inhalten die für sie passende Information auswählen können, indem sie mit sogenannten »Queries« gezielt Informationen abrufen, bestimmte Inhalte abonnieren und ihr Freund*innennetzwerk gestalten. Auch im Sinne der negativen Informationsfreiheit wächst die Souveränität der Nutzer*innen, da sie mithilfe der Query Informationen, die sie nicht aufnehmen möchten, in größerem Maße aussortieren können. Gleichzeitig sieht Seemann Personalisierung durch intransparente Algorithmen als problematisch an, denn hier »findet Informationbeschaffung [sic!] nicht selbstbestimmt statt, sondern

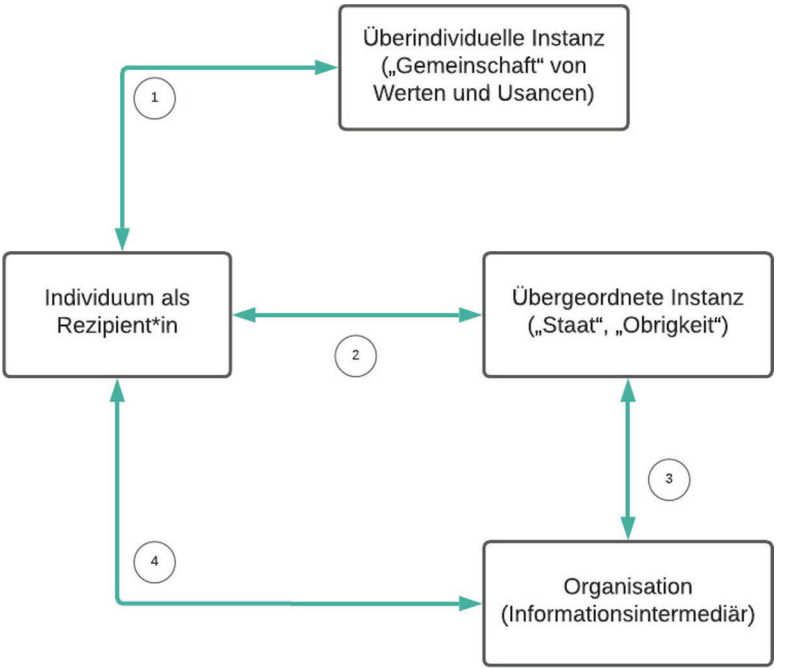
fremdgesteuert, mithilfe von Mechanismen, die wir nicht kontrollieren können« (Seemann 2014: 182).

Auch Bozdag nimmt mit seinem Konzept der *user autonomy* algorithmische Personalisierung in den Fokus. Dabei ist für ihn entscheidend, inwiefern Nutzer*innen die Kontrolle darüber ausüben, welche Information sie angezeigt bekommen. Allerdings will er *user autonomy* nicht als »full user control« (Bozdag 2013: 221) verstanden wissen: »User autonomy seems to have less to do with simply the degree of control and more to do with what aspects of the algorithm are controllable, and the user's conception and knowledge of the algorithm.« (ebd.: 221) Daher sollten Systeme, die auf Basis von Algorithmen Personalisierung vornehmen, mit den Nutzer*innen in Dialog treten und deutlich machen, warum und auf welcher Basis ein bestimmter Dienst personalisiert ist, sowie fragen, ob bestimmte Annahmen über die Nutzer*innen korrekt sind. So kontrollieren die Nutzer*innen zwar den Algorithmus nicht, können aber nachvollziehen, unter welchen Bedingungen bestimmte Empfehlungen gemacht werden.

2.2 Vier Relationen »digitaler Souveränität«

»Digitale Souveränität« bezieht sich im Diskurs um öffentliche Kommunikation also vor allem auf die Selbstbestimmung der Rezipient*innen gegenüber Informationsintermediären, also denjenigen, die Informationen auswählen, sortieren, personalisieren und gewichten (vgl. Abb. 2, Pfeil 4). Darüber hinaus identifiziert Hagenhoff (2020) aber noch drei weitere Beziehungen, in denen »digitale Souveränität« in der öffentlichen Kommunikation eine Rolle spielt (vgl. Abb. 2): Die Relation von Individuen als Rezipient*innen und über*individuellen* Instanzen (1), die Relation von Individuen als Rezipient*innen und über*geordneten* Instanzen (2) und die Relation von Organisationen bzw. Informationsintermediären und übergeordneten Instanzen (3).

Abbildung 2: Relationen »digitaler Souveränität« in der öffentlichen Kommunikation nach Hagenhoff (2020: 11ff.).



*(1) Relation von Individuen als Rezipient*innen und überindividuellen Instanzen (Wertzuschreibungen, Usancen)*

Überindividuelle Instanzen versteht Hagenhoff als Zusammenspiel von Werten und Usancen, die »für das Miteinander (implizite) Gepflogenheiten und Wertzuschreibungen [setzen], ohne dass diese einen formalisierten Prozess durchlaufen« (2020: 14). Sie werden oft auch als »Kultur« bezeichnet. Was zur »Hochkultur« zählt, wird im traditionellen Kommunikationskontext beispielsweise in der Literaturwissenschaft und im Feuilleton verhandelt. Im Internetkontext etablieren die Nutzer*innen von Soziale-Netzwerk-Seiten hingegen eine eigene »Kultur der Digitalität« (vgl. Sahner 2021; s. auch Stalder 2021), indem sie Memes erstellen, variieren und v.a. referenzieren. Für die Souveränität der Rezipient*innen ergeben sich damit folgende Fragen: Wie souverän agieren Rezipient*innen gegenüber überindividuellen Instanzen,

also Wertzuschreibungen und Gepflogenheiten? Welche Rolle spielt beispielsweise die Erwünschtheit verschiedener medialer Formen (Bücherlesen wird als wertvoller wahrgenommen als das Rezipieren von Facebook-Posts) oder die Bewertung bestimmter Inhalte (»Trivialliteratur« wird als weniger wertvoll wahrgenommen als »klassische« Literatur) für die kommunikative Selbstbestimmung der Rezipient*innen? Wie souverän können Rezipient*innen diese Usancen und Wertzuschreibungen gestalten und setzen?

*(2) Relation von Rezipient*in als Individuum und übergeordneter Instanz (»Staat«, »Obrigkeit«)*

Übergeordnete Instanzen wie z.B. staatliche Akteur*innen legen Regeln fest, die für die Kommunikation in einer Gesellschaft und damit sowohl für Organisationen als auch für Individuen gelten. Ein Beispiel ist die in Art. 5 des Grundgesetzes festgelegte Meinungs- und Informationsfreiheit, die für jedes Individuum u.a. das Recht festschreibt, sich aus allgemein zugänglichen Quellen ungehindert zu informieren. (Digitale) Souveränität spielt in dieser Relation in folgenden Fragen eine Rolle: Wie selbstbestimmt agieren Rezipient*innen gegenüber übergeordneten Instanzen (Meinungsfreiheit vs. staatliche Zensur)? Wie souverän wirken Rezipient*innen an der Gestaltung der Regeln mit, die für die öffentliche Kommunikation in einer Gesellschaft gelten (demokratische vs. autoritäre Staatsformen)?

(3) Relation Organisation (Informationsintermediär) und übergeordnete Instanz (»Staat«, »Obrigkeit«)

Die Beziehung zwischen Informationsintermediären und übergeordneten Instanzen wirft aus der Perspektive beider Akteur*innen Fragen der (digitalen) Souveränität auf. Erstens: Wie souverän agieren staatliche Akteur*innen gegenüber Organisationen wie Informationsintermediären, v.a. wenn Letztere über herausragende ökonomische Macht verfügen? Zweitens: Wie selbstbestimmt agieren Informationsintermediäre gegenüber übergeordneten Instanzen? So legen gesetzliche Vorgaben wie der Medienstaatsvertrag (MStV) in Deutschland beispielsweise verbindliche Regeln für Informationsintermediäre fest; deren Wirkmächtigkeit ist jedoch umstritten (vgl. Liesem 2020; Dogruel et al. 2020).

*(4) Relation Rezipient*in als Individuum und Organisation (Informationsintermediär)*

Die Relation der Rezipient*innen als Individuen zu Organisationen, also Informationsintermediären, knüpft an die oben beschriebenen Diskurse

um Filtersouveränität, Nutzer*innen-Autonomie und kommunikative Selbstbestimmung an: Hier geht es um die Frage, wie abhängig bzw. unabhängig Rezipient*innen von der Inhalte-Auswahl verschiedener Informationsintermediäre sind, die Informationen für sie verfügbar, sichtbar und rezipierbar machen. Wie selbstbestimmt, autonom und souverän sind Rezipient*innen bei der Auswahl von Informationen, die durch Informationsintermediäre vermittelt werden?

Die hier aufgeführten vier Relationen bieten einen Ausgangspunkt, um Souveränität in der öffentlichen Kommunikation zu diskutieren – sowohl im Kontext traditioneller Kommunikationsumgebungen, als auch im Internetkontext (vgl. Hagenhoff 2020).

2.3 Wie verändert Digitalisierung die Souveränitätszustände in der öffentlichen Kommunikation?

Wie also verändert die Digitalisierung die Souveränität in den vier oben beschriebenen Relationen in der öffentlichen Kommunikation? Problematisch ist es, dass im Diskurs um die Auswirkungen der Digitalisierung auf die öffentliche Kommunikation die Kategorie der Veränderung eine enorme Bestimmungsunschärfe aufweist, die sich sowohl in Bezug auf den präzisen Gegenstand der Veränderung als auch in Bezug auf den Referenzzustand und -zeitpunkt ausprägt (differenziert zum »Wandel« s. Klymenko 2019: 11f.). Solange die »Differenzqualität der bestaunten und besprochenen, verschiedenen Phänomene zu vorangegangenen Zuständen oder alternativen (etablierten) Prozessen und Technologien nicht und nicht systematisch herausgearbeitet wurde« (Hagenhoff 2020: 4), erzeugen diese Diskurse keinen substanziellen erkenntnistheoretischen Mehrwert. Vielmehr bedarf es einer gründlicheren, kriteriengeleiteten Analyse, die eine differenzierte Bewertung verschiedener Ausprägungen des Systems der öffentlichen Kommunikation ermöglicht.

An diesem Desiderat setzt dieser Beitrag an: Im Folgenden wird die Relation zwischen Rezipient*in und Informationsintermediär beispielhaft in den Blick genommen, um zu beschreiben, wie sich die Digitalisierung auf die Souveränitätszustände in der medienvermittelten öffentlichen Kommunikation auswirkt. Dazu ist eine Gegenüberstellung von traditionellen und Internet-Informationsintermediären gewinnbringend. Konkretisiert wird dieses anhand von Suchmaschinen als Internet-Intermediäre und Bibliotheken als traditionelle Intermediäre: Die Recherche in Bibliotheken wird vor allem in Forschungsarbeiten zu Privatsphäre-Fragen als Vorläufer oder Parallele zur

Suche in Suchmaschinen gesehen (vgl. Zimmer 2008; Nissenbaum 2010), sodass ein Vergleich dieser beiden Intermediärstypen auch für den Kontext der Nutzer*innen-Souveränität vielversprechend ist.

Ziel des Beitrags ist es, zu zeigen, wie auf Basis theoretischer Konzepte konkrete Kriterien für den Vergleich von traditionellen und Internet-Intermediären entwickelt und angewendet werden können. Die Analyse der Position von Suchmaschinen- und Bibliotheksnutzer*innen dient dabei der beispielhaften Illustration. Im Fokus dieses Beitrags stehen damit weniger die konkreten empirisch-heuristischen Erkenntnisse als vielmehr die Strategien, mit denen die Auswirkungen der Digitalisierung auf Souveränitätszustände in der medienvermittelten öffentlichen Kommunikation systematisch und kriteriengeleitet analysiert werden können.

3. Fallstudie: Souveränität als Salience bei Nutzer*innen von Bibliotheken und Suchmaschinen

Wie lässt sich also die Souveränität von Rezipient*innen in Relation zum traditionellen Intermediär *Bibliothek* und zum Internet-Intermediär *Suchmaschine* kriteriengeleitet analysieren? Das folgende Kapitel zeigt dies in einer Fallstudie auf. Dazu gibt Kapitel 3.1 zunächst einen Überblick über die Charakteristika von Bibliotheken und Suchmaschinen als Analyseobjekte. Zudem wird die Network-Gatekeeping-Theorie vorgestellt, die als theoretischer Rahmen und Analyseinstrument für die Untersuchung der Nutzer*innen-Position im traditionellen und im Internetkontext dient. Darauf aufbauend wird die Position der Nutzer*innen von Bibliotheken und Suchmaschinen anhand von vier Attributen analysiert und verglichen (s. Kap. 3.2 bis 3.5). Abschließend wird zusammengefasst, was sich daraus für die Differenzqualität der Nutzer*innen-Souveränität gegenüber Bibliotheken einerseits und Suchmaschinen andererseits ableiten lässt (s. Kap. 3.6).

3.1 Analyseobjekte und Analyseinstrument

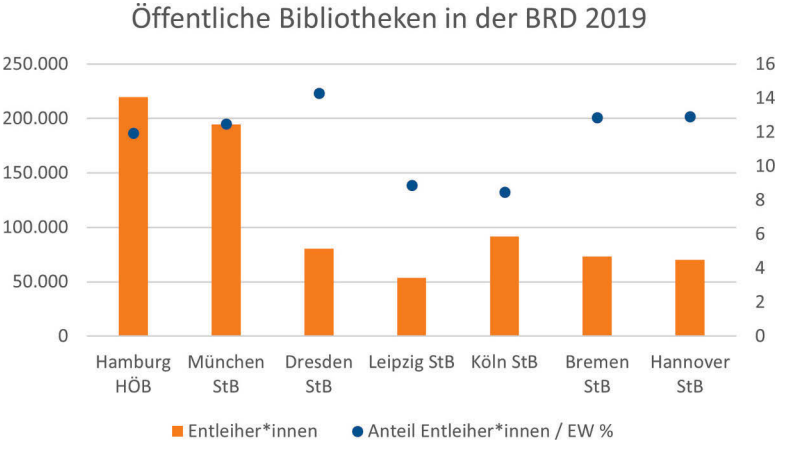
Analyseobjekt Bibliothek als traditioneller Informationsintermediär

Öffentliche Bibliotheken sind wichtige und relevante Intermediäre im System der medienvermittelten öffentlichen Kommunikation: Sie tragen zur Zirkulation redaktionell produzierter Informationen bei, indem sie aus den Neuerscheinungen der Medienmärkte Titel auswählen, diese warenartigen

Medien durch Erwerb oder Lizenzierung sowie physische Aufstellung in öffentlich zugängliche Information transformieren und durch Katalogisierung hierüber Transparenz für die Bürger*innen erzeugen (vgl. Umlauf 2015 und Rösch/Seefeldt/Umlauf 2019). Die Anzahl von gut 9.000 öffentlichen Bibliotheken in Deutschland (vgl. Rösch/Seefeldt/Umlauf 2019: 119) übersteigt die Anzahl der Buchhandlungen in Form von Ladengeschäften um das 1,5-fache (vgl. Börsenverein des Deutschen Buchhandels e.V. 2018).

Die praktische Bedeutung von Bibliotheken für die Zirkulation von Informationen kann anhand ihrer Nutzung sowie ihrer Reichweite abgeschätzt werden. Auf Basis der Kennzahlen der Deutschen Bibliotheksstatistik (2019) lassen sich – trotz einiger Unschärfen im Datenbestand – grobe Aussagen über die Größenklasse der Reichweite von Bibliotheken und auch über systematische Unterschiede zu Suchmaschinen treffen. Abbildung 3 zeigt sieben Bibliotheken, die im Jahr 2019 laut ihrer Eigenangaben in der Statistik mehr als 70.000 aktive Nutzer*innen oder über 5 Millionen Entleihungen verzeichneten.

*Abbildung 3: Aktive Nutzer*innen und Anteil der aktiven Nutzer*innen an den Einwohner*innen im Jahr 2019 (Deutsche Bibliotheksstatistik 2019).*



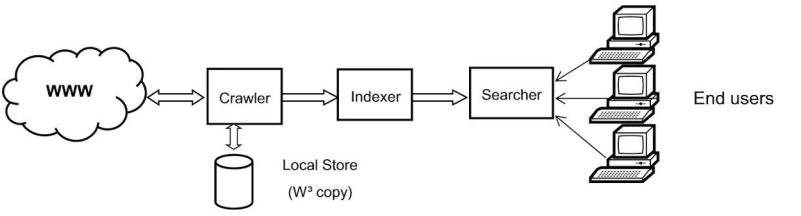
Bibliotheken umfassen nur einen Ausschnitt medial publizierter Inhalte. Die Größe dieses Ausschnitts kann eingeschätzt werden anhand der Anzahl

der Medieneinheiten einer Bibliothek. Für die zwölf größten Bibliotheken (mit einer Nutzer*innenzahl ab 50.000) liegt der Medianwert der verfügbaren Medieneinheiten bei ∼ 540.000, für kleinere Bibliotheken mit einer Zahl an aktiven Nutzer*innen zwischen 4.000 und 6.000 liegt er bei ∼ 45.000 Einheiten, über alle Bibliotheken bei ∼ 6.800 Einheiten. Das Verzeichnis Lieferbarer Bücher (VLB) listet demgegenüber ca. 2,5 Millionen Titel. Damit ist über Öffentliche Bibliotheken nur ein Bruchteil des Publizierten zugänglich.

Analyseobjekt Suchmaschine als Internet-Informationsintermediär

Suchmaschinen sind »die wichtigsten Navigationshilfen im Internet« (Jürgens/Stark/Magin 2014: 98). Sie ermöglichen Nutzer*innen, in der unüberblickbaren Zahl an verfügbaren Webseiten diejenigen zu finden, die zu ihrem Informationsbedürfnis passen (vgl. Unkel 2019). Suchmaschinen bestehen aus drei konzeptionellen Komponenten (vgl. Lewandowski 2018; s. Abb. 4): Sogenannte *Crawler* folgen den Links auf bereits bekannten Webseiten, finden so neue Webinhalte und speichern sie. Dieser Speicher wird laufend aktualisiert und bildet das »Rohmaterial« (Lewandowski 2018: 32), aus dem die Suchmaschine einen *Index* erstellt. Hierfür extrahiert der *Indexer* aus den gespeicherten Webinhalten die Informationen, die deren Wiederauffinden und Ranking ermöglichen (vgl. Unkel 2019). Der *Searcher* arbeitet an der Schnittstelle zu den Nutzer*innen: Er erstellt auf Basis des Index eine Sammlung von Webinhalten, die zur Nutzer*innenanfrage passen. Ein Rankingmodul sortiert die Suchergebnisse anschließend so, dass ganz oben diejenigen Inhalte angezeigt werden, die aus Sicht der Suchmaschine am relevantesten für die jeweilige Suchanfrage sind (vgl. Milker 2019).

Abbildung 4: Komponenten von Suchmaschinen (Lewandowski 2018: 31).



Prinzipiell verfolgen Suchmaschinen das Ziel, »ein vollständiges Abbild des World Wide Web« (Lewandowski 2018: 33) zu erstellen. Aufgrund der Dynamik und Größe des Webs ist es aber äußerst schwierig zu untersuchen, wie viele Dokumente es im Web insgesamt gibt; damit ist auch eine Aussage darüber, welcher Anteil des Webs über Suchmaschinen auffindbar ist, nahezu unmöglich. Es ist jedoch davon auszugehen, dass Suchmaschinen über das Verfolgen von Links auf bekannten Seiten nicht das komplette World Wide Web erfassen können. Beim Crawlen werden zudem bestimmte Dokumente aufgrund technischer oder inhaltlicher Aspekte ausgeschlossen, beispielweise wegen Urheberrechtsverletzungen, des Jugendschutzes oder der Einordnung als Spam (vgl. ebd.). Dennoch bilden Suchmaschinen insgesamt einen beträchtlichen Anteil aller frei zugänglichen Dokumente im Web ab – dies wird vor allem im Vergleich zu Bibliotheken deutlich, die wie oben beschrieben nur einen Bruchteil aller auf dem Buchmarkt verfügbaren Publikationen anbieten.

Suchmaschinen haben eine sehr hohe Reichweite: Nach Andree und Thomsen (2020) nutzten 99,0 Prozent der Internetuser*innen in Deutschland im Jahr 2019 Suchmaschinen. Auch die repräsentative Mediengewichtungsstudie der Landesmedienanstalten kommt zu dem Schluss, dass 2019 über die Hälfte der Personen über 14 Jahre in Deutschland täglich eine Suchmaschine nutzte (vgl. Die Medienanstalten 2020). Deutlicher Marktführer ist dabei Google (vgl. Abb. 5 u. 6).

Abbildung 5: Tagesreichweite von Suchmaschinenanbietern in Deutschland (Die Medienanstalten 2020: 24).

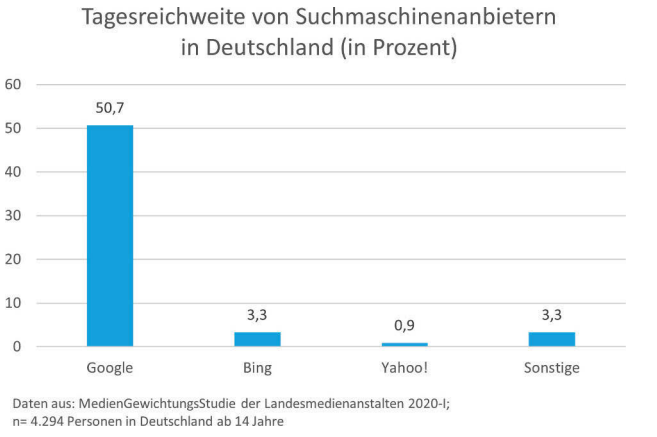
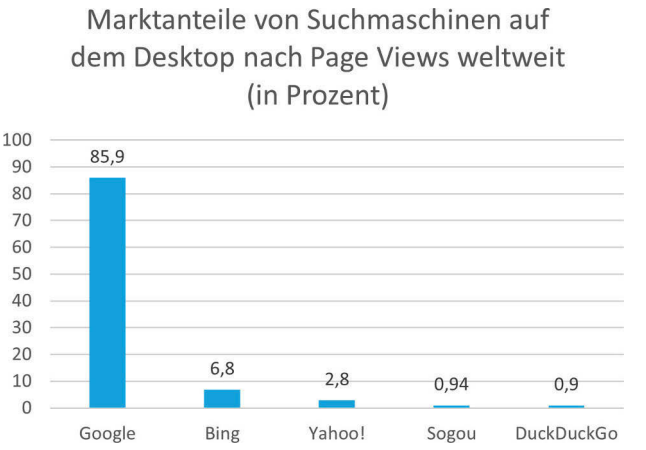


Abbildung 6: Marktanteile von Suchmaschinen auf dem Desktop nach Page Views weltweit (StatCounter 2021).



Network-Gatekeeping-Theorie als Analyseinstrument

Um die Relation zwischen Rezipient*innen und Informationsintermediären zu untersuchen, bietet die Network-Gatekeeping-Theorie (NGT) von Barzilai-Nahon (2008) einen theoretischen Rahmen. Sie setzt auf dem grundlegenden Phänomen des Gatekeeping auf, welches in allen Ausprägungsformen der öffentlichen Kommunikation anzutreffen ist. Barzilai-Nahon kritisiert allerdings traditionelle Gatekeeping-Ansätze, da diese den »changing communication environments« (DeIuliis 2015: 12) nicht gerecht werden, Gatekeeping als »one-way direction and top-down process« (Barzilai-Nahon 2008: 1494) begreifen und die Rolle der Rezipient*innen außer Acht lassen. Insbesondere die einfache Möglichkeit des Rollenwechsels von passiven Rezipierenden zu aktiven Beteiligten wird in den klassischen Ansätzen vernachlässigt. Mit der NGT entwirft Barzilai-Nahon daher eine interdisziplinäre Theorie, die den Gatekeeping-Ansatz für den Internetkontext ausbaut und erneuert (2009). Zentral ist dabei die Einführung des Begriffs der *Gated*, der diejenigen beschreibt, die einem Gatekeeping-Prozess unterliegen (Barzilai-Nahon 2008). Gated können individuelle Nutzer*innen, aber auch ökonomische Akteur*innen wie Unternehmen oder Verbände sein. *Gatekeeper* sind nach Barzilai-Nahon hingegen Instanzen, die Gatekeeping ausführen, die also Kontrolle

(s.o.: Points of Control) über Information ausüben »as it moves through a gate« (Barzilai-Nahon 2008: 1496; vgl. Kapitel 1.2).

Welche Position die Gated gegenüber dem Gatekeeper haben, ist in der NGT zentral und wird mit dem Begriff der *Gated Salience* beschrieben: *Salience* steht für die Wichtigkeit oder die Bedeutung der Gated für den Gatekeeper (vgl. Leavitt 2016) und damit »the degree to which gatekeepers give priority to competing gated claims« (Barzilai-Nahon 2009: 33), also die Möglichkeit der Gated, die Handlungen und Entscheidungen des Gatekeepers zu beeinflussen. Die Salience der Gated wird anhand von vier Attributen manifest: der politischen Macht der Gated gegenüber dem Gatekeeper; der Fähigkeit der Gated, selbst Informationen zu produzieren; der Beziehung der Gated zum Gatekeeper; und schließlich anhand der Alternativen, die zum Gatekeeper vorhanden sind (vgl. Leavitt 2016). Indem analysiert wird, in welcher Ausprägung ein Gated diese vier Attribute besitzt, kann die Salience eines bestimmten Gated gegenüber einem spezifischen Gatekeeper beschrieben werden (vgl. Barzilai-Nahon 2009). Damit bietet die NGT einen theoretischen Rahmen, um die Souveränität der Rezipient*innen als Gated in Relation zu Informationsintermediären als Gatekeeper zu analysieren.

Vorgehen bei der Analyse der Gated Salience

Oben wurde argumentiert, dass verschiedene Ausprägungen des Systems der öffentlichen Kommunikation einer kriteriengeleiteten Analyse bedürfen, um fundiertere Aussagen zu Andersartigkeit oder Veränderung erzeugen zu können. Die NGT bietet mit den vier Attributen nutzbare Kriterien, die im Folgenden auf die Untersuchungsobjekte Bibliothek sowie Suchmaschine angewendet werden. Untersucht werden soll, ob Gated ein Attribut besitzen oder nicht. Dieser Beitrag ist als ein erster Versuch einer solchen kriteriengeleiteten Analyse der Differenzqualität zu verstehen, der methodisch herausfordernd ist und daher Grenzen aufweist: Neben einer Analyse anhand allgemeiner Strukturmerkmale der betrachteten Intermediäre macht es die große Bandbreite der realen Ausprägungen der beiden abstrakten Intermediäre jedoch auch erforderlich, konkrete Untersuchungsobjekte auszuwählen, an denen Umsetzungen der abstrakt beschriebenen Attribute geprüft werden. Welche Beispiele ausgewählt werden, ist dabei wie in allen qualitativen Studien entscheidend: Nicht alle Fälle, die zu einem bestimmten Untersuchungsgegenstand passen, können analysiert werden; zugleich beeinflusst die Auswahl der Fälle, »in welche Richtung die Ergebnisse einer Untersuchung

verallgemeinert werden können« (Przyborski/Wohlrab-Sahr 2014: 177). Für diese Untersuchung können folgende Überlegungen angestellt werden:

Es ist davon auszugehen, dass die öffentliche Kommunikation grundsätzlich von Gatekeepern mit großer Reichweite in größerem Maße mitgestaltet wird als von solchen, die nur relativ wenige Rezipient*innen erreichen. Die Verbreitung von Suchmaschinen lässt sich an ihrer Tagesreichweite festmachen, sodass der in Deutschland reichweitenstärkste Anbieter Google im Folgenden beispielhaft in den Blick genommen wird. Als Referenzpunkt werden diejenigen Bibliotheken in Deutschland betrachtet, die die größte absolute Anzahl an aktiven Nutzer*innen und Entleihungen aufweisen: Eine Bibliothek, die eine hohe fünfstellige Zahl an Nutzer*innen aufweist, ist ein potenziell wirkmächtigerer Intermediär als eine Bibliothek mit wenigen hundert Nutzer*innen. Nicht überraschend ist, dass sich die in diesem Sinne reichweitenstärksten Bibliotheken in Großstädten befinden (vgl. Abb. 3). Während die reichweitenstärksten Bibliotheken und Suchmaschinen in Deutschland den Ausgangspunkt der Analyse bilden, werden zusätzlich Beispiele einbezogen, die sich minimal und maximal von den Ausgangsbeispielen unterscheiden. Wenn ein oder mehrere der Beispiele zeigen, dass Gated ein Attribut innehaben – also z.B. politische Macht auf den Gatekeeper ausüben können –, ist dies ein Indikator dafür, dass Gated das jeweilige Attribut besitzen; zeigen ein oder mehrere Beispiele hingegen, dass Gated das Attribut nicht innehaben – also z.B. erfolglos versuchen, politische Macht auf den Gatekeeper zu nehmen –, deutet dies darauf hin, dass Gated das Attribut nicht besitzen. Die ausgewählten Fälle sind damit nicht zwingend repräsentativ, »sie repräsentieren aber sehr wohl die Strukturmuster« des Untersuchungsgegenstands (Przyborski/Wohlrab-Sahr 2014: 182). Dieses Vorgehen ist eine – für diesen ersten Zugang zur Analyse der Differenzqualität vereinfachte – Anwendung des *theoretical samplings* (s. hierzu Truschkat/Kaiser-Belz/Reinartz 2007; Baur/Blasius 2014).

3.2 Salience als Politische Macht

Barzilai-Nahon (2008: 1501ff.) unterscheidet drei verschiedene Formen, wie Gated gegenüber dem Gatekeeper politische Macht ausüben können. Die erste Form von Macht besteht darin, dass ein*e Akteur*in eine*n andere*n Akteur*in dazu bringen kann, etwas zu tun, was diese*r sonst nicht getan hätte. Verfügen Gated über Macht dieser Art, können sie direkt Einfluss auf die Entscheidungen des Gatekeepers nehmen. In demokratisch organisierten Staaten

können Nutzer*innen von Informationsintermediären also politische Macht ausüben, indem sie als Wähler*innen die Gesetzgebung zu Informationsintermediären beeinflussen. Ob Regeln dann wirkmächtig sind, hängt davon ab, wie kostspielig die Ermittlung von Regelverstößen ist und wie effektiv Sanktionen wie Strafen oder Anreize wirken (vgl. Scott 2009). Die politische Macht der Gated hängt also auch davon ab, inwiefern die Einhaltung der gesetzlich festgelegten Regeln faktisch überprüft und sanktioniert werden kann. Eine Möglichkeit hierbei kann für Gated die gerichtliche Klage darstellen.

Gated können des Weiteren politische Macht ausüben, indem sie Einfluss auf die öffentliche Diskussion nehmen (zweite Form) und die Aufmerksamkeit sowie die Vorlieben von Entscheidungsträger*innen und anderen Gated beeinflussen (dritte Form). Nutzer*innen von Informationsintermediären können die öffentliche Diskussion beeinflussen, indem sie in kollektiven Aktionsgruppen, Interessengemeinschaften oder als Individuen mit großer Sichtbarkeit Forderungen an den Informationsintermediär stellen und verschiedene Formen des Protests ausüben (vgl. West 2017). Die gleichen Strategien können Nutzer*innen von Informationsintermediären anwenden, um die dritte Form von Macht auszuüben, z.B. indem sie mit individuellen oder kollektiven Aktionsformen andere Nutzer*innen beeinflussen oder die Aufmerksamkeit von Entscheidungsträger*innen auf eine bestimmte Problematik lenken, die die Praktiken des Informationsintermediärs mit sich bringen – beispielsweise durch Demonstrationen, Online-Petitionen und Postkarten- oder E-Mail-Aktionen an Entscheidungsträger*innen.

Politische Macht der Gated von Bibliotheken

Öffentliche Bibliotheken sind keine privatwirtschaftlichen Unternehmen, sondern meist Einrichtungen der öffentlichen Hand. Dies ist für die politische Macht der Gated von Bibliotheken entscheidend. Gut die Hälfte der etwa 9.000 Öffentlichen Bibliotheken in Deutschland befindet sich in kommunaler Trägerschaft oder der Trägerschaft von Landkreisen. Als »öffentliche Anstalten mit dem Status einer nachgeordneten Behörde« (Deutscher Bundestag – Wissenschaftliche Dienste 2008: 14) unterliegen sie verbindlichen Vorschriften und Regeln, die von Stadträten und Kreistagen erlassen werden. Über die Zusammensetzung dieser Gremien bestimmten die Nutzer*innen Öffentlicher Bibliotheken als Wähler*innen in der jeweiligen Kommune. Zudem steht den Nutzer*innen von Bibliotheken die Möglichkeit einer Klage gegen das Vorgehen von Bibliotheken offen – meist vor dem örtlichen Verwaltungsgericht. So wehrten sich Nutzer*innen verschiedener kommunaler

Bibliotheken in Deutschland im Zeitraum von 2000 bis 2015 gerichtlich gegen Hausverbote, Säumnisgebühren oder die Einstellung des Bücherbusses (vgl. Bibliotheksurteile 2020). Unterschieden werden müssen Öffentliche Bibliotheken in der Trägerschaft von Kommunen oder Landkreisen von solchen in der Trägerschaft von Pfarr- und Kirchengemeinden. Letztere unterstehen den für die Gemeinde zuständigen Pfarrer*innen oder rechtlich vertretenden Gremien, z.B. dem Kirchenvorstand oder Pfarr- und Kirchengemeinderäten (vgl. Rösch/Seefeldt/Umlauf 2019: 89). Gewählte Gremien haben nur in nachgeordneter Stellung nach dem*der Pfarrer*in Entscheidungsbefugnisse für die jeweilige Bibliothek. Zudem werden diese Gremien ausschließlich von den Mitgliedern der jeweiligen Kirchengemeinde gewählt (vgl. Evangelische Landeskirche in Baden 2007; Zawidzki/Gahlau 2018). Somit haben lediglich diejenigen Nutzer*innen kirchlicher Bibliotheken, die der entsprechenden Konfession angehören, als Wähler*innen Einfluss auf die Gremien, die Leitsätze und Vorschriften für die Bibliotheken festlegen. Nutzer*innen, die nicht Mitglied der jeweiligen Kirchengemeinde sind, können keinen direkten Einfluss auf kirchliche Bibliotheken nehmen.

Inwiefern Gated von Bibliotheken auf der zweiten und dritten Macht-Ebene Einfluss auf den Gatekeeper nehmen können, lässt sich nicht eindeutig bestimmen. Während einige Beispiele zeigen, dass Nutzer*innen erfolgreich Einfluss auf Entscheidungen des Gatekeepers nehmen, indem sie die öffentliche Diskussion, andere Nutzer*innen und Entscheidungsträger*innen beeinflussen, zeigen andere Beispiele, dass Nutzer*innen hierbei keine Einflussnahme gelingt. Wieder andere Beispiele machen deutlich, dass vereinzelte Bibliotheken ihre Nutzer*innen von sich aus aktiv in Entscheidungsprozesse einbinden. Für ein solches aktives Einbeziehen nutzen Bibliotheken verschiedene Methoden der Bürgerbeteiligung.

Für das Attribut der politischen Macht der Gated von Bibliotheken ergibt sich also ein differenziertes Bild: So können Gated von Bibliotheken, die von Kommunen oder Landkreisen getragen werden, eindeutig die erste Form politischer Macht auf den Gatekeeper ausüben. Die politische Macht der Gated von Bibliotheken in kirchlicher Trägerschaft hängt jedoch davon ab, ob die jeweiligen Gated Mitglied der entsprechenden Kirchengemeinde sind und wie stark die Stellung des Kirchen- oder Pfarrgemeinderates gegenüber dem*der Pfarrer*in ist. Ob Gated auf der zweiten und dritten Macht-Ebene Einfluss auf den Gatekeeper nehmen können, ist nicht eindeutig zu bestimmen; dies entscheidet sich von Fall zu Fall.

Politische Macht der Gated von Suchmaschinen

Dass Gated von Suchmaschinen in Deutschland mittels gesetzlicher Regulierung Einfluss auf Suchmaschinenbetreiber nehmen können, zeigen die Regelungen der *EU-Datenschutz-Grundverordnung (DSGVO)* und des *Medienstaatsvertrags (MStV)*. Der MStV verpflichtet Suchmaschinen als Medienintermediäre u.a. dazu, die Kriterien für die Selektion und Präsentation von Suchergebnissen transparent zu machen und zu verhindern, dass »diese Kriterien Angebote unmittelbar oder mittelbar unbillig systematisch behindern« (MStV § 93, Absatz 2). Spezielle Regelungen für Suchmaschinen enthält auch die DSGVO, indem sie das sogenannte »Recht auf Vergessenwerden« festschreibt. Dieses verpflichtet die Betreiber von Suchmaschinen dazu, Nutzer*innen die Möglichkeit zu geben, die Löschung von Suchergebnissen zur eigenen Person zu beantragen (vgl. Leutheusser-Schnarrenberger 2018; Datenschutz.org 2020).

Als Wähler*innen der Politiker*innen, die Gesetze in Deutschland bzw. in der Europäischen Union erlassen, haben Gated von Suchmaschinen also die Möglichkeit, die erste Form politischer Macht gegenüber Suchmaschinenbetreiber auszuüben. Inwieweit die Transparenz- und Diskriminierungsfreiheitsvorgaben des MStV Wirkung entfalten, ist allerdings umstritten (vgl. Liesem 2020; Dogruel et al. 2020). Zudem bleibt fraglich, inwiefern Regulierungsmaßnahmen in nationalem bzw. europäischem Recht greifen, da Suchmaschinen international agierende Unternehmen sind (vgl. Dörr/Schuster 2014).

Diese Problematik wird auch deutlich, wenn Nutzer*innen außerhalb der USA ihre Interessen gegenüber Suchmaschinenbetreibern wie Google mithilfe gerichtlicher Klagen durchzusetzen versuchen: Hier ist bislang die Frage ungeklärt, ob die Klagezustellung an einen deutschen Firmensitz des Suchmaschinenunternehmens zulässig ist oder ob Kläger*innen eine kostenaufwendige Klagezustellung in die USA auf sich nehmen müssen (vgl. Truscheit 2019; Emonts 2019).

Die Frage, ob Gated von Suchmaschinen die zweite und dritte Form von Macht gegenüber dem Gatekeeper ausüben können, kann nicht eindeutig beantwortet werden: Verschiedene Typen von Suchmaschinen-Gated haben in unterschiedlichem Maße die Möglichkeit, Einfluss auf die öffentliche Diskussion, andere Nutzer*innen und Entscheidungsträger*innen zu nehmen. So haben Gated, die zugleich Angestellte eines Suchmaschinenunternehmens sind, eine hervorgehobene Position und können auf der zweiten und dritten Macht-Ebene Einfluss auf den Gatekeeper nehmen: Die Entwicklung einer zensierten Suchmaschine für China scheiterte beispielsweise am Widerstand

von Google-Mitarbeiter*innen (vgl. Matthes 2018). Auch die Proteste gegen Neuerungen in der Google-Bildersuche zeigen, dass die politische Macht zweiter und dritter Form bei verschiedenen Typen von Gated unterschiedlich ausgeprägt ist: So ist der Einfluss, den Gated auf den Gatekeeper ausüben können, stark von der wirtschaftlichen Größe und Bedeutung der Gated abhängig (vgl. Initiative Urheberrecht 2017, 2018). Die Möglichkeit, die öffentliche Diskussion, andere Nutzer*innen und Entscheidungsträger*innen zu beeinflussen und damit politische Macht auf den Gatekeeper auszuüben, ist also nicht für alle Gated von Suchmaschinen gleichermaßen gegeben.

3.3 Salience als Fähigkeit der Produktion von Information

Für die Salience der Gated ist weiterhin entscheidend, ob sie die Fähigkeit besitzen, selbst Inhalte verschiedener Formate zu produzieren und zu verbreiten. Die Fähigkeit und Möglichkeit der aktiven Teilhabe an medial vermittelter Kommunikation entspricht der oben genannten umfänglichen Zugänglichkeit zur Öffentlichkeit. Die NGT unterscheidet sich dabei stark von traditionellen Gatekeeping-Ansätzen, die lediglich den Gatekeeper als Produzenten und Verbreiter von Inhalten untersuchen und die Informationsproduktion durch die Gated außen vor lassen (vgl. Barzilai-Nahon 2009). Gated besitzen das Attribut der Informationsproduktion aber nur dann in wirksamer Form, wenn die von ihnen produzierten Inhalte andere Nutzer*innen auch tatsächlich erreichen:

> »The ability of the gated to produce information does not necessarily ensure that information will reach other people. Information production is merely a prerequisite for information transfer […]. Therefore, although content is apparently easy to produce, some political, economical, and social impediments exist for the gated to reach other users.« (Barzilai-Nahon 2008: 1500)

Informationsproduktion der Gated von Bibliotheken

Die grundsätzliche Rolle von Bibliotheken besteht, wie oben beschrieben, darin, Bürger*innen Medien (unentgeltlich oder sehr kostengünstig) zugänglich zu machen. Die Bibliothek befindet sich innerhalb des Systems der öffentlichen Kommunikation funktional auf der gleichen Stufe wie der Buch- und Pressehandel. Die Unterstützung der Produktion von Informationen ist (bisher) nicht die Aufgabe dieses Typs von Intermediär. Mit der obigen Argumentation – die Produktion von Informationen ist wirkungslos ohne

Zirkulation oder Distribution – können dennoch zwei Aspekte diskutiert werden:

Zum einen kann die Frage thematisiert werden, wie sich das Portfolio von Öffentlichen Bibliotheken als Gatekeeper mit der Funktion, die Zirkulation von Medien zu unterstützen, zusammensetzt in Bezug auf die Art der Inhalteproduzent*innen. Traditionell werden Bücher von Verlagen erzeugt, also in professionellen Strukturen im oben diskutierten Sinne (Leistungsrollen) hervorgebracht. Im Zuge der Digitalisierung wurde das Selfpublishing möglich: Autor*innen veröffentlichen Bücher ohne diese professionellen Strukturen, aber mithilfe von Plattformen wie Kindle Direct Publishing oder Epubli. Über den etablierten Buchhandel sind solche Titel verfügbar, wenn sie über eine ISBN verfügen, also das zentrale Metadatum des Wertschöpfungssystems *Buch* aufweisen. In öffentlichen Bibliotheken spielen laut einer Studie von 2017 Titel von Selfpublishern »generell keine Rolle« (Behrens 2017: 187). Auch das Bibliothekskonzept der Bücherhallen Hamburg für das Jahr 2021 legt beispielsweise fest: »Wird ein Titel von einem Self-Publisher angeboten, wird er nicht in den Bestand aufgenommen, da keine Qualitätssicherung durch einen Verlag gegeben ist.« (Schwemer-Martienßen/Studt 2021: 93) Darüber hinaus dürften Selfpublishing-Titel dem Fokus der meisten Erwerbungsbibliothekar*innen in Öffentlichen Bibliotheken ohnehin entgehen: Zahlreiche Öffentliche Bibliotheken in Deutschland stützen sich bei der Erwerbung vorrangig auf einen Lektoratsdienst der Einkaufszentrale für Öffentliche Bibliotheken (ekz), der aus den etwa 80.000 Verlagspublikationen pro Jahr ca. ein Viertel auswählt und für Bibliothekar*innen rezensiert (vgl. ekz.bibliotheksservice GmbH 2021).

Zweitens könnten Bibliotheken ihren Nutzer*innen einen aktiven Kommunikationskanal bieten, in dem sie die Kommentierung bzw. Besprechung der gelesenen Werke auf den Bibliotheksseiten ermöglichen und hierüber eine moderne Variation der Lesegesellschaften ausprägen. So ermöglichen die Stadtbibliotheken Köln und Hannover ihren Nutzer*innen beispielsweise, »Leserbewertungen« zu einzelnen Titeln im Onlinekatalog der jeweiligen Bibliothek zu veröffentlichen. Eine solche Funktion wurde aber nur bei zwei der sieben Bibliotheken mit der größten Reichweite in Deutschland gefunden. Eher unwahrscheinlich ist es, dass auch Nutzer*innen von Bibliotheken mit geringer Reichweite Rezensionen über den Onlinekatalog des jeweiligen Gatekeepers verbreiten können: Die drei Bibliotheken, die 2019 die wenigsten Entleihungen verzeichneten, namentlich die Gemeindebüchereien Treben, Kettenkamp und Höxter, stellen gar keinen Onlinekatalog zur Verfügung.

Insgesamt haben Bibliotheksnutzer*innen das Attribut der Informationsproduktion – mit wenigen kleinen Ausnahmen – also nicht inne, was im Kern aber der definierten Aufgabe einer Bibliothek entspricht. Gleichzeitig hilft der etablierte Intermediär Öffentliche Bibliothek allerdings auch nicht dabei, dass zur Kommunikation ertüchtigte Individuen als Selfpublishing-Autor*innen hörbar werden, indem ihre Werke auf einem etablierten Weg zur Zirkulation gebracht werden.

Informationsproduktion der Gated von Suchmaschinen

Auch Suchmaschinen sind in ihrer funktionalen Logik innerhalb des Systems der öffentlichen Kommunikation nicht dazu entworfen worden, die Produktion von Informationen zu unterstützen, sondern produzierte Information zu finden. Dennoch kann auch hier, anknüpfend an die obige Diskussion des Selfpublishings, ein Aspekt diskutiert werden, der ggf. eine strukturelle Divergenz zu etablierten Intermediären aufzeigt. Mithilfe digitaler Tools wie Wordpress oder Tumblr, »that are ready-to-use and easy-to-use« (Barzilai-Nahon 2008: 1500), verfügt der*die aktiv kommunizierende Bürger*in über einen kommunikativen Zugang zur Öffentlichkeit. Wie argumentiert, wird die Produktion von Information aber erst dann wirksam, wenn potenzielle Empfänger*innen diese auch wahrnehmen und zu faktischen Rezipient*innen werden. Hierbei helfen Suchmaschinen, die, wie in Kapitel 3.1 beschrieben, konzeptionell alles finden, was im frei zugänglichen Internet positioniert wurde. Suchmaschinen sind daher ein prinzipiell wirksamer Intermediär, der bei der Zirkulation der produzierten Informationen hilft. Wie gut dieses faktisch gelingt, hängt a) von der technischen Implementierung, dem Geschäftsmodell und den Vorannahmen der Suchmaschinenanbieter ab, aber auch b) vom Klickverhalten der Webnutzer*innen und davon, ob es c) den Gated möglich wird, Fähigkeiten im Bereich von Search Engine Optimization (SEO) zu erwerben, also Strategien zu entwickeln, die die Webseite möglichst weit oben in der Ergebnisliste erscheinen lassen (vgl. Kelsey 2017).

Dabei können verschiedene Formen von Verzerrungen (sog. Bias) entstehen: Die Algorithmen, die über die Zusammensetzung von Suchergebnislisten entscheiden, sind zwangsläufig von menschlichen Vorannahmen geprägt und damit nicht neutral. Zudem ist die Sichtbarkeit selbst erstellter Inhalte einzelner Gated auch von deren jeweiligen Ressourcen abhängig: Da das Geschäftsmodell von Suchmaschinen wie Google auf dem Verkauf personalisierter Werbung basiert, sind Inhalte, die als bezahlte Anzeigen prominent in der Suchergebnisliste platziert werden, deutlich sichtbarer als andere Inhalte. Auch die

Umsetzung von SEO erfordert Zeit, Fähigkeiten oder finanzielle Ressourcen und führt damit zu Verzerrungen in der Sichtbarkeit von Inhalten in Suchergebnislisten. So können Medienangebote wie Spiegel Online beispielsweise eine deutlich größere Sichtbarkeit in Suchmaschinen erreichen als individuelle Gated (vgl. Brosius 2016; Lewandowski 2018).

3.4 Salience als Beziehung der Gated zum Gatekeeper

Die Salience der Gated gegenüber dem Gatekeeper wird auch durch die Beziehung zum Gatekeeper bestimmt. Zwischen Gated und Gatekeeper können Positionen ausgehandelt werden, wenn eine direkte und dauerhafte Verbindung zwischen beiden vorliegt. Ein direkter Austausch ermöglicht es den Gated, ihre Macht bzw. die Art der Beziehungen zum Gatekeeper zu verändern. Um die Beziehung zwischen Nutzer*innen und Informationsintermediären beschreiben zu können, muss also untersucht werden, ob es einen regelmäßigen, direkten und gegenseitigen Austausch zwischen dem jeweiligen Informationsintermediär als Gatekeeper und den Nutzer*innen als Gated gibt. Dazu müssen mehrere Fragen beantwortet werden:

- Kommunizieren die Gatekeeper direkt mit den Gated, und wenn ja, wie oft?
- Gibt es einen Kommunikationskanal, über den die Gated direkt mit dem Gatekeeper kommunizieren können?
- Erhalten die Gated eine Rückmeldung vom Gatekeeper? Reagieren Gatekeeper auf Anfragen, Kritik, Forderungen und Wünsche der Gated?

Beziehung der Gated von Bibliotheken zum Gatekeeper

Gated von Bibliotheken haben das Attribut der Beziehung zum Gatekeeper eindeutig inne: Die hier beispielhaft untersuchten Öffentlichen Bibliotheken bieten ihren Nutzer*innen etliche Kommunikationskanäle und Möglichkeiten, um mit ihren Mitarbeiter*innen Kontakt aufzunehmen – neben Besuchs- und Mailadressen finden Nutzer*innen auf den Bibliothekswebsites auch Telefonnummern und Online-Kontaktformulare. Der Austausch zwischen Bibliotheken und Nutzer*innen kann dabei als wechselseitig beschrieben werden: So veröffentlichte die Stadtbibliothek Bremen beispielsweise die Ergebnisse ihrer Nutzungsbefragung von 2019 auf ihrer Website. Dabei werden

einzelne Kritikpunkte und Fragen der Nutzer*innen herausgegriffen und von der Bibliothek beantwortet (vgl. Stadtbibliothek Bremen 2019a).

Darüber hinaus treten Bibliotheken als Gatekeeper von sich aus in die Kommunikation mit ihren Nutzer*innen, indem sie über neue Angebote und Dienstleistungen, Veranstaltungen und Neuerungen informieren, beispielsweise auf der eigenen Website, der Website des Trägers, auf Sozialen Netzwerk-Seiten, mit einem Newsletter oder mit Flyern, Broschüren und Plakaten (vgl. Bibliotheksportal 2017).

Wie ausführlich und regelmäßig Bibliotheken mit ihren Nutzer*innen kommunizieren und wie viele Kommunikationskanäle Nutzer*innen zur Verfügung stehen, hängt allerdings stark von der Größe der jeweiligen Bibliothek ab. Nimmt man als maximal kontrastierende Beispiele zu den reichweitenstärksten Bibliotheken in Deutschland diejenigen Bibliotheken in den Blick, die im Jahr 2019 die geringsten Ausleihzahlen verzeichneten, wird dies deutlich: Die Gemeindebibliotheken Treben, Kettenkamp und Höxter haben keinen Webauftritt; auch Kontaktdaten wie eine Telefonnummer oder eine Mailadresse sind nicht zu finden. Insgesamt haben Bibliotheksnutzer*innen das Attribut der Beziehung zum Gatekeeper dennoch eindeutig inne: Auch Nutzer*innen kleiner Bibliotheken ohne Webauftritt und Social-Media-Accounts haben die Möglichkeit, vor Ort mit den Bibliotheksmitarbeiter*innen Kontakt aufzunehmen und in einen direkten, wechselseitigen und dauerhaften Austausch zu treten.

Beziehung der Gated von Suchmaschinen zum Gatekeeper

Nutzer*innen der Suchmaschine Google finden hingegen nur mit Ausdauer einen Kommunikationskanal, über den sie den Suchmaschinenbetreiber kontaktieren können. Auf der Kontaktseite von Google wird zunächst die Adresse des Unternehmenssitzes in Irland angezeigt (vgl. Google 2021a; s. Abb. 7); die Postadresse der Hamburger Google-Zentrale und eine Telefonnummer mit deutscher Vorwahl ist nur mit weiterer Recherche zu finden (vgl. Google 2021b).

Abbildung 7: Kontaktseite von Google (Google 2021a).

Nutzer*innen werden unter dieser Nummer jedoch nicht mit einem*einer Mitarbeiter*in des Suchmaschinenanbieters verbunden, sondern gelangen nach mehreren automatisierten Auswahlmöglichkeiten schließlich zur Ansage »leider haben wir keine festen Support-Teams in diesem Office« und werden auf die Support-Seite von Google verwiesen. Gated des Suchmaschinenanbieters Google haben damit nur sehr eingeschränkt die Möglichkeit, den Gatekeeper direkt zu kontaktieren.

Auch wechselseitig ist der Kontakt der Gated zu Suchmaschinen nicht: Auf Anfragen erhalten Nutzer*innen meist keine Rückmeldung (vgl. Keddi 2015) oder lediglich »vorgefertigte Sätze« (Emonts 2019). Über Accounts in den Sozialen Netzwerk-Seiten Facebook, Instagram, Youtube und Twitter berichtet Google Deutschland jedoch von seinen Produkten und über Neuigkeiten aus dem Unternehmen (vgl. Google 2021a) und nutzt hierfür auch einen Blog in englischer Sprache (vgl. Google 2021c). Damit tritt Google Deutschland zwar mit denjenigen Nutzer*innen von sich aus in Kontakt, die auch Soziale-Netzwerk-Seiten nutzen. Von einem regelmäßigen, direkten und gegenseitigen Austausch zwischen Gatekeeper und Gated kann beim Suchmaschinenanbieter Google jedoch nicht gesprochen werden.

Auch die Nutzer*innen von Bing und Yahoo haben ähnlich eingeschränkte Möglichkeiten, mit den jeweiligen Suchmaschinenanbietern in Kontakt zu treten, und stehen nicht in direktem, regelmäßigem und wechselseitigem Kontakt mit dem Gatekeeper. Gleiches gilt für die Anbieter DuckDuckGo und Startpage, die sich von den marktführenden Suchmaschinen dadurch

unterscheiden und abgrenzen, dass sie die Privatsphäre ihrer Nutzer*innen schützen. Gated von Suchmaschinen haben damit das Attribut der Beziehung zum Gatekeeper nicht inne.

3.5 Salience in Form von Alternativen der Gated zum Gatekeeper

Das vierte und letzte Attribut, das den Gated Salience gegenüber dem Gatekeeper verleiht, sind Alternativen: Also die Chance der Gated, sich bei der Auswahl des Gatekeepers zwischen zwei oder mehr Möglichkeiten zu entscheiden. Dabei differenziert Barzilai-Nahon zwischen dem »legal or social right« (Barzilai-Nahon 2008: 1501), eine alternative Informationsquelle zu nutzen, und den Alternativen, die den Gated de facto zur Verfügung stehen. Gründe für einen Mangel an Alternativen gibt es mehrere: So kann der Gatekeeper ein Monopol haben; es gibt also keine Akteur*innen, Infrastrukturen oder Technologien, die einen vergleichbaren Dienst anbieten. Aber auch die Kosten oder der Aufwand, den die Nutzer*innen aufbringen müssten, um zu einem alternativen Angebot zu wechseln, können zu hoch sein (Lock-in-Effekt). Eine De-facto-Alternative ist auch dann nicht vorhanden, wenn Gated lediglich einen spezifischen Gatekeeper umgehen können, indem sie stattdessen einen anderen »within the same community« wählen, »which may well be subject to the same biases and procedures« (Barzilai-Nahon/Neumann 2005: 251). So kann ein*e Radiohörer*in beispielsweise als Alternative zu einem Radiokanal einen anderen Radiokanal wählen; dieser ist aber ebenfalls von einem vergleichbaren editorischen Gatekeeping-Prozess geprägt (vgl. ebd.).

Nutzer*innen eines bestimmten Informationsintermediärs steht also nur dann eine De-facto-Alternative zu Verfügung, wenn mindestens ein weiterer Informationsintermediär einen vergleichbaren Dienst anbietet und dabei nicht derselben Prozess- und Bias-Kultur unterliegt. Zugleich müssen Kosten und Aufwand eines Intermediärswechsels für die Nutzer*innen vertretbar sein.

Alternativen der Gated von Bibliotheken

Gated von Öffentlichen Bibliotheken haben nur in Ausnahmefällen eine De-facto-Alternative zur Verfügung. So stehen den etwa 11.014 Gemeinden in Deutschland (vgl. Rudnicka 2020) insgesamt nur knapp 5.000 Öffentliche Bibliotheken in kommunaler Trägerschaft gegenüber. Zählt man die Bibliotheken in kirchlicher Trägerschaft mit, gibt es dennoch nur in etwa 73 Prozent der Kommunen in Deutschland überhaupt eine Öffentliche Bibliothek. Dar-

über hinaus ist fraglich, inwiefern Bibliotheken in kirchlicher Trägerschaft für Gated von kommunalen Öffentlichen Bibliotheken als Gatekeeper mit einem vergleichbaren Angebot gelten können: Sie verfügen meist über ein stark eingeschränktes Angebot im Hinblick auf Öffnungszeiten, Bestand und Personal (vgl. Seefeldt 2018; vgl. Rösch/Seefeldt/Umlauf 2019).

Vor allem in größeren Städten stehen den Gated von Öffentlichen Bibliotheken auch wissenschaftliche Bibliotheken wie Hochschul-, Regional- oder Forschungsbibliotheken zur Verfügung. Diese unterscheiden sich in ihren Aufgaben sowie Zielgruppen und damit auch in den Beständen und Nutzungsbedingungen meist stark vom Angebot Öffentlicher Bibliotheken (vgl. ebd.). Damit können wissenschaftliche Bibliotheken eher als Ergänzung denn als Alternative zum Angebot Öffentlicher Bibliotheken verstanden werden.

Öffentliche Bibliotheken in anderen, z.B. benachbarten, Kommunen können ebenfalls nicht als De-facto-Alternativen zählen, da sie ähnlichen Prozessen und Bias-Kulturen unterliegen wie die Öffentliche Bibliothek der Heimatgemeinde und beispielsweise den gleichen Lektoratsdienst als Grundlage für den Bestandsaufbau nutzen (vgl. ekz Gruppe 2021). Bibliotheken sind zudem für die Nutzer*innen physischer Medien lokal fixierte Intermediäre. Einige Bibliotheken stellen Nutzer*innen nur einen Bibliotheksausweis aus, wenn sie ihren Wohnsitz in der entsprechenden Kommune haben (z.B. Stadtbibliothek Bremen 2019b). Je nach Entfernung der nächstgelegenen Kommune mit Öffentlicher Bibliothek und Lebenssituation der Nutzer*innen ist zudem der Aufwand eines Gatekeeper-Wechsels damit unterschiedlich hoch: Für Berufspendler*innen, die in einer Gemeinde arbeiten und in einer anderen Gemeinde wohnen, ist der Aufwand eines Gatekeeper-Wechsels zum Beispiel geringer als für mobilitätseingeschränkte Einwohner*innen in Gemeinden mit schlechter ÖPNV-Anbindung. Prinzipiell ist die Onleihe, also die Ausleihe elektronischer Bücher, ohne lokalen Bezug zur anbietenden Bibliothek möglich, jedoch realisieren nicht alle Bibliotheken diesen Dienst entsprechend nutzerfreundlich, also ohne persönliche Anmeldung vor Ort. Da E-Books zeitgleich nur von so vielen Nutzer*innen ausgeliehen werden können, wie die Bibliothek Lizenzen erworben hat, liegt es auch nicht zwingend im Interesse einer jeden Bibliothek, möglichst viele auswärtige Nutzer*innen zu attrahieren, wird hierdurch doch potenziell die Versorgung der Mitglieder der Kommune im Wettbewerb um attraktive Titel eingeschränkt. Da nicht alle Bibliothekskonten kostenfrei sind, ist eine beliebige Ausdehnung der Mitgliedschaften aus Perspektive der Gated nicht erstrebenswert. Auch Sortiments- und Online-Buchhandlungen können nicht als Alternativen gelten,

da die Nutzung ihrer Angebote mit deutlich höheren Kosten verbunden ist als die Nutzung von Bibliotheken.

Alternativen der Gated von Suchmaschinen

Ob Gated von Suchmaschinen eine Alternative zum Marktführer Google zur Verfügung steht, ist Gegenstand von Diskussionen: Mit dem sogenannten »*one click away*«-Argument wird angeführt, dass Nutzer*innen von Google ohne Aufwand und Kosten zu einer alternativen Suchmaschine wie beispielsweise Bing, Yahoo oder auch DuckDuckGo und Ecosia wechseln können. Ob diese Alternativen jedoch einen vergleichbaren Dienst anbieten, ist umstritten: So führt die Marktmacht von Google dazu, dass die Mehrzahl der Website-Betreiber*innen ihre Seiten im Hinblick auf die Auffindbarkeit durch den Such- und Ranking-Algorithmus von Google optimiert. Zudem hat Google die Möglichkeit, über eine immense Zahl an Nutzer*innen und deren Suchverhalten Daten zu sammeln und auszuwerten. Dadurch kann das Unternehmen seine Dienste optimieren, sodass es über einen »Innovationsvorsprung gegenüber kleineren Konkurrenten« (Hartl 2017: 118) verfügt.

So sieht das auch der Suchmaschinenanbieter Startpage, der auf seiner Website schreibt: »You can't beat Google when it comes to online search.« (Startpage o.J.) Daher bezahlt Startpage Google dafür, dessen Suchergebnisse zu nutzen – und garantiert Nutzer*innen gleichzeitig, dass keine Daten über ihre Suchanfragen und ihr Surfverhalten gesammelt und weitergegeben werden (ebd.). Damit bietet Startpage Nutzer*innen zumindest in Bezug auf den Schutz der Privatsphäre eine Alternative zum Suchmaschinenanbieter *Google*.

3.6 Vergleich der Salience der Gated von Bibliotheken und Suchmaschinen

Insgesamt wird deutlich, dass für mehrere Attribute keine eindeutige Aussage getroffen werden kann, ob Gated diese besitzen (vgl. Tab. 1, mit »?« markierte Felder). Die Gründe hierfür sind verschieden: Ob Gated ein Attribut besitzen, ist in einigen Fällen für verschiedene Gruppen von Gated unterschiedlich. So haben beispielsweise Interessenverbände in Deutschland nur in geringem Maße politische Macht gegenüber Suchmaschinenanbietern, während international bedeutsame Unternehmen als Gated in größerem Maße Einfluss auf Suchmaschinen als Gatekeeper nehmen können. Auch Gatekeeper unterscheiden sich teilweise innerhalb eines Gatekeeper-Typs so stark voneinander, dass ihre Gated einzelne Attribute in unterschiedlichem Ausmaß besitzen. Inwie-

fern Gated beispielsweise die erste Form von Macht gegenüber Bibliotheken ausüben können, unterscheidet sich danach, ob sie Bibliotheken in öffentlicher oder kirchlicher Trägerschaft gegenüberstehen. Ob Gated von Suchmaschinen eine De-facto-Alternative zum Anbieter Google haben, wird kontrovers diskutiert, sodass auch hier keine eindeutige Aussage getroffen werden kann. Ebenfalls offen bleibt, inwiefern Gated von Suchmaschinen per Gesetzgebung politische Macht gegenüber dem Gatekeeper ausüben können, da sowohl die Gültigkeit als auch der Wirkungsgrad entsprechender Regelungen in der Gesetzgebung auf EU- und Bundesebene umstritten sind. Von Fall zu Fall unterscheidet sich hingegen, ob Gated mit der zweiten und dritten Form von Macht Einfluss auf Bibliotheken nehmen können, sodass auch hier keine eindeutige Aussage möglich ist.

Für andere Attribute zeigt die Analyse aber deutlich, dass Gated diese nicht besitzen (vgl. Tab. 1, mit »x« markierte Felder): So haben Gated von Suchmaschinen keine Beziehung zum Gatekeeper, da sie keinen direkten und dauerhaften Kontakt mit den Suchmaschinenanbietern aufnehmen können. Gated von Bibliotheken fehlt hingegen das Attribut der Alternativen, da ihnen keine Gatekeeper zur Verfügung stehen, deren Dienste vergleichbar sind und die nicht der *same community* angehören.

Wieder andere Attribute können als gegeben angesehen werden (vgl. Tab. 1, mit »✓« markierte Felder): Gated von Suchmaschinen besitzen das Attribut der Informationsproduktion, da ihnen verschiedene einfach nutzbare Tools zur Verfügung stehen, um selbst Inhalte zu erstellen und über den Informationskanal des Gatekeepers zu verbreiten. Gated von Bibliotheken haben eine Beziehung zum Gatekeeper, da sie über verschiedene Kommunikationskanäle in einen direkten, dauerhaften und wechselseitigen Austausch mit den Bibliotheksmitarbeiter*innen treten können.

Insgesamt fällt auf, dass die Salience der Gated von Suchmaschinen etwas größer ist als die Salience der Gated von Bibliotheken. Die Salience der Gated hängt von der Anzahl der Attribute ab, die Gated besitzen. Gated von Suchmaschinen haben genau wie Gated von Bibliotheken jeweils ein Attribut, von dem eindeutig davon ausgegangen werden kann, dass sie es besitzen. Bei den Attributen, die die Gated eindeutig nicht besitzen, unterscheiden sich Suchmaschinen und Bibliotheken: Gated von Suchmaschinen entbehren nur ein Attribut, während Gated von Bibliotheken zwei Attribute fehlen. Für die übrigen zwei Attribute der Gated von Suchmaschinen kann keine eindeutige Aussage getroffen werden bzw. haben Gated das Attribut zum Teil inne; Gleiches gilt für das übrige Attribut der Gated von Bibliotheken.

Tabelle 1 Salience der Gated von Suchmaschinen und Bibliotheken im Vergleich.

	Suchmaschinen	Bibliotheken
Polit. Macht: 1. Form	?	?
Polit. Macht: 2. & 3. Form	?	?
Produktion von Information	✓	x
Beziehung zum Gatekeeper	x	✓
Alternativen	x	x

Insgesamt unterscheidet sich die Salience der Bibliotheksnutzer*innen also nur geringfügig von der Salience der Suchmaschinennutzer*innen. Unterschiedlich sind aber die Attribute, auf denen die Gated Salience jeweils beruht. Für die Souveränitätszustände in der Relation zwischen Rezipient*innen und Informationsintermediären lässt sich daher schlussfolgern, dass die Digitalisierung zwar Auswirkungen auf die Souveränität der Rezipient*innen hat; daraus folgt aber nicht, dass die Souveränität der Rezipient*innen bedeutend größer oder kleiner wird, sondern vielmehr, dass sie auf anderen Eigenschaften beruht.

4. Erreichtes und Desiderate

Dieser Beitrag hat untersucht, wie sich die Digitalisierung auf die Souveränität von Rezipient*innen in Relation zu Informationsintermediären auswirkt. Auf Basis der Network-Gatekeeping-Theorie wurden Kriterien entwickelt, mit denen die Rezipient*innen-Position gegenüber Informationsintermediären beschrieben werden kann. Anhand dieser Kriterien – politische Macht, Informationsproduktion, Beziehung und Alternativen – wurde die Souveränität der Nutzer*innen von Bibliotheken als traditionelle Intermediäre und von Suchmaschinen als Internet-Intermediäre beispielhaft untersucht und verglichen.

Das Ergebnis lässt sich auf unterschiedliche Weise interpretieren: So kann man einerseits zu dem Schluss kommen, dass die Befürchtungen zu Filterblasen und mangelnder Rezipient*innen-Souveränität im Kontext von Internet-Informationsintermediären unbegründet sind. Gleichermaßen kann man aber auch folgern, dass die Souveränität der Rezipient*innen in Relation zu Informationsintermediären nicht nur im Internetkontext beanstandenswert

gering ist, sondern im traditionellen Kontext ebenfalls kritisiert werden muss. Die Analyse der Nutzer*innen-Position in diesem Beitrag kann dabei als Ausgangspunkt dienen, um Strategien zu entwickeln, mit denen die Gated Salience in beiden Kontexten gefördert werden kann.

Diese Analyse unterliegt verschiedenen Limitationen. Zum einen liegen diese in der theoretischen Ausgangsbasis begründet: Laut Barzilai-Nahon ist die Salience der Gated veränderbar. Gated und Gatekeeper bewegen sich in einem »dynamic envrionment« (Barzilai-Nahon 2008: 1507), in dem sich die Rollen und Interessen der Gated und Gatekeeper stetig wandeln. Die Analyse der Gated Salience in diesem Beitrag muss daher als »snapshot of gatekeeping« (Barzilai-Nahon 2009: 34) verstanden werden, da die Salience von Gated nur für einen bestimmten Zeitpunkt in einem bestimmten Kontext beschrieben werden kann. So könnte zum Beispiel das Gesetz über digitale Dienste, das die EU-Kommission im Dezember 2020 vorgestellt hat, das Attribut der politischen Macht von Suchmaschinen-Gated stärken (vgl. Fanta 2020).

Darüber hinaus steht ein Aspekt nicht im Fokus der NGT, der aber in der öffentlichen Diskussion um Internet-Gatekeeper eine Rolle spielt: die Sammlung, Aggregation und Auswertung von Nutzer*innen-Daten durch Internet-Gatekeeper. Der Gatekeeper weiß viel über die Gated, die Gated aber wenig über den Gatekeeper, beispielsweise welche Daten über sie gesammelt werden, wer Zugriff auf diese Daten hat und wie sie genutzt werden. Es gibt also eine Informationsasymmetrie zwischen Gated und Gatekeeper (vgl. Helberger/Kleinen-von Königslöw/van der Noll 2015). Diese Problematik spielt in der NGT zwar indirekt eine Rolle, beispielsweise bei der Analyse der Attribute »Alternativen« und »Informationsproduktion«; um diesen Aspekt der Beziehung zwischen Gatekeeper und Gated zu fokussieren, könnte in zukünftigen Beiträgen aber als zusätzliches Attribut die »Informationssymmetrie« zwischen Gated und Gatekeeper analysiert werden.

Daraus ergeben sich Desiderate für weitere Analysen. Zukünftige Studien könnten die Auswahl der konkreten Gatekeeper deutlich erweitern, um einen umfassenderen Blick auf die Position der Gated von Bibliotheken und Suchmaschinen zu erhalten. In weiteren Analysen könnten auch Medienangebote wie Zeitschriften, Zeitungen und Rundfunkangebote sowie Buchhandlungen und Verlage als traditionelle Gatekeeper sowie Soziale-Netzwerk-Seiten und Nachrichtenaggregatoren als Internet-Gatekeeper in den Blick genommen werden, um einen umfassenden Vergleich der Gated Salience bei traditionellen und Internet-Gatekeepern zu ermöglichen. Nur so kann eine allgemeingültige Aussage darüber getroffen werden, wie sich die Digitalisierung auf die Souveräni-

tätszustände in der Relation zwischen Rezipienten*innen und Informationsintermediären auswirkt.

Formales Ziel des Beitrags war es, an das eingangs diagnostizierte Desiderat anzuknüpfen: Dieses besteht darin, dass der Diskurs um die Veränderungseffekte durch Digitalisierung und die damit verbundenen Chancen und Risiken eine enorme Bestimmungsunschärfe aufweist. Ohne Beschäftigung mit den Differenzen zwischen den Ausprägungen und Realisierungsformen eines Systems (hier: öffentliche Kommunikation) erzeugen diese Diskurse keinen erkenntnistheoretischen Mehrwert. Ausgangspunkt ist dabei, dass Transformation ein evolutionärer und kein disruptiver Prozess ist und verschiedene Ausprägungen sehr lange Zeit parallel bestehen. Wir haben gezeigt, dass eine systematische Analyse mithilfe von theoriegeleiteten Kriterien möglich – wenngleich empirisch herausfordernd – ist.

Was lässt sich abschließend also über »digitale Souveränität« in der öffentlichen Kommunikation sagen? »Digitale Souveränität« ist relational: Sie kann nur für eine bestimmte Beziehung in einem bestimmten Kontext und zu einem bestimmten Zeitpunkt beschrieben werden. In der öffentlichen Kommunikation spielen für die digitale Souveränität vier Relationen eine Rolle: die Beziehung zwischen Rezipient*in und Organisation/Informationsintermediären, überindividuellen und übergeordneten Instanzen sowie die Beziehung zwischen Organisationen/Informationsintermediären und übergeordneten Instanzen. Um eine Aussage darüber treffen zu können, wie sich die Digitalisierung auf die Souveränität in einzelnen Relationen auswirkt, muss nicht nur der Souveränitätszustand im Internetkontext, sondern auch in vergleichbaren traditionellen Kontexten kriteriengeleitet und empirisch analysiert werden. Nur durch den Vergleich der Souveränitätszustände in beiden Kontexten kann eine belastbare Aussage über die Veränderungseffekte getroffen werden, die die Digitalisierung bewirkt.

Literaturverzeichnis

Andree, Martin/Thomsen, Timo (2020): Atlas der digitalen Welt, Frankfurt a.M.: Campus.

Bagdikian, Ben H. (1971): The information machines: Their impact on men and the media, New York: Harper & Row.

Barzilai-Nahon, Karine (2008): »Toward a theory of network gatekeeping: A framework for exploring information control«, in: Journal of the American Society for Information Science and Technology 59 (9), S. 1493–1512.

Barzilai-Nahon, Karine (2009): »Gatekeeping: A critical review (PREPRINT)«, in: Annual Review of Information Science and Technology 43 (1), S. 1–79.

Barzilai-Nahon, Karine/Neumann, Seev (2005): »Gatekeeping in networks: A metatheoretical framework for exploring information control: Pre-print paper for presentation in the JAIS Sponsored Theory Development Workshop«. Online unter: https://bit.ly/3inM6H8, abgerufen am 28.01.2020.

Baur, Nina/Blasius, Jörg (2014): Handbuch Methoden der empirischen Sozialforschung, Wiesbaden: Springer VS.

Behrens, Jörg (2017): Book on demand: Auswirkungen auf den deutschen Buchmarkt. Dissertation an der Universität Erfurt, Norderstedt: Books on Demand.

Bender, Justus (2021): »So schadet uns das Internet«, in: Frankfurter Allgemeine Zeitung vom 02.02.2021. Onliner unter: https://bit.ly/3iibgHa, abgerufen am 27.09.2021.

Bibliotheksportal (2017): Kommunikationsgestaltung. Online unter: https://bit.ly/2ZPiNXD, abgerufen am 03.06.2020.

Bibliotheksurteile (2020). Website der HAW Hamburg. Online unter: https://www.bibliotheksurteile.de, abgerufen am 22.05.2020.

Boehme-Neßler, Volker (2019): »Big Data: Die Digitalisierung höhlt unsere Demokratie aus«, in: Die Welt vom 10.01.2019. Online unter: https://bit.ly/3F8NGGi, abgerufen am 27.09.2021.

Börsenverein des Deutschen Buchhandels e.V. (2020): Mediendossier Buchhandel Stationäres Sortiment. Online unter: https://bit.ly/3kVuAM4, abgerufen am 01.10.2020.

Bozdag, Engin (2013): »Bias in algorithmic filtering and personalization«, in: Ethics and Information Technology 15 (3), S. 209–227.

Brosius, Hans-Bernd (2016): »Warum Kommunikation im Internet öffentlich ist«, in: Publizistik 61 (4), S. 363–372.

Dammann, Finn/Glasze, Georg (2022): »›Wir müssen als Deutsche und Europäer unsere digitale Souveränität zurückgewinnen!‹ Historische Rekonstruktion und internationale Kontextualisierung der Diskurse einer ›digitalen Souveränitiät‹ in Deutschland«, in: Georg Glasze/Eva Odzuck/Ronald Staples (Hg.), Digitale Souveränität. Diskurse, Praktiken und Voraussetzungen »individueller« und »staatlicher Souveränität« im digitalen Zeitalter, Bielefeld: transcript, S. 29–60.

Datenschutz.org (2020): Recht auf Vergessen: Wie viel dürfen Suchmaschinenbetreiber speichern? Online unter: https://www.datenschutz.org/recht-auf-vergessen/, abgerufen am 22.10.2020.

DeIuliis, David (2015): »Gatekeeping Theory from Social Fields to Social Networks«, in: Communication Research Trends 34 (1), S. 4–23.

Deutsche Bibliotheksstatistik (2021): Variable Auswertung. Online unter: https://www.bibliotheksstatistik.de/vaAttribute, abgerufen am 26.02.2021.

Deutscher Bundestag – Wissenschaftliche Dienste (Hg.) (2008): Bibliotheksgesetzgebung in Deutschland: Stand und Perspektiven. Ausarbeitung. Online unter: https://bit.ly/30tB1b4, abgerufen am 24.09.2021.

Die Medienanstalten (2020): Mediengewichtungsstudie 2020–1 LOKAL: Gewichtungsstudie zur Relevanz der Medien für die lokale Meinungsbildung in Deutschland. Online unter: https://www.die-medienanstalten.de/themen/forschung/mediengewichtungsstudie, abgerufen am 02.03.2021.

Dogruel, Leyla/Stark, Birgit/Facciorusso, Dominique/Liesem, Kerstin (2020): »Die Regulierung von Algorithmen aus Expertensicht: Transparenz und Diskriminierungsfreiheit – zur Vielfaltssicherung im neuen Medienstaatsvertrag«, in: Media Perspektiven 3, S. 139–148.

Dörr, Dieter/Schuster, Simon (2014): »Suchmaschinen im Spannungsfeld zwischen Nutzung und Regulierung. Rechtliche Bestandsaufnahme und Grundstrukturen einer Neuregelung«, in: Birgit Stark/Dieter Dörr/Stefan Aufenanger (Hg.), Die Googleisierung der Informationssuche: Suchmaschinen zwischen Nutzung und Regulierung (= Media Convergence/Medienkonvergenz, Band 10), Berlin: de Gruyter.

ekz.bibliotheksservice GmbH (2021): »Lektoratsdienste 2021«. Online unter: https://bit.ly/3xSI8gC, abgerufen am 24.09.2021.

ekz Gruppe (2021): Teilnehmende Bibliotheken. Online unter: https://bit.ly/39Sef4m, abgerufen am 15.02.2021.

Emonts, Benjamin (2019): »›Google hat sich schön aus der Sache rausgemogelt‹«, in: Süddeutsche Zeitung vom 28.08.2019. Online unter: https://bit.ly/3m7j3bM, abgerufen am 14.05.2020.

Evangelische Landeskirche in Baden (2007): Ältestenkreis & Kirchengemeinderat. Online unter: https://bit.ly/39QlQAn, abgerufen am 22.05.2020.

Fanta, Alexander (2020) »Algorithmen sollen nicht willkürlich entscheiden dürfen«, in: Netzpolitik.org vom 28.09.2020. Online unter: https://bit.ly/2YhR1Cm, abgerufen am 06.11.2020.

Gerhards, Jürgen/Neidhardt, Friedhelm (1990): Strukturen und Funktionen moderner Öffentlichkeit: Fragestellungen und Ansätze, Berlin: WZB.

Glasze, Georg/Odzuck, Eva/Staples, Ronald (2022): »Einleitung: Digitalisierung als Herausforderung – ›Souveränität‹ als Antwort? Konzeptionelle Hintergründe der Forderungen nach ›digitaler Souveränität‹«, in: Georg Glasze/Eva Odzuck/Ronald Staples (Hg.), Digitale Souveränität. Diskurse, Praktiken und Voraussetzungen »individueller« und »staatlicher Souveränität« im digitalen Zeitalter, Bielefeld: transcript, S. 7–28.

Google (2021a): Wie können wir Ihnen helfen? Online unter: https://about.google/contact-google/, abgerufen am 04.03.2021.

Google (2021b): Unsere Standorte. Online unter: https://bit.ly/3kV9ai7, abgerufen am 04.03.2021.

Google (2021c): The Keyword: Blog. Online unter: https://www.blog.google/ abgerufen am 04.03.2021.

Hagenhoff, Svenja (2020): »Digitale Souveränität«: Kontextualisierung des Phänomens in der Domäne der medial vermittelten öffentlichen Kommunikation unter besonderer Berücksichtigung von Reader Analytics (= Erlanger Beiträge zur Medienwirtschaft, Band 14), Institut für Buchwissenschaft, Friedrich-Alexander-Universität Erlangen-Nürnberg. Online unter: urn://nbn:de:bvb:29-opus4-150157, abgerufen am 25.06.2022.

Hartl, Korbinian (2017): Suchmaschinen, Algorithmen und Meinungsmacht. Eine verfassungs- und einfachrechtliche Betrachtung, Wiesbaden: Springer VS.

Heine, Franziska (2011): »Demokratie auf Augenhöhe«, in: taz vom 13.07.2011. Online unter: https://bit.ly/39PAFmX, abgerufen am 27.09.2021.

Helberger, Natali/Kleinen-von Königslöw, Katharina/van der Noll, Rob (2015): »Regulating the new information intermediaries as gatekeepers of information diversity«, in: info 17 (6), S. 50–71.

Hindelang, Steffen (2019): Freiheit und Kommunikation. Zur verfassungsrechtlichen Sicherung kommunikativer Selbstbestimmung in einer vernetzten Gesellschaft, Berlin/Heidelberg: Springer.

Initiative Urheberrecht (2017): Neun Bildverbände kritisieren neue Google Bildersuche. Online unter: https://bit.ly/3F4vcHc vom 28.02.2017, abgerufen am 21.10.2020.

Initiative Urheberrecht (2018): Nach Getty-Deal: Google ändert seine Bildersuche. Online unter: https://bit.ly/30jp5sD vom 19.02.2018, abgerufen am 03.03.2021.

Jarren, Otfried (2008): »Massenmedien als Intermediäre. Zur anhaltenden Relevanz der Massenmedien für die öffentliche Kommunikation«, in: Medien

& Kommunikationswissenschaft 56 (3–4), S. 329–346, https://doi.org/10.5771/1615-634x-2008-3-4-329.

Jürgens, Pascal/Stark, Birgit/Magin, Melanie (2014): »Gefangen in der Filter Bubble? Search Engine Bias und Personalisierungsprozesse bei Suchmaschinen«, in: Birgit Stark/Dieter Dörr/Stefan Aufenanger (Hg.), Die Googleisierung der Informationssuche: Suchmaschinen zwischen Nutzung und Regulierung, Berlin: de Gruyter, S. 98–135.

Keddi, Laura (2015): Fragen an Google? Wir zeigen, wo Sie Antworten bekommen. Online unter: https://bit.ly/3ihiZoI, abgerufen am 28.05.202).

Kelsey, Todd (2017): Introduction to Search Engine Optimization: A Guide for Absolute Beginners, Berkeley: Apress.

Klymenko, Iryna V. (2019): Semantiken des Wandels: Zur Konstruktion von Veränderbarkeit in der Moderne, Bielefeld: transcript.

Landeszentrale für politische Bildung BW (2020): Digitale Demokratie: E-Government, E-Partizipation, Online-Wahlen. Online unter: https://www.lpb-bw.de/demokratie-digital, abgerufen am 27.09.2021.

Leavitt, Alexander C. (2016): Upvoting the news: Breaking news aggregation, crowd collaboration, and algorithm-driven attention on reddit.com, Dissertation an der University of Southern California, Annenberg School for Communication. Online unter: https://bit.ly/3Okmg4t, abgerufen am 06.02.2020.

Leutheusser-Schnarrenberger, Sabine (2018): »Das Recht auf Vergessenwerden«, in: Christian Bär/Thomas Grädler/Robert Mayr (Hg.), Digitalisierung im Spannungsfeld von Politik, Wirtschaft, Wissenschaft und Recht. 1. Band: Politik und Wirtschaft, Berlin: Springer, S. 231–238.

Lewandowski, Dirk (2018): Suchmaschinen verstehen, Berlin/Heidelberg: Springer.

Leyrer, Katharina (2018): Selektion und Bias in traditionellen und Internet-Informationsintermediären. Forschungsstand (= Erlanger Beiträge zur Medienwirtschaft, Band 10). Philosophische Fakultät und Fachbereich Theologie, Friedrich-Alexander-Universität Erlangen-Nürnberg. Online unter: urn:nbn:de:bvb:29-opus4-102405.

Liesem, Kerstin (2020): »Pionierleistung mit Signalwirkung: Die regulative Einhegung von Medienintermediären im Medienstaatsvertrag«, in: AfP 51 (4), S. 277–283.

Manjoo, Farhad (2016): »Tech's ›Frightful 5‹ will dominate digital life for foreseeable future«, in: The New York Times vom 20.01.2016. Online unter: https://nyti.ms/3zTy1H5, abgerufen am 24.09.2021.

Matthes, Marie-Charlotte (2018): »Google: MitarbeiterInnen gegen zensierte Suchmaschine für den chinesischen Markt«, in: netzpolitik.org vom 18.12.2018. Online unter: https://bit.ly/39OxVpT/, abgerufen am 21.10.2020.

Medienstaatsvertrag (MStV) vom 14./28. April 2020. Online unter: https://www.gesetze-bayern.de/Content/Document/MStV/true, abgerufen am 02.06.2021.

Milker, Jens (2019): »Einleitung«, in: Jens Milker (Hg.), Die Umsetzung des »Rechts auf Vergessenwerden« im deutschen Recht, Wiesbaden: Springer Fachmedien, S. 1–15.

Nissenbaum, Helen F. (2010): Privacy in context: Technology, policy, and the integrity of social life (= Stanford Law Books), Stanford: Stanford University Press.

Pariser, Eli (2011): The filter bubble: What the Internet is hiding from you, London: Viking.

Przyborski, Aglaja/Wohlrab-Sahr, Monika (2014): Qualitative Sozialforschung: Ein Arbeitsbuch, München: Oldenbourg.

Rösch, Hermann/Seefeldt, Jürgen/Umlauf, Konrad (2019): Bibliotheken und Informationsgesellschaft in Deutschland: Eine Einführung, Wiesbaden: Harrassowitz.

Rudnicka, J. (2020): »Gemeinden in Deutschland nach Gemeindegrößenklassen 2018«, in: Statista. Online unter: https://bit.ly/3zVRTte, abgerufen am 26.06.2020.

Sahner, Simon (2021): »Der Stoff aus dem Meme-Träume sind – Deepdive in die digitale Kultur«, in: 54books vom 16.09.2021. Online unter: https://bit.ly/3CZJ9Ey, abgerufen am 21.09.2021.

Samuelis, Theresa (2020): Das Internet hat demokratisches Potenzial. Ein Interview mit Ingrid Brodnig, Bundeszentrale für politische Bildung vom 07.05.2020. Online unter: https://bit.ly/3m5XtUU, abgerufen am 27.09.2021.

Schmid, Axel (2018): »Medien und Medienkommunikation«, in: Dagmar Hoffman/Rainer Winter (Hg.), Mediensoziologie. Handbuch für Wissenschaft und Studium, Baden-Baden: Nomos, S. 39–56.

Schweiger, Wolfgang (2017): Der (des)informierte Bürger im Netz, Wiesbaden: Springer Fachmedien.

Schwemer-Martienßen, Hella/Studt, Michael (2021): Bibliothekskonzept Bücherhallen Hamburg 2021, Bücherhallen Hamburg. Online unter: h

ttps://www.buecherhallen.de/bibliothekskonzept.html, abgerufen am 14.04.2021.

Scott, W. Richard (2009): Institutions and organizations: Ideas and interests, Los Angeles: Sage.

Seefeldt, Jürgen (2018): Öffentliche Bibliotheken und ihre Rolle für Bildung und Kultur in ländlichen Räumen, Kulturelle Bildung Online. Online unter: https://bit.ly/3CZjsDT, abgerufen am 27.10.2020.

Seemann, Michael (2014): Das neue Spiel: Strategien für die Welt nach dem digitalen Kontrollverlust, Freiburg: Orange Press.

Stadtbibliothek Bremen (2019a): Besucherumfrage 2019. Online unter: https://www.stabi-hb.de/download, abgerufen am 24.09.2021.

Stadtbibliothek Bremen (2019b): Online-Anmeldung in der Stadtbibliothek Bremen. Online unter: https://bit.ly/39OTJl6, abgerufen am 14.04.2021.

Stalder, Felix (2021): Kultur der Digitalität, Berlin: Suhrkamp.

Stark, Birgit/Magin, Melanie/Jürgens, Pascal (2021) »Maßlos überschätzt. Ein Überblick über theoretische Annahmen und empirische Befunde zu Filterblasen und Echokammern«, in: Mark Eisenegger/Marlis Prinzing/Patrik Ettinger/Roger Blum (Hg.), Digitaler Strukturwandel der Öffentlichkeit, Wiesbaden: Springer VS, S. 303–321.

Startpage (o.J.): So machen wir die Websuche privat. Online unter: https://startpage.com/, abgerufen am 26.06.2020.

StatCounter (2021): Desktop Search Engine Market Share Worldwide: Nov 2020. Online unter: https://bit.ly/39RZWwQ, abgerufen am 12.04.2021.

Truscheit, Karin (2019): »Prozess abgesagt: ›Google ist eingeknickt‹«, in: Frankfurter Allgemeine Zeitung vom 28.08.2019. Online unter: https://bit.ly/3mbekGa, abgerufen am 13.05.2020.

Truschkat, Inga/Kaiser-Belz, Manuela/Reinartz, Vera (2007): »Grounded Theory Methodologie in Qualifikationsarbeiten: zwischen Programmatik und Forschungspraxis – am Beispiel des Theoretical Samplings«, in: Historical Social Research, Supplement 19, S. 232–257.

Umlauf, Konrad (2015): »Bibliotheken als Organisationen zur Bereitstellung von Lektüre«, in: Ursula Rautenberg/Ute Schneider (Hg.), Lesen: Ein interdisziplinäres Handbuch, Berlin/Boston: de Gruyter.

Unkel, Julian (2019): Informationsselektion mit Suchmaschinen: Wahrnehmung und Auswahl von Suchresultaten, Baden-Baden: Nomos.

West, Sarah Myers (2017): »Raging against the machine: Network gatekeeping and collective action on social media platforms«, in: Media and Communication 5 (3), S. 28.

Zawidzki, Winfried/Gahlau, Christoph (2018): Die wichtigsten Fragen zur Pfarrgemeinderatswahl, Erzbistum Bamberg. Online unter: https://sicherheit.pfarrbriefservice.de/pbs/dcms/sites/pgr/bayern/pfarrgemeinderat/index.html, abgerufen am 22.05.2020.

Zimmer, Michael (2008): »Privacy on planet Google: Using the theory of ›Contextual Integrity‹ to clarify the privacy threats of Google's quest for the perfect search engine«, in: Journal of Business & Technology Law 3, S. 109–126.

Der relationale Charakter von »digitaler Souveränität«

Zum Umgang mit dem »Autonomie/Heteronomie«-Dilemma in sich transformierenden Arbeitswelten

Stefan Sauer, Ronald Staples, Vincent Steinbach

Abstract *Die Sphäre der Arbeit wird durch ein paradoxes Kräftespiel von Autonomie und Kontrolle geprägt. Spätestens seit Erwerbsarbeit paradigmatisch für Arbeit an sich steht, müssen alle konkreten wie institutionalisierten Arbeitsbeziehungen mit dem Problem umgehen, wie Arbeitskraft in Arbeit transformiert wird. Die Frage nach Souveränität von Beschäftigten verknüpfte sich bislang eher mit dem Durchsetzen von (kollektiven) Interessen, objektiviert in Tarifverträgen. In der modernen Wissensarbeit werden dem Subjekt hohe Freiheitsgrade zugestanden und auch von dessen Seite aus erwartet, was sich unter dem Schlagwort »Selbstorganisation« subsummieren lässt. Tatsächliche Souveränitätsgewinne als Gestaltungschancen im Arbeitshandeln setzen komplexe Rahmenbedingungen voraus: Vertrauen und gelingende Anerkennungsverhältnisse, (digitale) Kommunikationskompetenzen. Arbeitsorganisation stellt insofern ein fragiles Gebilde dar, das durch Ansprüche an »digitale Souveränität« der Beschäftigten herausgefordert wird. Der Text rekonstruiert, wie Arbeit zwischen Autonomie und Kontrolle changiert, und argumentiert, dass sie sich dabei auf gelingende Anerkennungsverhältnisse und gewährtes Vertrauen verlassen muss. Ausgehend von der Beschreibung selbstorganisierten Arbeitens wird aufgezeigt, dass »digitale Souveränität« eine produktive Analysekategorie moderner Arbeitsbeziehungen sein kann, wenn man sie hinsichtlich möglicher Handlungsspielräume als eine relationale Kategorie reformuliert, mit der sich Arbeitssituationen bezeichnen lassen, in der sich Beschäftigte situativ Souveränität erwirtschaften im Sinne von Gestaltungsoptionen – und sie nicht als (vertraglich realisierte, normative) Eigenschaft denkt.*

Die möglichen gesellschaftlichen Folgen von digitaler Transformation lassen sich in den klassischen Modernisierungstheorien finden. Demnach wird

angenommen, dass digitale Transformation die ungleiche Verteilung von Produktionsressourcen reproduziert und festigt (Marx), Rationalisierung radikalisiert (Weber) oder die funktionale Differenzierung weiter ausbuchstabiert wird (Durkheim). In der ersten Überlegung zur Verbindung der Klassiker der Modernisierung mit der digitalen Transformation scheinen sich diese Makroentwicklungen fortzusetzen: Die Leitunternehmen eines digitalen Kapitalismus erweisen sich durch ein verändertes Produktionsmodell als äußerst rentabel und entziehen sich tendenziell den Regulationsformen, die auf das Produktionsmodell der industriellen Moderne abgestimmt sind (vgl. Nachtwey/Staab 2020). Durch das Abschöpfen und Bearbeiten des stetig wachsenden Stroms von Daten sollen gleichzeitig eine objektivere Beobachtung und Interpretation von Welt sowie ihren Bedürfnissen machbar sein. Darüber hinaus schafft die digitale Transformation allein durch die Verdatung der analogen Welt weitere, spezielle Bereiche der Lebenswelt, die sich v.a. durch Spezialwissen im Umgang mit der Schnittstellenproblematik (vgl. Nassehi 2019: 204) zwischen analoger und digitaler Welt beschäftigen müssen.

Für die konkrete Gestaltung von Erwerbsarbeit zeigen sich prominente, gegensätzliche Strömungen: Wo beispielsweise die Anhänger*innen der New-Work-Bewegung (vgl. Bergmann 2019) in der digitalen Transformation zumindest die Chance zu digitaler Kreativität und Abschaffung der Lohnarbeit sehen und die Transformation als Freiheitstreiberin adressieren, assoziieren überwachte Arbeiter*innen auf dem *shop floor* in globalen Logistikunternehmen wohl weniger Befreiungsgedanken mit der digitalen Transformation (vgl. Schaupp 2021).

Sowohl die Rahmenbedingungen von Arbeit als auch ihre Inhalte und die zur Verfügung stehenden Werkzeuge verändern sich im Verhältnis zur Hochzeit der industriellen Moderne rasant. Die soeben genannten gegensätzlichen Strömungen in der Erwerbsarbeit gehen mit unterschiedlichen Erwartungen bzw. Möglichkeiten, individuelle Entscheidungen zu treffen, einher. Die Unsicherheit, was digitale Transformation für die Zukunftsfähigkeit von Berufen und konkreten Arbeitsverhältnissen bedeutet, ist groß, wobei als prominentes Resilienzkriterium wie künftige Kompetenz, Agilität (als besonderer Flexibilitätstyp) im Diskurs zirkuliert (vgl. Bauer/Hofmann 2018). Diese Flexibilitätserwartungen zeigen bereits an, dass die Beziehungen in der Arbeitswelt dynamischer werden und bürokratisch-hierarchische Strukturen ihre Orientierungsfunktion in der Gestaltung von Arbeitsverhältnissen verlieren. Daher stellt sich die Frage, wie in Arbeitsverhältnissen souverän gehandelt werden kann. Oder anders gefragt: Wer ist das Subjekt des

Handelns in der Erwerbsarbeit? Die individuellen Beschäftigten, das jeweilige Team, die Abteilung oder Arbeitgebenden in Gestalt einer Organisation? Die institutionalisierten und rechtlich objektivierten Arbeitsbeziehungen von unselbstständig Beschäftigten scheinen hier gegen Erstere zu sprechen[1]. Bei Selbstständigen bzw. Unternehmer*innen sind die Verhältnisse ein wenig anders gelagert. Sie sind zwar nicht direkt von einem*einer Arbeitgebenden abhängig, allerdings sind sie sehr viel direkter als Arbeitnehmer*innen von ihrer Position auf den Märkten abhängig. Die Produktion von Gütern aller Art hängt zudem immer mehr von Wissen ab, welches in der Regel auch nicht von einer Organisation (oder einem Unternehmen) allein produziert wird, sondern netzwerkartig entsteht (vgl. Windeler 2001). Die Wertschöpfungsnetzwerke spätkapitalistischer Wirtschaft sind zudem keine geschlossenen Systeme einzelner Akteure, sondern hochkomplexe und überaus fragile offene Systeme (ausführlich hierzu Castells 2017: 239f.). Der Preis für hocheffiziente Industrie- und Dienstleistungsproduktion ist ihre Irritationsanfälligkeit, weil einzelne Systeme nur mehr schwerlich identifizier- und damit isolierbar sind. Welches Unternehmen hat beispielsweise vorausschauende Strategien für eine weltweite Pandemie entwickelt?

Für sie bzw. für Organisationen im Allgemeinen scheint es zunehmend der Fall zu sein, dass »digitale Souveränität« informierten und reflektierten Risikoabwägungen bzw. -entscheidungen in immer kleiner werdenden Zeitintervallen entspricht. Der schneller werdende Takt der Entscheidungen ist dabei an die steigende Rechen- bzw. Übertragungskapazität der digitalen Infrastruktur gekoppelt. Wer dabei den Überblick über die Daten bewahrt, hat Wettbewerbsvorteile, nimmt man doch auf Basis von Daten eine sachliche Zukunft vorweg, die mit einer quantifizierbaren Wahrscheinlichkeit eintritt, und wird als Organisation handlungsfähig (s. Esposito 2014). Algorithmen formalisieren Entscheidungen auf Basis von Beobachtungen (Daten) und geben Handlungsanweisungen (Output), die je nach Wahrscheinlichkeit im Rechenmodell des Algorithmus mehr oder weniger belastbar sind (vgl. MacKenzie 2019). Das Verfügen über digitale Infrastruktur ermöglicht es Organisationen, Handlungsoptionen in globalen Wertschöpfungsnetzwerken zu generieren.

1 Neben der Verrechtlichung bringt die Institutionalisierung von Arbeitsbeziehungen auch sehr spezifische Erwartungserwartungen hervor, die man über das Konzept des »psychologischen Vertrages« beschreiben kann (Rousseau 1989). Abhängigkeitsverhältnisse sind dabei nicht nur entlang der offiziellen Hierarchie zu finden, sondern auch in umgekehrter Richtung, bekannt als *Unterwachung*.

Dies kann als eine notwendige Voraussetzung für die Souveränität von Organisationen gesehen werden, gleichwohl die Frage nach der Datenhoheit damit noch nicht geklärt ist[2]. Souveränität kann so gesehen keine Zustandszuschreibung sein, sondern ist vielmehr ein Verhältnis, das die Differenz von Handlungsmöglichkeiten und -restriktionen wiedergibt und (auch) zeitlich instabil ist[3]. In der Arbeitssoziologie ist in diesem Zusammenhang das Spannungsfeld von Autonomie/Heteronomie die eingeführte Begrifflichkeit. In ihm entfaltet sich das Problem, dass die Arbeitswelt i.d.R. durch Herrschaftsverhältnisse strukturiert ist. Heteronomie bezeichnet dabei Ordnung durch Institutionalisierung, die der einzelnen Person als gegeben erscheint (vgl. Wolf 1999: 107). Autonomie versteht Wolff mit Blick auf Castoriadis als eine Selbstgesetzlichkeit, deren Voraussetzung nicht radikale Individualisierung ist, sondern Gleichheit aller (vgl. ebd.: 111).

Häufig in einer Marx'schen Traditionslinie stehend, untersucht die Arbeitssoziologie Arbeitsverhältnisse eher aus Perspektive der Beschäftigten, die als Subjekte von Arbeit angesehen werden und spezifischen heteronomen Verhältnissen unterworfen sind, als aus jener der Organisationen. Diese Verhältnisse setzen sich zusammen aus den institutionellen Rahmenbedingungen und dem je konkreten Arbeitsverhältnis in einem Betrieb[4]. Aus Beschäftigtenperspektive scheint (digitale) Souveränität eine uneindeutige Größe zu sein: Als Mitglied einer Organisation produziert man Daten sowohl intentional als auch als Nebenfolge des eigenen Handelns. Gleichzeitig ist man den Regeln und Gepflogenheiten der Organisation und ihrer Kultur qua Arbeitsvertrag unterworfen. Die Autonomie bzw. Heteronomie von Arbeitnehmer*innen in Betrieben lässt sich also auch daran abschätzen, zu welchem Grad sie eine informierte, reflektierte Entscheidung treffen können. Oder

2 Benutzt ein Unternehmen beispielsweise für seine Dateninfrastruktur Angebote von Amazon, kann man dann noch von »digitaler Souveränität« sprechen? Spannend in diesem Zusammenhang ist der Beitrag von Albrecht Fritzsche (2022) in diesem Band, der »digitale Souveränität« selbst als verwertbare Ressource reformuliert.

3 Exemplarisch zeigt sich das im Hochfrequenzhandel der Finanzindustrie. Dieser ist sowohl von dem Verfügen über die Marktkomplexität bearbeitender Algorithmen als auch von der geographischen Nähe zu leistungsfähigen Internetknoten abhängig (vgl. MacKenzie 2018).

4 Unter dem Titel *Humanisierung der Arbeit* wurde ein breit angelegtes Forschungsprogramm in der BRD aufgelegt, das diese Verhältnisse unter den Vorzeichen der Automatisierung stärker in den Blick nehmen sollte. Damit verbunden hat sich auch eine emanzipatorische Hoffnung an das Erwerbsarbeitssubjekt (s. hierzu Matthöfer 1980).

übersetzt in die Sprache digitaler Infrastruktur: zu welchem Grad sie Zugang zu Beobachtungen in Form von Daten haben und diese in ihren Entscheidungen verarbeiten können sowie zu welchem Grad andere (bspw. der*die Arbeitgebende) Zugang zu Daten über sie und ihr Handeln haben und diese verarbeitet werden. Historisch gesehen werden spätestens seit der Systematisierung von Arbeitsorganisation (vgl. Taylor 1998) auch Daten zur Arbeit erhoben und zur Kontrolle bzw. Steuerung von Beschäftigten verwandt. Eine Zuschreibung an das Handeln von Beschäftigten als ein souveränes bewegt sich also zwischen den Polen absoluter Autonomie und Heteronomie und nicht jenseits davon. Die Digitalisierung von Arbeit wäre dann eine neue Dimension, die sowohl Souveränitätsgewinne als auch deutliche Verluste mit sich bringen kann. Die Fragen, wer über was Bescheid weiß und wer bis zu welchem Grad durch- und ausgeleuchtet wird, ist abhängig von bewussten Entscheidungen und strukturellen wie kulturellen organisationalen Settings – und damit nicht zuletzt auch eine Frage von Anerkennung und Missachtung von Beschäftigten und ihren Leistungen (vgl. Honneth 1994, 2008).

Das Gewähren von Anerkennung kann allerdings als eine Form von Souveränität verstanden werden, die daraus entsteht, dass die vielfältigen Abhängigkeitsverhältnisse als solche reflektiert und zum Ausgangspunkt für weiteres Handeln gemacht werden. »Souveränität« wäre dann zu verstehen als eine konstitutiv relationale Kategorie, die eben nicht zwei voneinander unabhängige (autonome) Subjekte voraussetzt, sondern die geschichteten sozialen Beziehungen in Arbeitsverhältnissen als Ausgangspunkt setzt. Eine notwendige Randbedingung, um Arbeitsbeziehungen auf der Basis wechselseitiger Anerkennung gestalten zu können, scheint uns darüber hinaus Vertrauen zu sein. Dieses ist selbst keine Selbstverständlichkeit, wenn man sich beispielsweise vor Augen führt, mit welcher Zähigkeit die Debatte um Homeoffice geführt wird und um die Angst, dass Beschäftigte nichts mehr leisten, sobald sie unbeaufsichtigt sind. Gleichzeitig stellt die Arbeitswelt hohe Erwartungen an das Arbeitssubjekt; leistungsbereit, lernwillig, sozial kompetent, resilient, flexibel und noch einiges mehr soll es sein, dies kulminiert im Konzept der selbstorganisierten Arbeit. Die hohen Anforderungen an Selbstorganisation stehen somit im Widerstreit mit häufig auf Misstrauen basierenden Unternehmenspolitiken. Digitalisierung ist in dieser Konstellation kein disruptiver Gamechanger, sondern Katalysator arbeitsweltlicher Trends, die zwischen Autonomie und Heteronomie pendeln. Dazu tragen im Besonderen die höheren Anforderungen an Kommunikation in ihren digital mediatisierten Formen bei (vgl. Klemm/Staples 2015). Hierüber verschieben sich möglicherweise auch die be-

trieblichen Machtverhältnisse und es entstehen neue Unsicherheitszonen, die von den Akteur*innen besetzt werden müssen (vgl. Crozier/Friedberg 1979). Digitalisierung wirkt als Verstärker, der die konstitutiven Grundprobleme der modernen Arbeitswelt sichtbarer macht, berufliche Optionen beeinflusst und die Frage nach dem gesellschaftlichen Integrationspotenzial von Arbeit mit neuer Schärfe stellt. Fasst man diese Bedingungen, die die Arbeitsverhältnisse konturieren, zusammen – Autonomie/Heteronomie als Ausdruck der Strukturierung von Machtverhältnissen sowie Anerkennung und Vertrauen als Eckpfeiler von Selbstorganisation –, dann wird deutlich, dass »Souveränität« keine Zustandsbeschreibung sein kann, sondern eine relationale Größe darstellt, die trotz dieser widersprüchlichen Rahmenbedingungen beobachtbar ist. Beschäftigungsverhältnisse, die als »digital souverän« bezeichnet werden können, müssen daher eine Reihe von Strukturbedingungen erfüllen und diese in der Arbeitspraxis produktiv machen. »Digitale Souveränität« wird daher als »relationale Souveränität« bezeichnet, und die folgenden Abschnitte problematisieren die institutionellen wie situativen Bedingungen, unter denen sie in Beschäftigungsverhältnissen sichtbar werden kann.

Um die komplexe Gemengelage zu rekonstruieren, gehen wir folgendermaßen vor: Wir skizzieren in einem ersten Schritt die grundsätzliche Paradoxie von Selbstorganisation im betrieblichen Kontext (s. Kap. 1.). Erwerbsarbeit ist nicht nur einer der Dreh- und Angelpunkte von gesellschaftlicher Integration, sondern auch die zentrale Sphäre für Anerkennung, insbesondere Wertschätzung. Daher erläutern wir das Konzept der Anerkennungsverhältnisse nach Axel Honneth und diskutieren, wie institutionalisierte Anerkennungsverhältnisse durch selbstorganisierte Arbeit in digitalisiertem Kontext unter Druck geraten (s. Kap. 2.). Im folgenden Schritt diskutieren wir die Rolle von Digitalisierung als potenziell polarisierende Kraft von Selbstorganisation und Anerkennung im betrieblichen Kontext entlang der Frage, wie Digitalisierung zur »relationalen Souveränität« von Arbeitsverhältnissen beitragen kann und welche Implikationen dies in der betrieblichen Praxis aufweist. Wir problematisieren dabei das Mehr an Kommunikation, welches Digitalisierung mit sich bringt, weil es im Arbeitskontext offenbar auch Dinge gibt (situiertes Wissen, Erfahrungswissen, Anerkennung/Wertschätzung, Vertrauen), die sich schlecht oder gar nicht digital substituieren lassen (s. Kap. 3.). Wenn diese Annahme zutrifft, dann ist digitale Kommunikation darauf angewiesen, dass Vertrauen und Anerkennungsverhältnisse bereits im Betrieb institutionalisiert sind oder sich zusätzliche kommunikative Praktiken etablieren, die funktional Vertrauen repräsentieren. Dem Vertrauen kommt eine Schlüssel-

funktion zu, wenn es um konkrete Positionen auf dem Kontinuum der Kontrolle von Arbeit geht. Daher wird in einem vierten Teil das Verhältnis von Vertrauen und Anerkennung in einer sich digital transformierenden Arbeitswelt beleuchtet (s. Kap. 4.), bevor die vor dem Hintergrund einer »digitalen Souveränität« sich aufwerfenden Probleme einer abschließenden Betrachtung unterzogen werden (s. Kap. 5.).

1. Die Frage nach Selbstorganisation – und die Paradoxie von Autonomie und Heteronomie

Die Fragen nach Autonomie oder Heteronomie von Beschäftigten ebenso wie die nach Selbstorganisation (vgl. Dietrich 2001: 88; Ismael 2011: 333.) sind in Betrieben weniger durch die Forderung nach Souveränität als vielmehr durch eine grundlegende Paradoxie geprägt (vgl. Smith/Lewis 2011): Einerseits zeichnen sich Betriebe durch Strukturen, feste Mitgliedschaften und geregelte Verfahren aus, andererseits sind sie von kreativen, selbstständig handelnden Beschäftigten abhängig – und auf beide Seiten kann trotz ihrer (potenziellen) Widersprüchlichkeit nicht verzichtet werden (vgl. Clegg/Cunha/Cunha 2002). In einer individualisierten Welt gilt Autonomie als eine Art Ideal, wobei die Soziologie schon sehr früh deutlich gemacht hat, dass sich Gesellschaften nur in Abhängigkeiten bzw. Interdependenzen entwickeln können[5]. Souveränitätszuschreibungen in mehrdimensionalen Abhängigkeitsverhältnissen wie in der Arbeitswelt erscheinen dann fast als eine Zumutung. Das genannte Paradox verweist auf den Befund, dass die Organisation von Arbeit in Betrieben generell zwischen Autonomie und Heteronomie oszilliert; denn typische Grundlage von Arbeitsbeziehungen in Erwerbsarbeit ist die Mitgliedschaft in einer Organisation (Betrieb). Mit Abschluss eines Arbeitsvertrags unterwirft man sich den Regeln des Betriebs auf Basis der institutionellen Einbettung der industriellen Beziehungen. Der Grad an Heteronomie schwankt dann je nach tradiertem System (vgl. Anderson 2019) und den spezifischen Machtkonstellationen (vgl. Friedberg 1995). Bei allen Verschiedenheiten in Bezug auf Branchen, Betriebsgrößen

5 Durkheim entwickelt hierfür das Bild von der »organischen Solidarität«, um zu verdeutlichen, dass die Teile von arbeitsteilig differenzierten Gesellschaften durch eben jene Differenzierung und deren Anerkennung voneinander abhängig sind (vgl. Durkheim 1977: 256ff.).

etc. wird zumeist eine polarisierende Tendenz wahrgenommen: tayloristisch anmutende, eng getaktete und starr kontrollierte Arbeitsorganisation am *shop floor*, Prononcieren der Selbstorganisation in hochqualifizierten Bereichen von Kreativ- und Wissensarbeitenden (vgl. Bergmann 2019). Der polarisierenden Wahrnehmung stehen die Befunde gegenüber, dass auch am *shop floor* häufig selbsttätig (re-)agiert und kooperiert wird (bspw. Matsuki 2010) und dass Selbstorganisation als Management- und (Nicht-)Führungskonzept (auch im Bereich hochqualifizierter arbeitsweltlicher Tätigkeiten) stets auch fremdorganisiert ist, da (a) Selbstorganisationsstrukturen *top-down* ins Werk gesetzt werden, (b) diese mit »beschränkter Haftung« auskommen müssen (bspw. fehlende/beschränkte Ressourcenverfügung) und (c) Selbstorganisation zu Widersprüchen zwischen verschiedenen Ebenen (individuelle und gruppenbezogene Arbeitsorganisation, betriebliche und ggf. betriebsübergreifende Prozesse und Strukturen etc.) führt, für die Managementkonzepte keine Lösung anbieten (vgl. Pongratz/Voß 1997). Konkret bedeutet dies, dass Managementkonzepte wie beispielsweise die derzeit reüssierenden agilen Projektmanagementansätze nicht von den Beschäftigten selbst, sondern von übergeordneten Instanzen implementiert werden (vgl. Kalkowski/Mickler 2009). Führungskräfte, nicht die Beschäftigten der Projekte, entscheiden über Form, Inhalt und Procedere der zu implementierenden Ansätze. Dies sogar doppelt: Ansätze wie beispielsweise das derzeit meistgenutzte agile Projektmanagement-Framework *Scrum* (vgl. Sutherland/Schwaber 2007) weisen in der betriebspraktischen Umsetzung eine sehr hohe Varianz auf, bei der nicht selten die eigentlichen Konzepte »nach Lehrbuch« nicht mehr wiederzuerkennen sind – und das, obwohl auch diese Lehrbücher, insbesondere unter dem Credo der Selbstorganisation betrachtet, eine überraschend normative Schlagseite aufweisen (vgl. Sauer/Pfeiffer 2012; Pfeiffer/Nicklich/Sauer 2021). Fraglich ist darüber hinaus, welche Grenzen die Selbstorganisation aufweist, wenn Ziele gesetzt, Prozesse definiert oder Ressourcen (nicht) bereitgestellt werden: Wird selbstorganisiert nur verhandelt, wie unter fix definierten »äußeren« Umständen gehandelt werden kann, oder haben Selbstorganisierte das Recht auf eigene Ressourcenverfügung, Prozessdefinition und Zieldefinitionen? Letzteres würde die Integrationskraft von (kapitalistischen) Betrieben herausfordern (vgl. Stadelbacher/Böhle 2016; Jégou/Souayah 2021). Schließlich findet das eigene (teambasierte oder individuelle) Vorgehen nicht im »luftleeren Raum« statt, sondern ist – zumeist betriebsintern wie -extern – in komplexe Strukturen und Produktlebenszyklen einzufügen. Bei den aktuell reüssierenden agilen Managementmethoden gelten jedoch – allen ungelösten

Fragen auf Teamebene zum Trotz – die Skalierung in der organisationalen Praxis (vgl. Komus 2020) und der Umgang mit dem Paradox von Autonomie und Heteronomie als Hauptproblemfelder (vgl. Vijayasarathy/Turk 2008; Prange/Heracleous 2018).

Die digitale Transformation wirkt hier von zwei Seiten beschleunigend: Technisch stellt sie alternative Möglichkeiten zur Kooperation bereit und macht neue Vernetzungs- und Kooperationsmodelle attraktiv. Sozial verändern sich mit ihr die Ansprüche von Belegschaften an die Gestaltung von Arbeit durch neue Leitbilder – vom kollektiv orientierten, körperlich beanspruchten (männlichen) Facharbeiter hin zu einem*einer individualisierten, ortsunabhängigen, digitalen Wissensarbeiter*in (vgl. Vogt 2016). Bereits hier zeigt sich also: Das Verständnis von Selbstorganisation ist häufig ein verkürztes, und Selbstorganisieren findet jenseits hiervon statt – nicht zuletzt, um Selbstorganisationskonzepte ins Werk setzen zu können. Damit ist darauf verwiesen, dass auch Managementtechniken Moden unterliegen und zwischen den Polen von Autonomie und Heteronomie oszillieren (vgl. Nicklich/Sauer/Pfeiffer 2021). Darüber hinaus operieren Organisationen in der Regel in organisationalen Feldern (vgl. DiMaggio/Powell 1983), wo sie ihr Handeln dann auch an den erfolgreichsten oder vermeintlich innovativsten Organisationen orientieren (vgl. Meyer/Rowan 1977). Es hat sich allerdings speziell in den Hochtechnologieunternehmen und jenen der Kreativwirtschaft die Einsicht durchgesetzt, dass komplexe, ergebniskontrollierte Wissensarbeit produktiver ist, wenn sie keiner *tayloristischen* Prozesskontrolle unterliegt[6]. Kritisch gewendet, wird Heteronomie durch Selbstorganisation nicht weniger, sie wird lediglich in das Arbeitssubjekt hineinverlagert. Souveränitätsgewinne scheinen dann nur in Form von abweichendem Verhalten möglich[7], und es hat sich gezeigt, dass selbstorganisiertes Arbeiten zwar im Diskurs mit Autonomie verknüpft wird, sich Asymmetrien in der Beschäftigung deswegen

6 Wobei die Rolle von Projektmanagementsystemen, seien sie nun »agil« genannt oder nicht, durchaus eine Prozesskontrolle ausüben, allerdings selbstorganisiert. Ein wenig fühlt man sich hier an die Einübung protestantischer Beichtpraxis erinnert, die von der Beichte gegenüber dem Priester absieht, aber im Gegenzug ein ständiges Zeugnisablegen vor sich selbst verlangt und damit eine Habitualisierung eines Schuldbewusstseins. Im Anschluss an Foucault, exemplarisch für die *critical management studies*, siehe den Band von McKinlay und Starkey (1998).

7 Legt man beispielsweise eine spiegelnde Oberfläche unter die Computermaus, simuliert das Aktivität, die einen beruflich genutzten Rechner daran hindert, in den Ruhemodus zu wechseln, und einer überwachenden Instanz Aktivität vorgaukelt.

jedoch nicht auflösen. Um von souveränen Beschäftigungsverhältnissen zu sprechen, scheint »Selbstorganisation« also nicht hinreichend zu sein. Allerdings stellt wohl der entscheidende Motor für selbstorganisiertes Arbeiten das damit verknüpfte Anerkennungsversprechen dar: So sind beispielsweise das selbstkontrollierte Arbeiten (Vertrauensarbeitszeit) oder eine teambasierte Selbstorganisation Formen von Anerkennung jenseits des Gehalts.

2. Freiheitsgrade von Arbeit – und Anerkennung von Arbeitenden

Die Ansprüche an Selbstorganisation seitens der Beschäftigten wie auch der Betriebe bzw. des Managements sind eng mit Fragen nach den Anerkennungsverhältnissen in Arbeit verknüpft, also ihrer Möglichkeit nach Sozialintegration (vgl. Honneth 2008: 341). Selbstorganisation kann sowohl Anerkennung beinhalten als auch ihrer besonders bedürfen. Die Ausweitung von Befugnissen, Selbstabstimmung, Kooperation und die Rücknahme von Kontrollen und Berichtspflichten wird von Beschäftigten häufig als Anerkennung – bzw. genauer: Wertschätzung – erlebt (vgl. Sauer 2017: 217 ff). Mit Selbstorganisation geht somit eine Art (gefühlter) Vertrauensvorschuss einher, der als Wertschätzung (vgl. Honneth 1994: 144) wahrgenommen wird. Im Gegenzug gelten Tätigkeiten, die wenig Freiheitsgrade aufweisen, starren Vorgaben folgen müssen und detailliert kontrolliert werden, als wenig wertschätzend und unattraktiv. Selbstorganisation ist auf Wertschätzung allerdings auch in besonderem Maße angewiesen, da in ihrem Rahmen erbrachte Leistungen oft informell und nicht objektivierbar sind, nicht dokumentiert und daher leicht negiert werden können. Digitalisierung scheint hier von doppelter Relevanz zu sein: *Zum einen* spielt sie eine große Rolle bei der Polarisierung von wenig organisierten und größtenteils selbstorganisierten Tätigkeiten, indem sie beispielsweise Transparenz erhöht, die sowohl für stärker selbstorganisiertes Vorgehen als auch für ein Mehr an Kontrolle verwendet werden kann. Dies gilt ebenso für Berufe und ganze Branchen wie beispielsweise die »Kreativindustrie« oder den – im Vergleich hierzu recht »altbacken« wirkenden – Maschinenbau. *Zum anderen* werden manche Tätigkeiten durch Digitalisierung unterstützt, während andere sich mit dem Ruch des Rückständigen plagen oder durch Digitalisierung (weiter) entwertet werden. Automatisierung kann zu einer Entwertung von beruflichen Fertigkeiten führen *(pick by light)* oder auch zur perspektivisch gänzlichen Rationalisierung eines Berufsfeldes (Controller). Darüber hinaus

verschärfen und polarisieren digital induzierte Automatisierungen Anerkennungskämpfe zwischen ganzen Branchen.

In Bezug auf das Verhältnis Selbstorganisation und Anerkennung kann – detaillierter – konstatiert werden, dass durch Digitalisierung und die hiermit verbundenen Selbstorganisationskonzepte das konkrete Selbstorganisieren der Beschäftigten qualitativ wie quantitativ verändert wird. Es wird zum einen schlicht mehr, da selbstorganisiert zu Bewältigendes durch den partiellen Rückzug des Managements zunimmt, zum anderen werden vormals informelle, implizite Handlungspraxen expliziert. Für die Frage nach Anerkennung ist hierbei wichtig, dass Selbstorganisieren tendenziell ausgeweitet und (verstärkt) beachtet wird, da Beachtung eine Voraussetzung für Anerkennung wie – als Gegenteil – Missachtung ist (vgl. Voswinkel 2001: 43). Während Nichtbeachtetes nicht anerkannt wird – wie sollte es auch –, kann Beachtetes anerkannt oder auch missachtet werden. Die Explikation eines (vermehrten) Selbstorganisierens birgt somit nicht nur die Chance auf Anerkennung für vormals »selbstverständlich« mitlaufende bzw. ignorierte Leistungen sowie darüber hinausgehende »neue« Leistungen, sondern ebenso das Risiko der Missachtung. Anerkennung ist somit kein Automatismus, der aus Chancen zum Selbstorganisieren, kreativen Tätigsein etc. abzuleiten wäre, sondern sehr voraussetzungsvoll – und dies gilt auch in Bezug auf ihre Ausgestaltung. Denn *echte* Anerkennung meint weder oberflächliches Lob noch bloße Reputation (vgl. Voswinkel 2005), sondern kann im Betrieb auf verschiedenen Ebenen stattfinden und die Entlohnung, betriebliche Organisation von Arbeit, Betriebskultur, Kommunikation und Kooperation sowie Möglichkeiten zur eigenen Sinnstiftung in und durch Arbeit umfassen (vgl. Sauer 2017). Diese Feststellung ist wichtig, da sie auch die Bedingungen für »relationale Souveränität« betrifft: Sie muss stets auf dem Boden der institutionalisierten sozialen Beziehungen im Betrieb gesehen werden.

Anerkennung kann nach Honneth, dessen Ansatz häufig als ausdifferenziertester verstanden wird (vgl. Kropf 2005: 135), in drei Modi, *Liebe, Achtung/Recht und Wertschätzung/Solidarität*, untergliedert werden (nach Honneth 1994), wobei die Begriffe »Liebe«, »Recht« und »Wertschätzung« in Bezug auf die Arbeitswelt (ein-)gängiger sind. Kurz zusammengefasst, meint »Liebe« Anerkennung als individuelle Person und impliziert eine gewisse Affektivität und Exklusivität, wogegen »Recht« auf die Anerkennung universeller Rechtsnormen (bspw. Menschenrechte, Bürgerrechte, Betriebsverfassung etc.) fokussiert und sich gerade durch einen hohen Grad der Verallgemeinerbarkeit und nicht affektiven Gültigkeit, nach Honneth (1994: 177) gar durch ein »universa-

listische[s] Begründungsprinzip«, auszeichnet. Wertschätzung rangiert, vom Standpunkt der sozialen Inklusion aus, zwischen diesen beiden Modi: Wertschätzung wird für individuelle Leistungen, die zu einer institutionalisierten oder interaktiv ausgehandelten Zielstellung beitragen, gezollt, notwendiger Hintergrund ist somit ein »intersubjektiv geteilte[r] Werthorizont« (ebd.: 196).

Wertschätzung kann aufgrund der Doppeldeutigkeit des Leistungsbegriffs zwei verschiedene Ausformungen annehmen: Würdigung für großes Engagement wie beispielsweise körperlich schwere Tätigkeiten, langjährige Betriebsmitgliedschaften, integratives Wirken in einem (Projekt-)Team oder unermüdlichen Einsatz für eine wichtige Zielstellung und Bewunderung für großen Ertrag, beispielsweise bahnbrechende Entdeckungen und disruptive Innovationen, auch bei (scheinbar) geringem Aufwand, wobei im Zuge der Subjektivierung von Arbeit Würdigung tendenziell prekärer und Bewunderung virulenter wird (vgl. Voswinkel 2002).

Trotz der von Voswinkel (ebd.) postulierten Tendenz zugunsten bewunderter und zuungunsten gewürdigter Leistungen, die sich auf die gesellschaftliche Makro- ebenso wie die organisationale Mesoebene bezieht, kann auf der Mikroebene konkreten Arbeitshandelns und Selbstorganisierens nicht vom rückhaltlosen »Durchdringen« dieser Tendenz ausgegangen werden. Ähnliches gilt in Bezug auf die Wirkmächtigkeit von auf Titeln und Zertifizierungen basierender Reputation (vgl. Voswinkel 2001) zuungunsten der Anerkennung. Grund hierfür ist die unmittelbare Verwobenheit der Mikroebene mit (sozialem) Handeln (vgl. Maiwald/Sürig 2018). Soziales Handeln – und damit auch Arbeitshandeln – ist durch eine Unmittelbarkeit gekennzeichnet, die (ggf. vorausgehende) Zuschreibungen und (scheinbare) Erfolge mit dem Blick auf konkretes (gemeinsames) Handeln und die Beiträge, die Einzelne hierzu leisten, verbindet. Soziales Handeln führt aus dieser Perspektive immer eine strategische Seite und eine situierte, performative Seite zusammen[8]. Solche Beiträge können dem unmittelbaren Erreichen der jeweiligen Zielstellung dienen und werden so nach dem Anerkennungsmodus der Wertschätzung verhandelt, sie können aber auch im Sinne von Rücksichtnahme und Teamkultur wertvoll sein und entsprächen so als (kollegiale) Fürsorge einer (erweiterten) Interpretation des Anerkennungsmodus *Liebe*.

8 Arbeit wird in der Regel als zweckrationales Handeln gedacht. Konkretes Arbeitshandeln erschöpft sich aber nicht darin, sondern die konkrete Praxis ereignet sich stets unter dem Eindruck von situativen Einflüssen, die über strategische Projektion nicht vorreguliert werden können. Yannick Kalff zeigt dies am Beispiel von Projekten (2018).

Und schließlich wird im sozialen Handeln zumeist recht unmittelbar deutlich, inwieweit eine handelnde Person als allgemeingültig gefasste Normen zwischenmenschlichen Umgangs, wie sie dem Anerkennungsmodus *Recht* entsprechen, einhält. Kurz zusammengefasst: Auf der Mikroebene des sozialen Handelns werden individuelle Beiträge zu gemeinsamen Zielstellungen sowie Grade an Rücksichtnahme und normenbasiertem Agieren deutlich. So kann beispielsweise eine Führungskraft, die ein wichtiges Problem nicht lösen kann oder durch negativ konnotiertes Verhalten auffällt, sich nicht auf die Wirkung ihrer Reputation als Führungskraft verlassen. Auf die Arbeit bezogen, lässt sich hierbei noch ein qualitatives »Mehr« hinsichtlich der Wertschätzung konstatieren: Mit Fokus auf das Arbeitsvermögen als »qualitativ zu füllenden Strukturbegriff« (Pfeiffer 2004: 142) ist davon auszugehen, dass Beschäftigte, die gemeinsam arbeiten, über ein ähnliches Arbeitsvermögen sowie einen ähnlichen Erfahrungshorizont in Bezug auf die jeweilige Tätigkeit verfügen. Sie können sich somit qualitativ in einer wesentlich tiefergehenden Art für ihr Handeln wertschätzen, fachlich wesentlich besser die Qualität der eingebrachten Beiträge beurteilen, als dies Außenstehenden möglich ist (vgl. Sauer 2017: 118ff., 135ff.). Die allgemeinen sowie situierten Anerkennungsformen beeinflussen also auch die Relation von Autonomie und Heteronomie, strukturell und performativ. Allerdings ist noch ungeklärt, wie Digitalisierungsprozesse konkret auf dieses komplexe Verhältnis einwirken. Im Duktus Voswinkels (2002; s.o.) kann jedoch befürchtet werden, dass die mittels Digitalisierung geschaffene Transparenz eine (scheinbare) »Objektivierung« der Arbeit verstärkt, die einseitig an Bewunderung – und weit weniger an Würdigung, Rücksichtnahme etc. – orientiert ist: Es zählt, was mittels digitaler Tools messbar ist – und weit weniger, was erst die Bedingungen für die messbaren Ergebnisse schafft oder aus verschiedensten Gründen keine erfolgreichen Ergebnisse liefert.

Die Beschreibung der Wirkweisen von Anerkennungsverhältnissen stützt die These von der nur relational herzustellenden Souveränität. In spezifischen Anerkennungsverhältnissen können souveräne Arbeitssituationen entstehen, wenn sie es schaffen, trotz heteronomer Rahmung die Handlungsmöglichkeiten der Beteiligten zu erweitern und nicht zu beschränken. Ob die digitale Transformation hier polarisierend sein kann oder lediglich die vorhandenen Ungleichheiten intensiviert, wird in den folgenden beiden Abschnitten noch näher diskutiert, da digital mediatisierte Kommunikation besondere Anforderungen mit sich bringt. Digitalisierung hier vornehmlich im Kontext von Kommunikation zu diskutieren, erscheint uns sinnvoll, da sowohl das selbst-

organisierte Arbeitssubjekt als auch Anerkennungsverhältnisse kommunikativ hergestellt werden und Anerkennungsverhältnisse für Selbstorganisations- und Kommunikationsprozesse von großer Relevanz sind. »Digitale Souveränität« bezieht sich dann in dieser Hinsicht weniger auf die Frage nach Datenhoheit als vielmehr auf die Kommunikationsmöglichkeiten. Diese wiederum liegen quer zu den Anerkennungsformen in zunehmend selbstorganisierten Beschäftigungsverhältnissen.

3. Zwischen Fremd- und Selbstorganisation: Digitalisierung als polarisierende Kraft? Oder die besonderen Ansprüche an (digitale) Kommunikation in der Wissensarbeit

Angetrieben durch neue technische Automatisierungs- und Kontrollmöglichkeiten und zugleich neue digitale Geschäftsmodelle, lässt sich ein beschleunigtes Auseinanderdriften der Arbeitswelt in gegensätzliche Bereiche konstatieren (vgl. grundlegend Schiller 1999). Zum einen ermöglicht Digitalisierung einen ungeahnten Automatisierungsschub, der eine weitreichende Re-*Taylorisierung* von Arbeit zur Folge haben kann[9]. Davon sind nicht nur vermeintlich »einfache« Tätigkeiten betroffen, sondern auch berufsfachliche. Auf der anderen Seite stehen hochqualifizierte Jobs, denen die digitale Transformation einen signifikanten Zuwachs an (individuellen) Freiheitsgraden verspricht. Hierzu gehören auch Themen rund um neue Methoden des Zusammenarbeitens (*Agilisierung*, *co-creation*, *we economy* etc.) und das Ausrufen einer gänzlich anderen, kreativen Arbeitswelt ohne körperliche Mühsal (*new work*, s. Bergmann 2004).

Weiter gilt es, die betriebliche Ebene zu berücksichtigen: Was ist in der Organisation sichtbar – welche Leistung ändert sich durch Digitalisierung? Wird die Tendenz, lediglich Objektivierbares anzuerkennen, weiter verstärkt? Führen neue Managementkonzepte zur Wertschätzung selbstorganisierten Arbeitens oder müssen Beschäftigte die Verantwortung für Prozesse übernehmen, die sie letztlich nicht steuern können?

Gleichzeitig erhöht sich in digitalisierten Betrieben die Kommunikationsintensität, aber auch der Kommunikationsbedarf, denn digitale Kommunika-

9 Dies meint nicht nur eine Renaissance von standardisierter, engmaschig kontrollierter Arbeit, sondern wie Sarah Nies (2021) empirisch zeigt, eine Verknüpfung von Subjektivierung, Eigenverantwortung und standardisierter, digitaler Kontrolle.

tion ist zwar schnell, allerdings alles andere als eindeutig, sondern interpretationsbedürftig. Besonders Selbstorganisation erfordert mehr Kommunikation in Form von z.B. Koordinierung oder Übersetzungsleistung, weil fachlich heterogene Gruppen mehr kooperieren müssen. Sichtbar ist das an mehr Schnittstellenpositionen (vgl. Kaiser 2021).

Das Gewähren bzw. Zeigen von Anerkennung ist in der Arbeitswelt an formalisierte Kommunikationen geknüpft, aber auch an die je spezifische Organisationskultur. Luhmann folgend kann man argumentieren, dass mehr Kommunikation mehr Kontingenz oder Unsicherheit erzeugt, da ihr Gelingen unwahrscheinlich ist (vgl. Luhmann 1997, 1987). So kann konstatiert werden, dass Selbstorganisation als betriebliche Antwort an aufsteigende Komplexität selbst zur Steigerung von Komplexität und Kontingenz beiträgt. Dabei vollzieht sich Kommunikation auch im Betriebskontext mittlerweile meist digital mediatisiert[10]. Gelingen ist hier zwar tagtäglich evident, jedoch verdeckt das den Umstand, dass gelingende digitale Kommunikation wesentlich voraussetzungsvoller ist als analoge. Merkmale digitaler Kommunikation haben u.a. Klemm und Staples (2015) herausgearbeitet: Pseudotypisierung, weil leiblich nicht kopräsent, Kontextualisierung von Inhalten, da symbolische Zeichen nicht transportiert werden können, Handlungsdruck, weil instantane Übermittlung.

Darüber hinaus liegt digital mediatisierte Kommunikation laut Esposito entkoppelt vor: Die kommunikative Dreiheit von Information – Mitteilung – Verstehen ist aufgehoben (vgl. Esposito 1993). Digital mediatisierte Kommunikation transportiert ausschließlich Information (vgl. Halfmann 1995). Entsprechend muss die Information und deren Kontext rekonstruiert werden, damit kommunikativer Anschluss vollzogen werden kann. Der Rekonstruktionsprozess birgt weiterhin Risiken der »richtigen« Übersetzung.

Bei aller technischen Infrastruktur und Versuchen der Standardisierung von digital mediatisierter Kommunikation bleiben die situierten, habitualisierten kommunikativen Kompetenzen der Beteiligten ein zentraler Faktor für gelingende digital mediatisierte Kommunikation. Anzuerkennen, dass digital mediatisierte Kommunikation und damit das Gestalten von sozialen Beziehungen in asymmetrischen Verhältnissen voraussetzungsvoll ist, scheint

10 Bereits 2018 hat eine Befragung der Bitkom ergeben, dass E-Mail das meist genutzte Kommunikationsmittel in deutschen Unternehmen ist (s. hier die Aufbereitung von Brandt 2018). Die diversifizierte Nutzung von digitalen Kommunikationsmitteln dürfte seither kaum abgenommen haben.

ein anhaltender Prozess zu sein (vgl. Lee/Staples 2018). Schließlich sind genau die Akteur*innen, die die informellen kommunikativen Kompetenzen inkorporiert haben, diejenigen, die sich neue Machtquellen erwirtschaften können, wenn ein Betrieb verstärkt auf Selbstorganisation als Strukturprinzip setzt. Crozier und Friedberg haben bereits früh gezeigt, wie sich durch koordiniertes Handeln die Autonomie-Heteronomie-Relation verschieben kann (1979). Erinnert man sich daran, wie (a) wenig souverän selbstorganisiertes Arbeiten an sich ist, wie (b) prekär gelingende Anerkennungsverhältnisse sind und wie (c) voraussetzungsvoll digitale Kommunikation ist, so hilft dieser Ansatz zu verstehen, wie »relationale Souveränität« unter asymmetrischen Bedingungen doch noch entstehen kann.

Die Autoren modellieren hierfür Kooperation in Organisationen spielmetaphorisch. Akteur*innen handeln strategisch, um Ziele zu erreichen, wobei dies nicht deckungsgleich sein muss mit den Organisationszielen. Innerhalb dieser Handlungsfelder identifizieren sie Unsicherheitszonen bzw. Machtquellen (vgl. Porschen-Hueck/Weihrich/Huchler 2018). Die Unsicherheitszonen der Direktion/Manipulation von Kommunikation und Informationsflüssen sowie jene der Problemlösungsfähigkeit für das Problem der Autonomie/Heteronomie sind in digital mediatisierten Arbeitsorganisationen von Interesse.

Die erste Unsicherheitszone hängt direkt mit einem Kommunikationswandel zusammen: Ändert sich die Vermittlung von Kommunikation bzw. Information, ändert sich auch das Vermögen der Direktion oder Manipulation. Unterschiedliche Prognosen können hier abgegeben werden: Erstens eröffnet die digitale Vermittlung den Kampf um diese Unsicherheitszone neu. Wie bereits bemerkt, sind informelle Kompetenzen nun für gelingende Kommunikation noch wichtiger als im analogen, kopräsenten Bereich. Die Unsicherheitszone kann hierdurch neu abgesteckt werden, und bereits etablierte Positionen stehen wieder zur Disposition. Zweitens eröffnet die digitale Vermittlung auch der Verfestigung von machtvollen Relationen eine Tür: Wenn bereits im analogen Bereich Kommunikationsexpertinnen und -experten diese Unsicherheitszone besetzt haben, dann verfügen diese wohl auch über einen strategischen Vorteil in der Aneignung weiterer informeller kommunikativer Kompetenzen. In letzter Konsequenz hieße das, dass sich machtvolle Relationen weiter verfestigen, die Position der Kommunikationsexpertinnen und -experten zentralere Bedeutung erlangt und sich zuletzt eine kommunikative Hierarchie ausbilden kann.

Das hat direkte Folgen für die zweite Unsicherheitszone: der Besitz oder das Vermögen einer schwer zu ersetzenden, funktionalen Fähigkeit oder Spezialisierung (vgl. Crozier/Friedberg 1979: 52ff.). Diese Problemlösefähigkeit muss sich auf ein Problem beziehen, das den Arbeitsablauf der Organisation gravierend beeinflusst. Gerade bei Organisationen, die sich an Selbstorganisation ausrichten, scheint gelingende Kommunikation noch wichtiger und anspruchsvoller – schließlich treffen hier häufig fachfremde Gruppen aufeinander, die sprichwörtlich nicht die gleiche Sprache sprechen. Durch diese Verschiebung von Unsicherheitszonen kommt kommunikativen Fähigkeiten auch anerkennungstheoretisch eine neue Bedeutung zu, wenn das virtuose Beherrschen der digitalen Kommunikationsklaviatur Gegenstand von Bewunderung oder im Sinne von Würdigung schlicht vorausgesetzt wird. Subjektivierungstheoretisch könnte das dann aber auch bedeuten, dass weniger sichtbare Stimmen gänzlich verschwinden, wie Turco in ihrer Studie zeigt (2016).

Digital mediatisierte Kommunikation verändert also Unsicherheitszonen in der Arbeitsorganisation. Versteht man Anerkennungsverhältnisse ebenfalls als kommunikativ verfasst, dann unterliegen auch diese neuen Bedingungen. Denn das Gewähren von Anerkennung beruht zum einen auf objektivierten Formen von Kommunikation, beispielsweise dem Gehalt, und zum anderen – wie im Abschnitt zur Selbstorganisation erörtert – auf situierter Praxis. In den neu entstehenden Unsicherheitszonen müssen diese beiden Formen zur Deckung gebracht werden, soll es nicht zu dysfunktionalen Beziehungen kommen. Konkret heißt das: Im Arbeitsvertrag ist ein variabler Gehaltsbestandteil festgelegt, der sich aufgrund von betriebswirtschaftlichen Kennzahlen ergibt. Wie schafft man (das Unternehmen oder auch der*die konkrete Vorgesetzte) gelingende Anerkennung, wenn eine beschäftigte Person zum Stichtag nach Kennzahlenergebnis keine Prämie zusteht, der*die Beschäftigte aber in der Praxis maßgeblich zum Erfolg der Abteilung beigetragen hat? An diesem Punkt schneiden sich viele der Abhängigkeitsdimensionen von Arbeit, und für alle Beteiligten an der Situation (Beschäftigte und Vorgesetzte) ist diese dilemmatisch. In welchem Ausmaß verlässt man sich als Vorgesetzte*r auf digital generierte Kennzahlen? Und wie schafft man es als Beschäftigte*r, Aufgaben zu bearbeiten, ohne dabei im Hinterkopf zu haben, dass das eigene Handeln und Kommunizieren digital beobachtet und vermessen wird? Kann »relationale Souveränität« in diesem Zusammenhang bedeuten, eine Unsicherheitszone performativ zu besetzen? Und was wäre die Voraussetzung hierfür?

4. Vertrauen und Anerkennung in der digitalisierten Arbeit

Ein grundlegendes Problem von Betrieben ist die Transformation eingekaufter Arbeitskraft in Arbeit, und ein grundlegendes Distinktionskriterium im Spektrum von *vermarktlichter* Erwerbsarbeit stellt die Selbst- bzw. die Fremdorganisation dar. In Gestalt von Homeoffice[11] und Vertrauensarbeitszeit ist selbstorganisierte Arbeit – nicht zuletzt im Zuge der pandemiebedingten Beschränkungen spätestens seit 2020 – für viele Beschäftigte beruflicher Alltag geworden. Gerade bei dieser abwesenden Form von Selbstorganisation entsteht für Organisationen Ungewissheit, können sie die Umwandelung der eingekauften Arbeitskraft doch nicht mehr in traditioneller Weise durch hierarchisch organisierte Überwachung kontrollieren. Diese Ungewissheit, welche Leistungen Beschäftigte wann und wie erstellen, können Organisationen mittels Vertrauen in kalkulierbare Risiken transformieren. Betriebe sichern sich dadurch zunächst wieder ihre Entscheidungsfähigkeit, und Beschäftigte, denen dieses Vertrauen in Gestalt von Homeoffice entgegengebracht wird, empfinden dieses als Wertschätzung ihrer Arbeit und Person. Allerdings ist digitale Kontrolle der Beschäftigten möglich, beispielsweise durch Kontrolle von Log-Protokollen. Arbeitszeit wird dann festgemacht am Anmeldezeitraum über einen beruflich genutzten Rechner oder an der Anmeldung auf der beruflich genutzten Kooperationsplattform. Allerdings kann Vertrauen (als zentraler Bestandteil von psychologischen Verträgen, wie Rousseau gezeigt hat) durch Daten nicht hergestellt werden, obgleich Daten als funktionale Äquivalente zu Vertrauen betrachtet werden können.

Die Beschäftigung der Sozialwissenschaften mit dem Phänomen »Vertrauen« ist mehrdimensional und hochkomplex[12]. Das Phänomen »Vertrauen« scheint in allen Bereichen menschlichen Lebens relevant und, wie Luhmann herausarbeitet, eine soziale Beziehung ganz eigener Qualität zu sein (vgl.

11 Homeoffice ist ein Kofferausdruck, in welchem sich verschiedenste Varianten von Telearbeit und mobiler Arbeit versammeln. Die Unschärfe stellt für Organisationen daher auch ein Problem dar. Denn woran knüpft sich »Home«? Muss man dafür an seinem Hauptwohnsitz sein oder stellt dies die Ver-Ortung von Arbeit und damit die Trennung von Arbeit und Leben grundsätzlich infrage?

12 Interessant hierzu Stähelis (2021) Beobachtung, dass das Etablieren von Netzwerken, die in Organisationen ja sehr zentrale informelle Beziehungen darstellen, die Bildung von Vertrauen behindern kann, wenn statt Kooperation nur mehr Gelegenheiten genutzt werden, um Kontakte zu knüpfen (vgl. ebd.: 82).

Luhmann 2014). In der Arbeitswelt stehen Arbeitgeber*innen vor dem Problem von Vertrauen und/oder Kontrolle: Wer vertraut, nimmt Ungewissheiten in der Zukunft vorweg, kann aber auch enttäuscht werden. Wer kontrolliert, sichert zwar (scheinbar) eine gewisse Zukunft, spricht dem*der Kontrollierten allerdings die Anerkennung/Wertschätzung durch Vertrauen ab – und benötigt Ressourcen für die Kontrolle.

Vertrauen hat – allgemeiner gesprochen – mehrere Funktionen: Vertrauen soll (1) komplexitätsreduzierend wirken (vgl. Luhmann 2014), es soll (2) Handlungssteuerung in Gegenwart und Zukunft ermöglichen (vgl. Endreß 2002: 30) und es wirkt (3) als Lösung spezifischer Risikoprobleme (vgl. Luhmann 2001: 144; s. Peetz/Staples/Steinbach 2021). Beschränkt man die Funktionen von Vertrauen auf diese drei, so kann man zwischen Vertrauen und digitalen Daten funktionale Äquivalenz erkennen. Auch digitale Daten reduzieren Komplexität, schaffen Handlungssteuerung und können zur Lösung bestimmter Risikoprobleme beitragen. Dennoch gibt es eine Funktion von Vertrauen in sozialen Beziehungen, die eine funktionale Äquivalenz und daher auch eine Überführung von Vertrauen in digitale Daten *et vice versa* unmöglich macht: Nur Vertrauen kann Informationsgrenzen überwinden. Laut Simmel ist Vertrauen auch als funktionaler Ersatz für Information über Handlungsmotive anderer Akteure denkbar (vgl. Hartmann 2001). Für Daten ist das jedoch nicht möglich. Daten müssen interpretiert werden, um zu Informationen zu werden, und verlieren dadurch ihre Objektivität, die sie in maschinellen Systemen besitzen. Grund dafür ist die Inkommensurabilität der kommunikativen Operationsweisen von sozialen und maschinellen Systemen.

Blickt man auf das Verhältnis von Menschen und Maschinen, so gibt es eine Reihe von Möglichkeiten, dieses zu beschreiben (vgl. Muhle 2018). Muhle skizziert die prominentesten und schlägt dabei selbst einen kommunikationstheoretischen Zugang vor. Dem folgend, lässt sich ein kommunikationstheoretischer Zugang zum Verhältnis von Mensch und Maschine so skizzieren: Soziale Systeme operieren sinnhaft-rekursiv, maschinelle Systeme kausal-rekursiv (vgl. Miebach 2011; Karafillidis 2013). Es ist also eine Interpretationsleistung der sinnhaft-rekursiven sozialen Systeme, wenn sie sich auf Datenoutput beziehen oder sich diesen aneignen. Die im maschinellen Bereich objektiven Daten erhalten dadurch ein Downgrade: Sie haben im Bereich der sozialen Systeme nur noch die Zuschreibung der Objektivität.

Arbeitszeitkontrolle oder die Kontrolle von Arbeitsleistung in selbstorganisierter Arbeit als Vertrauens- und Anerkennungsproblem kann daher nur unzureichend auf Basis von Daten gelöst werden. Daten sind nur im maschinel-

len System eindeutig, strukturieren Zukunft nur im maschinellen System und bearbeiten Informationsgrenzen nur im maschinellen System. Daten können nur bei Aneignung zu Informationen werden. Informationen existieren nur in sozialen Systemen, weil diese sinnhaft-rekursiv operieren. Wie o.g. brauchen soziale Systeme aber Handlungssteuerung in Gegenwart und Zukunft. Oder anders gesagt: Es »steigt mit zunehmender Komplexität auch der Bedarf für Vergewisserungen der Gegenwart, zum Beispiel für Vertrauen« oder eben Daten (Luhmann 2014: 15), wie die Empirie zeigt. Dass der Vergewisserung über Daten aber ein Anerkennungsproblem inhärent ist, wollen wir zeigen.

Das Ergebnis der Aneignung maschinell präsentierter Daten zu Informationen kann sich aufgrund der Kontingenz – ausgedrückt durch mannigfaltige Aneignungstechniken (Analyseverfahren, verwendete Software etc.) – unterscheiden.

Wenn nun also versucht wird, auf Basis scheinbar objektiver Daten ein Risikoproblem (Transformationsproblem) in sozialen Systemen zu lösen, wird der soziale Sinn, der mit der Aneignung von Daten in Informationen einhergeht, vernachlässigt und die dabei produzierte Kontingenz ignoriert. Gerade diese Kontingenz scheint es zu sein, die Vertrauen mit Anerkennung verbindet. Vertrauen zeichnet sich durch einen flüchtigen, präreflexiven Zustand aus. Es ist nur Vertrauen, wenn es auch gebrochen werden kann (s. Luhmann 2014). Die zugeschriebene Objektivität von Daten in der Benutzung durch soziale Systeme lässt einen solchen Zustand nicht zu, auch wenn es ihn gibt. Schließlich ist die Objektivität der Daten in sozialen Systemen nur eine Zuschreibung.

Hinsichtlich des Ausgangsproblems der Kontrolle von selbstorganisiertem Arbeiten scheint das Verhältnis von sozialen Systemen und maschinellen Systemen Konflikte zu produzieren, beziehen sich die Kontrollierenden doch auf scheinbar objektive Daten, welche von den Kontrollierten jedoch auch ganz anders interpretiert werden können (erinnert sei an das obige Beispiel, in dem Log-ins als beruflich aktive Zeit interpretiert werden). Ursächlich ist nach Darstellung der Theorielage einerseits die Überführung eines sozialen Problems in ein technisches (Vertrauen/Anerkennung in Daten). Andererseits ist in der Behandlung des Problems die Inkommensurabilität der Operationsweisen Ursache des Problems. Wie in anderen Bereichen auch (Personalentscheidung, Daten in Verfahren) zeigt jedoch die Praxis ein ambiges Bild beim Einsatz von Daten: Der Bezug auf Daten erscheint zunächst als Lösung für (Entscheidungs-)Probleme und produziert dann doch – zumindest theoretisch – weitere Probleme. Allerdings findet sich dieses kommunikationstheoretische

Problem auch in der konkreten Gestaltung von Arbeitsbeziehungen wieder, wenn Telearbeit als Einfallstor von Entgrenzung, weil schlecht kontrollierbar, problematisiert wird (vgl. Berzel/Schroeder 2021). Wir haben vorhin gezeigt, dass in Organisationen Unsicherheitszonen entstehen, in denen die Machtverhältnisse nicht eindeutig sind bzw. neu geordnet werden können. Nimmt man die kommunikationstheoretischen Erkenntnisse ernst, dann stellt sich die Frage, ob »digitale Souveränität« nicht jene Zone in betrieblichen Beziehungen bezeichnen kann, in welcher aufgrund digitaler Transformation die Beziehungen, und das heißt auch Vertrauen, sowie die Struktur der betrieblichen Anerkennungsverhältnisse neu ausgehandelt werden müssen. Damit würde man sich von dem (juristisch weiterhin bestehenden Problem) der Datenhoheit lösen und mehr fragen, wie Beschäftigte und Arbeitgeber*innen ihre Beziehungen strukturieren und wie sie aus dem gemeinsamen Bezug auf Daten Handlungsoptionen generieren. Das würde das obige Beispiel zum Gratifikationsproblem dann genauso einschließen wie die Gestaltung beruflicher Beziehungen in einem digitalen Kommunikationsraum (bspw. die VW-Richtlinie, dass E-Mails nach 19:30 Uhr die Server nicht mehr verlassen). Auf analytischer Ebene wird man dem relationalen Charakter »digitaler Souveränität« von Beschäftigten, den wir hier vor dem Hintergrund von Autonomie und Heteronomie beleuchten wollen, dadurch gerecht, wenn man dazu passend auch Aushandlungsprozesse in den sozialen Beziehungen eben z.B. in puncto Hierarchie in den Blick nimmt.

5. Abschließende Betrachtungen

»Souveränität« bleibt für die Arbeitssoziologie ein herausfordernder Begriff, da insbesondere Erwerbsarbeit, wie gezeigt, stets in verschiedene *vermachtete* Strukturen wie Arbeitsbeziehungen, Wertschöpfungsketten etc. eingebunden ist. Daher stellten wir die Differenz von Autonomie und Heteronomie (in der Arbeit) der Frage nach individueller Souveränität an die Seite[13]. An ein solchermaßen relationales Verständnis schließt auch unser Verständnis von Digitalisierung an, die wir nicht als per se souveränitätsfördernd oder -verhindernd verstehen, sondern die sowohl autonomie- als auch heteronomie-

13 Inwiefern Organisationen bzw. Unternehmen souverän sind in ihrem Handeln, können wir in diesem Zusammenhang nicht beantworten, aber die Organisation Studies wären hier eher skeptisch.

orientiert eingesetzt und ausgestaltet werden kann. Sie läuft daher Gefahr, zu einer weiteren Polarisierung von Ungleichheit in der Erwerbswelt beizutragen (s. hierzu die Beiträge von Tretter 2022 und Dammann/Glasze 2022 in diesem Band). Wir haben im Text auf mehreren Ebenen Prozesse skizziert und daran anschließende Probleme aufgezeigt, die die Relation von Autonomie und Heteronomie in der digitalen Transformation beeinflussen können. Ausgangspunkt unserer Überlegungen ist ein Status quo der Organisation von Erwerbsarbeit, in dem der *Taylorismus* überwunden scheint und wo indirekte Steuerung und *Vermarktlichung* der Organisation von Arbeit einerseits mehr Freiheitsgrade versprechen und andererseits mehr Kommunikation erfordern. Damit einher gehen die Umformung des Transformationsproblems von Arbeit sowie die zunehmend schwierigere Herstellung von Solidarität bzw. Wertschätzung als ein Modus von Anerkennung. Die Digitalisierung von Arbeit und ihrer Gestaltung tritt zu diesen Grundproblemen hinzu.

Konkret haben wir versucht, konzeptionelle Rahmungen zu finden, die sichtbar machen können, wo digitale Transformation einen Einfluss auf eine als relational verstandene Souveränität von Arbeitsverhältnissen haben kann. Klar scheint allerdings lediglich, dass digitale Transformation als Strukturveränderung im Kosmos der Erwerbsarbeit in allen Dimensionen derselben wirkt. Außerdem scheint es für Arbeitsverhältnisse relevante Bezugsgrößen zu geben, die sich digitaler Transformation widersetzen, wie z.B. Wertschätzung durch Vertrauen oder Erfahrungswissen (s. Böhle 2017). In anderen Dimensionen dieses Kosmos wirkt Digitalisierung möglicherweise stark verändernd, beispielsweise wenn wir die Herstellung von Solidarität oder kommunikativ begründete Hierarchien betrachten. Deutlich wird vor allen Dingen, dass Souveränität sich in diesen Konstellationen als eine Zuschreibung zeigt. Wir schlagen sogar vor: als eine Zuschreibung an die Qualität von sozialen Beziehungen in einem arbeitsbezogenen Kontext. Wie eingangs an den widersprüchlichen Erwartungen gezeigt, die an selbstorganisiertes Arbeiten herangetragen werden, scheint es nicht erkenntnisförderlich, wenn »digitale Souveränität« als Eigenschaft von Subjekten verstanden wird.

Aufgrund der Schwierigkeiten, die die Gestaltung von Arbeitsbeziehungen an sich zu meistern hat durch Anerkennungsansprüche und das Problem von Vertrauen, schlagen wir vor, »digitale Souveränität« als eine Bezeichnung für die situierte Gestaltung von Arbeitsbeziehungen zu benutzen. Diese zeichnet sich dann dadurch aus, dass sie den Unterschied zwischen sozialer Beziehung und ihrer digitalen (maschinellen) Vermittlung und Objektivierung erkennen und zur Gestaltung der neuen Unsicherheitszonen im Betrieb produktiv ma-

chen kann. Das Grundproblem des Changierens von Arbeitsbeziehungen zwischen Autonomie und Heteronomie wird dadurch nicht aufgelöst, aber »digital-relationale Souveränität« kann in der hier vorgeschlagenen Weise zu einer produktiven Analysekategorie werden. Diese löst sich dabei von einer Souveränitätssemantik, die Souveränität als ein »Verfügen über« versteht, und verschiebt den Blick auf das Gestalten von komplexen sozialen Beziehungen. Die Vorbedingung, um eine derartige situierte Praxis zu ermöglichen, ist vorrangig die Gestaltung von vertrauensvollen Anerkennungsbeziehungen in den Organisationen. Selbst dann dürfte die Feststellung von digital-relationalen souveränen Beziehungen eine Ex-post-Zuschreibung sein. Dies ist dann jedoch eine Aufgabe für empirische Forschung, die untersucht, in welchen Teilbereichen der Arbeitswelt günstige oder ungünstige Bedingungen zur Verfügung gestellt werden und wo digitale Transformation wirkungsvoll in Erscheinung tritt.

Literaturverzeichnis

Anderson, Elizabeth (2019): Private Regierung: wie Arbeitgeber über unser Leben herrschen (und warum wir nicht darüber reden), Berlin: Suhrkamp.

Bauer, Wilhelm/Hofmann, Josephine (2018): »Arbeit, IT und Digitalisierung«, in: Josephine Hofmann (Hg.), Arbeit 4.0 – Digitalisierung, IT und Arbeit (= Edition HMD), Wiesbaden: Springer Fachmedien, S. 1–16, https://doi.org/10.1007/978-3-658-21359-6_1.

Bergmann, Frithjof (2004): Neue Arbeit, neue Kultur, Freiburg: Arbor.

Bergmann, Frithjof (2019): New work, new culture: Work we want and a culture that strengthens us, Winchester/Washington: Zero Books.

Berzel, Alexander/Schroeder, Wolfgang (2021): Homeoffice – eine Transformation der Arbeitswelt. Systematischer Überblick und Perspektiven der Gestaltung. Online unter: https://kobra.uni-kassel.de/handle/123456789/13026, abgerufen am 24.02.2022.

Böhle, Fritz (Hg.) (2017): Arbeit als Subjektivierendes Handeln. Handlungsfähigkeit bei Unwägbarkeiten und Ungewissheit, Wiesbaden: VS Verlag.

Brandt, Mathias (2018): So kommunizieren Unternehmen in Deutschland. Digitales Bild, Statista vom 13.09.2018. Online unter: https://de.statista.com/infografik/15443/von-unternehmen-in-deutschland-genutzte-kommunikationskanaele/, abgerufen am 22.02.2022.

Castells, Manuel (2017): Der Aufstieg der Netzwerkgesellschaft: Das Informationszeitalter. Wirtschaft. Gesellschaft. Kultur. (= Neue Bibliothek der Sozialwissenschaften, Band 1), Wiesbaden: Springer Fachmedien, https://doi.org/10.1007/978-3-658-11322-3.

Clegg, R. Stewart/da Cunha, João Vieira/e Cunha, Miguel Pina (2002): »Management paradoxes. A relational view«, in: Human Relations 55, S. 483–509.

Crozier, Michel/Friedberg, Erhard (1979): Macht und Organisation: die Zwänge kollektiven Handelns, Königstein: Athenäum.

Dammann, Finn/Glasze, Georg (2022): »›Wir müssen als Deutsche und Europäer unsere digitale Souveränität zurückgewinnen!‹ Historische Rekonstruktion und internationale Kontextualisierung der Diskurse einer ›digitalen Souveränität‹ in Deutschland«, in: Georg Glasze/Eva Odzuck/Ronald Staples (Hg.), Was heißt digitale Souveränität? Diskurse, Praktiken und Voraussetzungen »individueller« und »staatlicher Souveränität« im digitalen Zeitalter, Bielefeld: transcript, S. 29–60.

Dietrich, Andreas (2001): Selbstorganisation. Management aus ganzheitlicher Perspektive, Wiesbaden: Deutscher Universitäts-Verlag.

DiMaggio, Paul/Powell, Walter W. (1983): »The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields«, in: American Sociological Review 48 (2), S. 147–160, https://doi.org/10.2307/2095101.

Durkheim, Émile (1977): Über die Teilung der sozialen Arbeit, Frankfurt a.M.: Suhrkamp.

Endreß, Martin (2002): Vertrauen, Bielefeld: transcript, https://doi.org/10.14361/9783839400784.

Esposito, Elena (1993): »Der Computer als Medium und Maschine«, in: Zeitschrift für Soziologie 22 (5), S. 338–354.

Esposito, Elena (2014): »Algorithmische Kontingenz. Der Umgang mit Unsicherheit im Web«, in: Alberto Cevolini (Hg.), Die Ordnung des Kontingenten. Beiträge zur zahlenmäßigen Selbstbeschreibung der modernen Gesellschaft (= Innovation und Gesellschaft), Wiesbaden: Springer Fachmedien, S. 233–249, https://doi.org/10.1007/978-3-531-19235-2_10.

Friedberg, Erhard (1995): Ordnung und Macht: Dynamiken organisierten Handelns, Frankfurt a.M./New York: Campus.

Fritzsche, Albrecht (2022): »Konturenbildung im Gestaltungsraum der digitalen Transformation – eine Reflektion der Debatte über ›digitale Souveränität‹ aus betriebswirtschaftlicher Sicht«, in: Georg Glasze/Eva Odzuck/

Ronald Staples (Hg.), Was heißt digitale Souveränität? Diskurse, Praktiken und Voraussetzungen »individueller« und »staatlicher Souveränität« im digitalen Zeitalter, Bielefeld: transcript, S. 229–245.

Halfmann, Jost (1995): »Kausale Simplifikationen. Grundlagenprobleme einer Soziologie der Technik«, in: Jost Halfmann (Hg.), Theoriebausteine der Techniksoziologie (= Technik und Gesellschaft, Band 8), Frankfurt a.M./New York: Campus, S. 211–226.

Hartmann, Martin (2001): »Einleitung«, in: Martin Hartmann/Claus Offe (Hg.), Vertrauen. Die Grundlage des sozialen Zusammenhalts, Frankfurt a.M./New York: Campus, S. 7–37.

Honneth, Axel (1994): Kampf um Anerkennung. Zur moralischen Grammatik sozialer Konflikte, Frankfurt a.M.: Suhrkamp.

Honneth, Axel (2008): »Arbeit und Anerkennung. Versuch einer Neubestimmung«, in: Deutsche Zeitschrift für Philosophie 56 (3), S. 327–341, https://doi.org/10.1524/dzph.2008.56.3.327.

Ismael, Jennan (2011): »Self-organization and self-governance«, in: Philosophy of the Social Sciences 41 (3), S. 327–351.

Jégou, Olivier/Souayah, Fyriel (2021): »What do workers get out of agility? Examining workers' capability for democratic self-government of work«, in: Sabine Pfeiffer/Manuel Nicklich/Stefan Sauer (Hg.), The agile imperative. Dynamics of virtual work, Cham: Palgrave Macmillan, S. 203–224.

Kaiser, Stephan (2021): »Organisationale Verankerung und Schnittstellenmanagement der Mitarbeiterkommunikation«, in: Sabine Einwiller/Sonja Sackmann/Ansgar Zerfaß (Hg.), Handbuch Mitarbeiterkommunikation: Interne Kommunikation in Unternehmen, Wiesbaden: Springer Fachmedien, S. 209–219.

Kalff, Yannick (2018): Organisierendes Arbeiten: zur Performativität von Projekten, Bielefeld: transcript.

Kalkowski, Peter/Mickler, Otfried (2009): Antinomien des Projektmanagements. Eine Arbeitsform zwischen Direktive und Freiraum, Berlin: Edition Sigma.

Karafillidis, Athanasios (2013): »Erklärungen in rekursiven Verhältnissen«, in: Zeitschrift für Theoretische Soziologie 1 (2), S. 218–238.

Klemm, Matthias/Staples, Ronald (2015): »Warten auf Antwort«, in: Kornelia Hahn/Martin Stempfhuber (Hg.), Präsenzen 2.0, Medienkulturen im digitalen Zeitalter, Wiesbaden: Springer VS, S. 113–134

Komus, Ayelt (2020): Status quo (scaled) agile 2020. Ergebnisbericht. Online unter: www.status-quo-agile.de, abgerufen am 20.03.2021.

Kropf, Julia (2005): Flexibilisierung – Subjektivierung – Anerkennung. Auswirkungen von Flexibilisierungsmaßnahmen auf die Anerkennungsbeziehungen in Unternehmen, München: Biblion Verlag.

Lee, Horan/Staples, Ronald (2018): »Digitale Solidarität unter Arbeitnehmer*innen«, in: Industrielle Beziehungen/The German Journal of Industrial Relations 25 (4), S. 495–517.

Luhmann, Niklas (1987): Soziale Systeme: Grundriss einer allgemeinen Theorie, Frankfurt a.M.: Suhrkamp.

Luhmann, Niklas (1997): Die Gesellschaft der Gesellschaft, Frankfurt a.M.: Suhrkamp.

Luhmann, Niklas (2001): »Vertrautheit, Zuversicht, Vertrauen: Probleme und Alternativen«, in: Martin Hartmann/Claus Offe (Hg.), Vertrauen. Die Grundlage des sozialen Zusammenhalts, Frankfurt a.M./New York: Campus, S. 143–161.

Luhmann, Niklas (2014): Vertrauen, Konstanz: UVK Verlagsgesellschaft.

MacKenzie, Donald (2018): »Material signals: A historical sociology of high-frequency trading«, in: American Journal of Sociology 123 (6), S. 1635–1683, https://doi.org/10.1086/697318.

MacKenzie, Donald (2019): »How algorithms interact: Goffman's ›interaction order‹ in automated trading«, in: Theory, Culture & Society 36 (2), S. 39–59.

Maiwald, Kai-Olaf/Sürig, Inken (2018): Mikrosoziologie: eine Einführung, Studientexte zur Soziologie, Wiesbaden/Heidelberg: Springer VS.

Matsuki, Norio (2010): »Acquisition of skills on the shop-floor. Visualization and substitution of skills in manufacturing«, in: Synthesiology 3 (1), S. 47–55.

Matthöfer, Hans (1980): Humanisierung der Arbeit und Produktivität in der Industriegesellschaft, Köln: Bund-Verlag.

McKinlay, Alan/Starkey, Ken (1998): »Managing Foucault: Foucault, management and organization theory«, in: Alan McKinlay/Ken Starkey (Hg.), Foucault, management and organization theory. From panopticum to technologies of self, London/Thousand Oaks/New Delhi: Sage, S. 1–13.

Meyer, John W./Rowan, Brian (1977): »Institutionalized organizations: Formal structure as myth and ceremony«, in: American Journal of Sociology 83 (2), S. 340–363.

Miebach, Bernhard (2011): »Computer und soziale Systeme: Strukturelle Kopplung oder Material Agency?«, in: Soziale Systeme 17 (1), S. 97–119.

Muhle, Florian (2018): »Sozialität von und mit Robotern? Drei soziologische Antworten und eine kommunikationstheoretische Alternative«, in: Zeitschrift für Soziologie 47 (3), S. 147–163.

Nachtwey, Oliver/Staab, Philipp (2020): »Das Produktionsmodell des digitalen Kapitalismus«, in: Sabine Maasen/Jan-Hendrik Passoth (Hg.), Soziologie des Digitalen – Digitale Soziologie? (= Soziale Welt, Sonderband), Baden-Baden: Nomos, S. 285–304.

Nassehi, Armin (2019): Muster: Theorie der digitalen Gesellschaft, München: C.H. Beck.

Nicklich, Manuel/Sauer, Stefan/Pfeiffer, Sabine (2021): »Antecedents and consequences of agility—On the ongoing invocation of self-organization«, in: Sabine Pfeiffer/Manuel Nicklich/Stefan Sauer (Hg.), The agile imperative: Teams, organizations and society under reconstruction? (= Dynamics of Virtual Work), Cham: Palgrave Macmillan, S. 19–38.

Nies, Sarah (2021): »Eine Frage der Kontrolle? Betriebliche Strategien der Digitalisierung und die Autonomie von Beschäftigen in der Produktion«, in: Berliner Journal für Soziologie 31, S. 475–504, https://doi.org/10.1007/s11609-021-00452-8.

Peetz, Siglinde/Staples, Ronald/Steinbach, Vincent (2021): »Goodbye world. On the incommensurability of technical and sensemaking communication«, in: Proceedings of the STS Conference Graz 2021, https://doi.org/10.3217/978-3-85125-855-4-17.

Pfeiffer, Sabine (2004): Arbeitsvermögen. Ein Schlüssel zur Analyse (reflexiver) Informatisierung, Wiesbaden: Springer VS.

Pfeiffer, Sabine/Nicklich, Manuel/Sauer, Stefan (Hg.) (2021): The agile imperative: teams, organizations and society under reconstruction?, Cham: Palgrave Macmillan.

Pongratz, Hans/Voß, G. Günter (1997): »Fremdorganisierte Selbstorganisation. Eine soziologische Diskussion aktueller Managementkonzepte«, in: Zeitschrift für Personalforschung 11 (1), S. 30–53.

Porschen-Hueck, Stephanie/Weihrich, Margit/Huchler, Norbert (2018): »Dynamisches Grenzmanagement in Offenen Organisationen«, in: Olaf Geramanis/Stefan Hutmacher (Hg.), Identität in der modernen Arbeitswelt: Neue Konzepte für Zugehörigkeit, Zusammenarbeit und Führung (= uniscope. Publikationen der SGO Stiftung), Wiesbaden: Springer, S. 235–257.

Prange, Christiane/Heracleous, Loizos (Hg.) (2018): Agility.X: How organizations thrive in unpredictable times, Cambridge: Cambridge University Press.

Rousseau, Denise M. (1989): »Psychological and Implied Contracts in Organizations«, in: Employee Responsibilities and Rights Journal 2 (2), S. 121–139.

Sauer, Stefan (2017): »Partizipative Forschung und Gestaltung als Antwort auf empirische und forschungspolitische Herausforderungen der Arbeitsforschung?«, in: Industrielle Beziehungen. Zeitschrift für Arbeit, Organisation und Management 24 (3), S. 3–4.

Sauer, Stefan/Pfeiffer, Sabine (2012): »(Erfahrungs-)Wissen als Planungsressource: Neue Formen der Wissens(ver-?)nutzung im Unternehmen am Beispiel agiler Entwicklungsmethoden«, in: Getraud Koch/Jürgen Warneken (Hg.): Wissensarbeit und Arbeitswissen, Frankfurt a.M./New York: Campus, S. 195–210.

Schaupp, Simon (2021): »Algorithmic integration and precarious (dis)obedience: On the co-constitution of migration regime and workplace regime in digitalised manufacturing and logistics«, in: Work, Employment and Society 36 (2), S. 1–18, https://doi.org/10.1177/09500170211031458.

Schiller, Dan (1999): Digital capitalism: Networking the global market system, Cambridge: MIT Press.

Smith, Wendy K./Lewis, Marianne W. (2011): »Toward a theory of paradox: A dynamic equilibrium model of organizing«, in: Academy of Management Review 36 (2), S. 381–403.

Stadelbacher, Stephanie/Böhle, Fritz (2016): »Selbstorganisation als sozialer Mechanismus der reflexiv-modernen Herstellung sozialer Ordnung? Zur gesellschaftlichen Verortung von Selbstorganisation und ihre theoretisch-konzeptuelle Bestimmung«, in: Fritz Böhle/Werner Schneider (Hg.), Subjekt – Handeln – Institution. Vergesellschaftung und Subjekt in der Reflexiven Moderne, Weilerswist: Velbrück, S. 324–356.

Stäheli, Urs (2021): Soziologie der Entnetzung, Frankfurt a.M.: Suhrkamp.

Sutherland, Jeff/Schwaber, Ken (2007): The scrum papers. Nuts, bolts and origins of an agile process. Online unter: https://www.academia.edu/download/64196137/scrumpapers.pdf, abgerufen am 10.04.2022.

Taylor, Frederick W. (1998): The principles of scientific management, Mineola: Dover Publications.

Tretter, Max (2022): »›Digitale Souveränität‹ als Kontrolle. Ihre zentralen Formen und ihr Verhältnis zueinander«, in: Georg Glasze/Eva Odzuck/Ronald Staples (Hg.), Was heißt digitale Souveränität? Diskurse, Praktiken und Voraussetzungen »individueller« und »staatlicher Souveränität« im digitalen Zeitalter, Bielefeld: transcript, S. 89–125.

Turco, Catherine J. (2016): The conversational firm: Rethinking bureaucracy in the age of social media (= The middle range), New York: Columbia University Press.

Vijayasarathy, Leo R./Turk, Daniel E. (2008): »Agile software development: A survey of early adopters«, in: Journal of Information Technology Management 19 (2), S. 1–8.

Vogt, Kristoffer C. (2016): »The post-industrial society: From utopia to ideology«, in: Work, Employment and Society 30 (2), S. 366–376, https://doi.org/10.1177/0950017015577911.

Voswinkel, Stephan (2001): Anerkennung und Reputation. Die Dramaturgie industrieller Beziehungen; mit einer Fallstudie zum »Bündnis für Arbeit«, Konstanz: UVK Verlagsgesellschaft.

Voswinkel, Stephan (2002): »›Bewunderung ohne Würdigung‹. Paradoxien der Anerkennung doppelt subjektiver Arbeit«, in: Axel Honneth (Hg.), Befreiung aus der Mündigkeit. Paradoxien des gegenwärtigen Kapitalismus, Frankfurt a.M./New York: Campus, S. 65–92.

Voswinkel, Stephan (2005): Welche Kundenorientierung? Anerkennung in der Dienstleistungsarbeit, Berlin: Edition Sigma.

Windeler, Arnold (2001): Unternehmungsnetzwerke: Konstitution und Strukturation, Wiesbaden: Westdeutscher Verlag.

Wolf, Harald (1999): Arbeit und Autonomie: ein Versuch über die Widersprüche und Metamorphosen kapitalistischer Produktion, Münster: Westfälisches Dampfboot.

Autor*innen

Benenson, Zinaida ist Privatdozentin und leitet die Forschungsgruppe »Human Factors in Security and Privacy« an der Friedrich-Alexander-Universität Erlangen-Nürnberg. Ihre Forschungsschwerpunkte umfassen benutzbare IT-Sicherheit (Entwicklung von graphischen Oberflächen, Nutzerakzeptanz von Schutzmaßnahmen, Social Engineering) und IT-Sicherheit für das Internet der Dinge.

Dammann, Finn ist wissenschaftlicher Mitarbeiter am Institut für Geographie der FAU Erlangen-Nürnberg. Seine Forschungsinteressen liegen im Bereich Politische Geographien der digitalen Transformation und im interdisziplinären Schnittfeld zwischen Kritischer Kartographie und GIScience.

Freiling, Felix ist Inhaber des Lehrstuhls für Informatik (IT-Sicherheitsinfrastrukturen) an der Friedrich-Alexander-Universität Erlangen-Nürnberg. Seine Forschungsschwerpunkte sind in der Cyberkriminalität und der Forensischen Informatik angesiedelt.

Fritzsche, Albrecht ist Professor an der Fakultät für Wirtschaftswissenschaften der Internationalen Universität Rabat (Rabat Business School) in Marokko und koordiniert dort den Forschungsbereich Innovation und Komplexitätsmanagement. Er hat in den Fächern Technikphilosophie und Betriebswirtschaftslehre promoviert. Seine Forschungsarbeiten befassen sich mit einer Reihe unterschiedlicher Fragestellungen im Kontext von Digitalisierung und Innovation.

Glasze, Georg leitet den Lehrstuhl für Kulturgeographie an der FAU Erlangen-Nürnberg. Seine Forschungsinteressen liegen im Bereich der Politischen

Geographie, der geographischen Stadtforschung sowie der soziotechnischen Raumverhältnisse in der digitalen Transformation.

Hagenhoff, Svenja ist Professorin am Institut für Buchwissenschaft, Department Medienwissenschaften und Kunstgeschichte der Friedrich-Alexander-Universität Erlangen-Nürnberg und seit 2021 zudem interimistische Sprecherin des neu gegründeten Departments Digital Humanities and Social Studies. Sie hat an der Georg-August-Universität Göttingen in Wirtschaftsinformatik promoviert und habilitiert.

Hofmann, Franz ist Inhaber des Lehrstuhls für Bürgerliches Recht, Recht des Geistigen Eigentums und Technikrecht an der Friedrich-Alexander-Universität Erlangen-Nürnberg. Er lehrt und forscht vor allem im Bereich der Digitalisierung aus der Perspektive des Rechts des Geistigen Eigentums. Besonders interessieren ihn die Haftung von Online-Plattformen und die Rechtsdurchsetzung im Internet.

Kammerl, Rudolf ist Inhaber des Lehrstuhls für Pädagogik mit dem Schwerpunkt Medienpädagogik an der Friedrich-Alexander-Universität Erlangen-Nürnberg. Seine Forschungsschwerpunkte sind Sozialisation, Erziehung und Bildung einer mediatisierten Gesellschaft.

Leyrer, Katharina ist wissenschaftliche Mitarbeiterin am Institut für Buchwissenschaft und am Department Digital Humanities and Social Studies an der FAU Erlangen-Nürnberg. Ihre Forschungsschwerpunkte liegen bei Informationsintermediären, wertebasierter Technologie-Entwicklung und Theorien der Informationsethik.

Meyer-Wegener, Klaus leitete bis Mai 2020 den Lehrstuhl für Informatik (Datenmanagement) an der Friedrich-Alexander-Universität Erlangen-Nürnberg. Seine Forschungsschwerpunkte sind Multimedia-Datenbanken, Dokument- und Prozessverwaltung (Workflow-Management), Datenstromsysteme sowie Datenmanagement für (Big-Data-)Analysen.

Müller, Jane leitet die BMBF-Nachwuchsforschungsgruppe »Digitale Souveränität Jugendlicher« an der Friedrich-Alexander-Universität Erlangen-Nürnberg. Ihre Arbeitsschwerpunkte liegen im Bereich der Sozialisation in einer

mediatisierten Welt, der Kinder- und Jugendmedienforschung und der Relationalität von Medienpraktiken.

Odzuck, Eva Helene ist habilitierte Politikwissenschaftlerin und vertritt derzeit als Universitätsprofessorin den Lehrstuhl für Politische Philosophie, Theorie und Ideengeschichte an der Friedrich-Alexander-Universität Erlangen-Nürnberg. Sie forscht zur Herausforderung der Demokratie durch emergierende Technologien sowie zur politischen Philosophie und Ideengeschichte des Liberalismus.

Rückert, Christian ist Strafrechtswissenschaftler mit Forschungsschwerpunkten im Bereich der Cyberkriminalität, des Strafprozessrechts, des Europäischen Strafrechts und der IT-Forensik. Er vertritt derzeit die W3-Professur für Deutsches, Europäisches und Internationales Strafrecht, Strafprozessrecht und Wirtschaftsstrafrecht an der Universität Mannheim. Zuvor war er Wissenschaftlicher Mitarbeiter und Habilitand am Lehrstuhl von Christoph Safferling an der Friedrich-Alexander-Universität Erlangen-Nürnberg.

Safferling, Christoph ist Inhaber des Lehrstuhls für Strafrecht, Strafprozessrecht, Internationales Strafrecht und Völkerrecht an der Friedrich-Alexander-Universität Erlangen-Nürnberg. Seine Forschungsschwerpunkte liegen neben dem Völkerstrafrecht und der Juristischen Zeitgeschichte auch im Bereich der Cyberkriminalität. Er ist u.a. Principal Investigator des DFG-Graduiertenkollegs »Cyberkriminalität und Forensische Informatik«.

Sauer, Stefan ist Akademischer Rat an der FAU Erlangen-Nürnberg. Seine Arbeitsschwerpunkte sind Arbeitssoziologie, Gender Studies, Kritische Theorie und Methodologie.

Staples, Ronald ist wissenschaftlicher Assistent an der FAU Erlangen-Nürnberg. Er beschäftigt sich mit dem Wandel von Organisationen, dem Entstehen von Innovationen und damit, wie Digitalisierung Interaktionsordnungen verändert.

Steinbach, Vincent ist wissenschaftlicher Mitarbeiter am Institut für Soziologie an der FAU Erlangen-Nürnberg und Promovierender im Graduiertenkolleg »Das Sentimentale in Literatur, Kultur und Politik«. Seine Interessenschwer-

punkte sind Wissens-, Medien- und Techniksoziologie sowie die Soziologie des Vertrauens.

Tretter, Max ist wissenschaftlicher Mitarbeiter am Lehrstuhl für Systematische Theologie II (Ethik) an der Friedrich-Alexander-Universität Erlangen-Nürnberg. In seiner Forschung setzt er sich ethisch u.a. mit Digitalisierung und Künstlicher Intelligenz auseinander. Einen besonderen Fokus legt er dabei auf die Konzepte der Ungewissheit und Gewissheit, die epistemischen Verschiebungen infolge des Einsatzes von KI- und Digitaltechnologien sowie die normativen Fragen, die sich daraus ergeben.

Politik in der digitalen Gesellschaft

Jeanette Hofmann, Norbert Kersting,
Claudia Ritzi, Wolf J. Schünemann (Hg.)

Politik in der digitalen Gesellschaft

Zentrale Problemfelder und Forschungsperspektiven

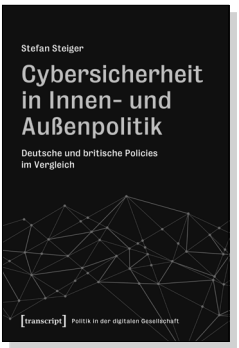
2019, 332 S., kart., 25 SW-Abbildungen
39,99 € (DE), 978-3-8376-4864-5
E-Book: kostenlos erhältlich als Open-Access-Publikation
PDF: ISBN 978-3-8394-4864-9

Kathrin Braun, Cordula Kropp (Hg.)

In digitaler Gesellschaft

Neukonfigurationen zwischen Robotern, Algorithmen und Usern

2021, 318 S., kart., 3 SW-Abbildungen, 22 Farbabbildungen
29,00 € (DE), 978-3-8376-5453-0
E-Book: kostenlos erhältlich als Open-Access-Publikation
PDF: ISBN 978-3-8394-5453-4
ISBN 978-3-7328-5453-0



Stefan Steiger

Cybersicherheit in Innen- und Außenpolitik

Deutsche und britische Policies im Vergleich

April 2022, 322 S., kart., 3 SW-Abbildungen
40,00 € (DE), 978-3-8376-6064-7
E-Book: kostenlos erhältlich als Open-Access-Publikation
PDF: ISBN 978-3-8394-6064-1
ISBN 978-3-7328-6064-7

Leseproben, weitere Informationen und Bestellmöglichkeiten finden Sie unter www.transcript-verlag.de