»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«

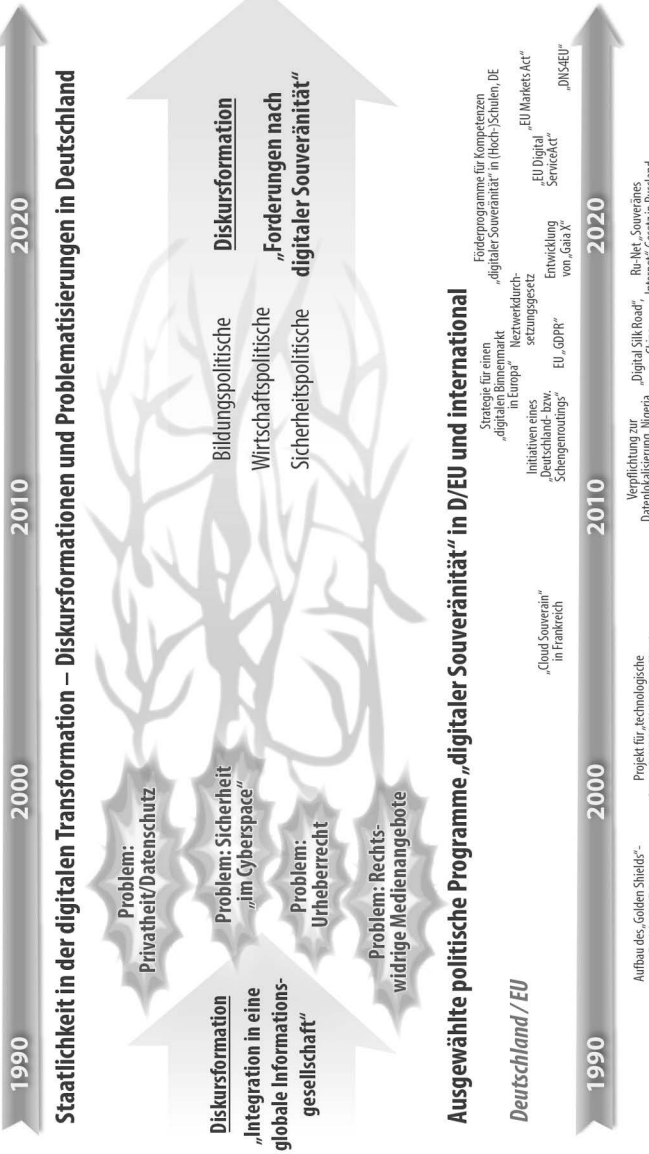
Wie die historische Rekonstruktion öffentlich-politischer Diskurse in Deutschland zeigt, wurden digitale Kommunikationssysteme in den 1990er-Jahren auch in Deutschland in erster Linie als Treiber einer Vernetzung und Überwindung von Grenzen diskutiert. Das Leitbild der »Integration in eine globale Informationsgesellschaft« 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.