Aspekt in den Debatten – sowohl in den Medien als auch auf der politischen Ebene – zu kurz kommt: »Es genügt nicht, über die *Möglichkeiten* künftiger Rechtsverletzungen zu debattieren, ohne die *Wahrscheinlichkeit* zu berücksichtigen, mit der die neuen Technologien eingesetzt werden [Herv. i. O.].« Andererseits spielen Teilimplementationen einzelner Aspekte in die Debatten um den deutschen Staat im digitalen Zeitalter durchaus eine Rolle. Dies wird insbesondere daran deutlich, dass die unter dem Label »Digitale Souveränität« geführten Gestaltungdiskurse in einer doppelten Abgrenzung, einerseits gegenüber der autoritären *Staats*souveränität in China und andererseits der libertären *Markt*souveränität in den USA, geführt werden.

IV.4.3 Vision: Digital souveräner Staat

Wie steht es um die Vision eines digitalen Staates jenseits der dystopischen und utopischen Erzählungen?

> »Auch nach Jahren der wissenschaftlichen, gesellschaftlichen und politischen Debatten über den Megatrend des 21. Jahrhunderts fehlt uns eine klare Richtung, wie die Digitalisierung gestaltet werden soll« (Piallat 2021: 20).

Es verwundert daher nicht, wenn Klenk et al. (2020a: 13) festhalten, dass sich noch keine »positive Vision des Digitalen Staates […] herausgeschält [hat], außer dass er transparent, offen und gut vernetzt sein soll.« Seit Kurzem scheint sich allerdings für den deutschen (aber auch den europäischen) Kontext so etwas wie eine Zukunftsvision des Staates im digitalen Zeitalter herauszukristallisieren – wenngleich die Debatte um das Thema der *digitalen Souveränität* bislang nicht explizit mit dieser Intention geführt wird. Im Folgenden wird argumentiert, dass die digitale Souveränität zwar als analytisches Konzept nicht zu gebrauchen sei, jedoch eine veritable Vision für den Staat im digitalen Zeitalter – im Sinne einer klaren Idee über die Richtung und das Ziel der notwendigen Gestaltung einer offenen Zukunft – und damit ein politisches Leitbild sein könne.

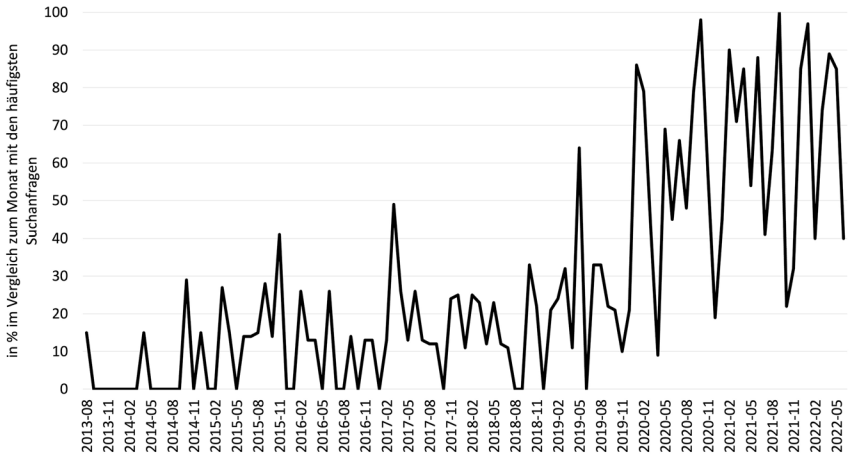
Mit der Vision stehen die Ziele staatlicher Steuerung im Fokus. Gleichwohl stellt eine Zukunftsvision allenfalls eine notwendige aber keinesfalls eine hinreichende Bedingung für gelingende Steuerung dar. Dies wird an den Debatten um die digitale Souveränität deutlich, deren Betrachtung sich allein aufgrund ihrer begrifflich inhärenten Verortung sowohl im Kern des Staatsverständnisses – mit der Souveränitätsfrage – als auch im direkten Bezug zum digitalen Zeitalter geradezu aufdrängt. »Die[] Souveränität ist das eifersüchtig gehütete Zentralmoment des modernen Staates« (Mergel 2019: 258), das im digitalen Zeitalter aus unterschiedlichen Richtungen unter Druck gerät (siehe Kapitel II.2).[23] Damit offenbart die Auseinandersetzung mit dem Digitale-Souveränität-Diskurs zahlreiche Herausforderungen, die mit der Suche nach einer angemessenen und

23 Dies führt Pernice (2020: 224) nicht zuletzt zu einer grundsätzlich kritischen Sicht auf die Nutzung des Begriffs Souveränität im digitalen Kontext: »In der digitalen Konstellation von Souveränität zu sprechen, sei es staatliche Souveränität, digitale Souveränität oder auch Datensouveränität, könnte eine gefährliche Illusion sein, jedenfalls ist es irritierend.«

aus Steuerungsperspektive nützlichen Vision einhergehen können – angefangen bei der Definition des Begriffs.

Dieser ist erst in den letzten Jahren in Deutschland[24] zu einem der neuen, viel gebrauchten und diskutieren, politischen und wissenschaftlichen Buzzwords aufgestiegen. Kaum ein Handbuch oder Sammelband, das Digitalisierung im Titel trägt oder thematisch bearbeitet, kommt darum herum, einen entsprechenden Artikel unterzubringen. Sie finden sich von Pohle (2020a) im »Handbuch Digitalisierung in Staat und Verwaltung«, von Jäger et al. (2022) im Technikfolgeabschätzung-Sammelband »Digitalisierung und die Zukunft der Demokratie«, von Thiel im Band »Politik in der digitalen Gesellschaft« oder gleich doppelt von Pohle und Thiel (2019) sowie Ritzi und Zierold (2019) im Sammelband »Internet und Staat«. Andere Sammelbände wie etwa von Friedrichsen und Bisa (2016) oder Glasze et al. (2022b) tragen »Digitale Souveränität« bereits im Buchtitel.

Abbildung 8: Google Trend zum Suchbegriff »Digitale Souveränität«



Quelle: Google Trends (https://trends.google.de/trends/?geo=DE); Stand: 05.07.2022; eigene Darstellung.

24 Pohle (2021: 8) weist darauf hin, dass der Begriff digitale Souveränität *[digital sovereignty]* insbesondere auf der nationalen und europäischen Ebene gebraucht wird, während er auf der internationalen Ebene seltener Verwendung findet. Dies sei damit zu erklären, dass der Begriff international »nationalstaatlich-isolationistisch besetzt« sei und »autoritären Staaten und Gegnern eines freien, offenen Internets in die Hände spielen könnte.« Auf der europäischen Ebene ist der Begriff eng verbunden mit dem Konzept der *open strategic autonomy (OSA)*. Dieses spiegelt sich zuletzt etwa im *Digital Markets Act (DMA)* (März 2022) und im *Digital Services Act (DSA)* (April 2022) wider. Hierin würde sich eine langsame Abkehr von der neoliberalen Effizienzlogik des Marktes zugunsten von »protecting, transforming, and projecting an increasingly geopoliticized and digitalized single market« abzeichnen (Schmitz/Seidl 2022: 31).

Der Aufstieg des Begriffs begann in Deutschland im Jahr 2013. Kontinuierlich im gesellschaftlichen Diskurs etabliert hat er sich etwa seit den 2020er-Jahren, wenn man die Suche nach »Digitale Souveränität« bei Google zugrunde legt (siehe Abbildung 8).

Wie sich die politische Relevanz des Themas »Digitale Souveränität« entwickelt, zeigen die Plenarprotokolle der Bundestagsreden. Im Plenum taucht der Begriff das erste Mal im November 2013 in einer Rede von Hans Peter Friedrich (CSU), zur Zeit seines Wechsels vom Innenministerposten zum Bundesminister für Ernährung und Landwirtschaft, auf. Dessen Rede fand im Rahmen der Debatte um die von Edward Snowden öffentlich gemachten Abhöraktivitäten der NSA und ihre Auswirkungen auf Deutschland und die transatlantischen Beziehungen statt.

> »Wir können die *digitale Souveränität Europas* nur dann erhalten, wenn es uns gelingt, in der Zukunft die *technologische Souveränität über die Netzinfrastruktur* [Herv. d. A.] und die Netztechnik zu erlangen und zu verstärken« (Deutscher Bundestag 2013a: 45).[25]

Dazu passend konstatiert auch Pohle (2021: 7), dass die »Verwendung des Begriffs der digitalen Souveränität […] in Deutschland mit den Snowden-Enthüllungen 2013 ihren Anfang« nahm. Thomas Oppermann (SPD) formulierte etwas zurückhaltender und unter ausschließlichem Rückgriff auf den Begriff der *technologischen Souveränität*:

> »Unsere Unternehmen erleiden Milliardenverluste durch Industriespionage. Wir können sie nicht effektiv genug davor schützen. Deshalb müssen wir auch über die *Rückgewinnung oder zumindest über die partielle Wiederherstellung technologischer Souveränität* [Herv. d. A.] nachdenken. Das bedeutet sichere Netze, sichere Kommunikation, Verschlüsselung und weitere Vorsorge. Das bedeutet vor allen Dingen mehr Forschung und Entwicklung in diesem Bereich« (Deutscher Bundestag 2013a: 55).

Bereits hier wird eine erste Lesart der digitalen Souveränität als *technologische Unabhängigkeit* im Bereich Infrastruktur sowie Hard- und Software deutlich. Eine zweite Lesart in der Plenardebatte betonte Günther Krings (CDU):

> »Unsere Aufgabe in Deutschland und Europa ist die Rückgewinnung der *digitalen Souveränität im Umgang mit unseren Daten* [Herv. d. A.]. Dazu müssen wir nicht nur rechtliche, sondern auch technische Vorkehrungen und Strategien entwickeln« (ebd.: 58)

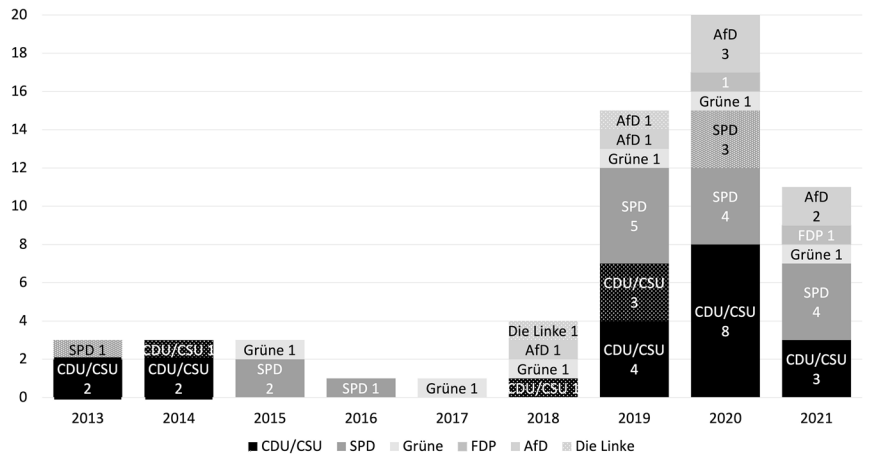
Hierbei erfolgt eine Fokussierung auf die *Datensouveränität* und damit die Ebene der Inhalts-, Dienste- und Netzpolitik. Beide Lesarten lassen sich der *sicherheitspolitischen Dimension* der Debatte zuordnen. Dieser Fokus war 2013 den Snowden-Enthüllungen geschuldet, verbleibt aber auch heute weiterhin einer der beiden Schwerpunkte in den politischen Diskussionen um die Bewältigung der Herausforderung der (Wieder-)Herstel-

25 Das hier angesprochene Ziel staatlicher Souveränität über die Internet-Infrastruktur unterscheidet sich deutlich von dem chinesischen Streben nach »internet sovereignty« (im Sinne einer möglichst vollständigen Nutzer:innenüberwachung sowie Kontrolle über Zugang und Inhalte) (siehe auch Kapitel IV.4.1) oder Russlands Bemühungen um eine abkoppelbares, autarkes russischen Netzwerk (vgl. Pohle/Thiel 2019: 67f.).

lung der digitalen Souveränität der Bundesrepublik. Der zweite Schwerpunkt neben der Sicherheitspolitik liegt weiterhin auf der Wirtschaftspolitik.

Vor der vertiefenden Betrachtung der inhaltlichen Dimensionen des Digitale-Souveränität-Diskurses soll kurz die kongruent zur obigen Google-Suche verlaufende Zunahme der Begriffsnutzung in Bundestagsreden aufgezeigt werden.

Abbildung 9: Anzahl der Redebeiträge im Bundestag, in denen die Begriffe »digitale Souveränität« oder »technologische Souveränität« auftauchen



Anmerkung: Schraffiert = ausschließlich »technologische Souveränität«.
Quelle: OpenDiscourse (https://opendiscourse.de); Stand: 21.05.2021; eigene Darstellung.

Insgesamt findet sich der Begriff der digitalen Souveränität in den Plenarprotokollen des Deutschen Bundestages bis zur 19. Legislaturperiode (Stand: 21.05.2021) in 50 Redebeiträgen.[26] Darunter entfallen vier Reden auf die damalige Kanzlerin Angela Merkel und drei auf Minister (Hans Peter Friedrich, Alexander Dobrindt, Helge Braun). Verstärkt gebraucht wurde der Begriff in Plenardebatten seit 2019, besonders häufig von Politiker:innen der damaligen Regierungskoalition aus CDU, CSU und SPD. Bei Redner:innen aus der CDU/CSU-Fraktion taucht der Begriff in 19 Reden, bei der SPD in 16 Reden auf. Wird die Suche um den inhaltlich nahestehenden Begriff der technologischen Souveränität erweitert, der in drei Redebeiträgen mit der Nennung digitaler Souveränität zusätzlich gebraucht wird, kommen zwölf Reden hinzu, in denen ausschließlich der Begriff der technologischen Souveränität fiel (siehe Abbildung 9).[27]

Eine einfache Auswertung anhand weiterer in den Reden genutzter Begriffe zeigt erste Tendenzen inhaltlicher Schwerpunkte auf. Zum einen dominiert die ökonomische

26 Der Begriff technologische Souveränität findet sich im selben Zeitraum in 15 Redebeiträgen.

27 Zur Einordnung: Der ungleich konkretere und in Digitalstrategien genutzte Begriff der »Blockchain« kommt in 86 Reden (das erst Mal am 18.05.2017), der des »Cyberwar« in 21 Reden (zum ersten Mal am 16.11.2000) und der des »Hackback« in 15 Reden (das erste Mal am 19.04.2018) vor (Stand: 21.05.2021).

Perspektive: Die Begriffe »Wirtschaft« unter »Unternehmen« finden sich in 71 Prozent beziehungsweise 53,2 Prozent der 63 Redebeiträge. Im Vergleich dazu kommen »Bürgerinnen« und »Bürger« in 38,7 Prozent und die »Zivilgesellschaft« nur in 9,7 Prozent der Redebeiträge vor. Zum anderen findet sich in den Reden eher der Begriff »Sicherheit« (59,7 %) als derjenige der (informationellen) »Selbstbestimmung« (3,2 %). Die Kombination aus wirtschafts- und sicherheitspolitischem Fokus könnte mit erklären, weshalb die »USA« (69,4 %) deutlich öfter als »China« (30,6 %) referenziert werden.[28]

Ausgehend vom sicherheitspolitischen Kontext der Debatte durch die Enthüllungen der Geheimdiensttätigkeiten im Internet durch Edward Snowden hat sich der Fokus bis heute deutlich stärker auf das wirtschaftspolitische Feld verschoben. Damit bestätigt sich, was andere Analysen (beispielsweise anhand von Strategiepapieren) für die Debatten in Deutschland und Europa nachgezeichnet haben, nämlich, »dass sich in demokratischen Staaten eine stark wirtschafts- und sicherheitspolitische Sichtweise auf die digitale Souveränität durchsetzt« (Pohle 2021: 8).

> »Die Handlungsempfehlungen und neubegründeten Kompetenzen zielen vorwiegend auf die Sicherung einer zukunftsfähigen digitalen Infrastruktur und die Wettbewerbsfähigkeit der deutschen Wirtschaft und Industrie ab« (Pohle 2020a: 251, siehe auch b: 21).

Für diesen doppelten Fokus lässt sich eine enge Verknüpfung mit der Politik des mittleren Weges konstatieren, die Deutschlands und Europas Perspektive auf digitale Souveränität zwischen den USA und China verortet.

Auf China entfällt die weiterhin vorhandene sicherheitspolitische Dimension. Sie kreist um Themen wie den Aufbau des 5G-Mobilfunknetzes (wo es im Kern um die Nichtbeteiligung des chinesischen Mobilfunkausrüsters Huawei geht) und die Notwendigkeit eigener (europäischer) Kapazitäten in der Mikrochip-Fertigung. Bei dem Aufbau einer solchen Halbleiterindustrie spielen Sicherheitsaspekte jedoch nur eine untergeordnete Rolle. Schwerer wiegt die Abhängigkeit von China in den Lieferketten bei der Just-in-time-Produktion in der Automobilindustrie. Kurzarbeit in deutschen Autokonzernen in der Zeit der Coronapandemie war nicht zuletzt auf fehlenden Teilenachschub aus China zurückzuführen. Gegenüber den USA wiederum dominiert grundsätzlich diese wirtschaftspolitische Dimension. Hierbei geht es insbesondere um den *Plattformkapitalismus* und die Dominanz US-amerikanischer Internet- und Softwarekonzerne, erweitert um die Dimension des *Datenkapitalismus* insbesondere im Rahmen des Hypes um Big Data und Künstliche Intelligenz (KI). Die Abhängigkeit von US-Unternehmen bei der Nutzung von Plattformen und Dateninfrastrukturen wird als zentrales Problem – nicht nur in der individuellen Dimension – wahrgenommen. Denn diese Konzerne »greifen […] in staatliche Aufgabenbereiche ein und unterlaufen deren Fähigkeit zur Selbstregulierung« (Pohle 2021: 6). Daher folgen die Antworten in den Digitalstrategien dieser Problemwahrnehmung. Diese reichen von der Identifikation relevanter Schlüsseltechno-

28 Was sich in den Redebeiträgen im Bundestag nicht findet sind Begriffe wie »autark« oder »Autonomie« – »unabhängig« dagegen kommt in 11,3 % der Reden vor.

logien (KI, Blockchain), in deren Entwicklung investiert[29] und worin eigene nationale und/oder europäische Kompetenzen aufgebaut werden sollen,[30] bis hin zu konkreten europäischen Projekten,[31] etwa im Bereich der Cloud-Alternativen zu Amazon (Amazon Web Services; AWS) oder Microsoft (Azure) mit dem Projekt Gaia-X.[32] Gerade an diesem Beispiel werden jedoch die Herausforderungen überdeutlich. Auf der einen Seite wird die Unabhängigkeit von den übergroßen US-amerikanischen Unternehmen angestrebt. Auf der anderen Seite werden diese in das Projekt – als mögliche Anbieter der technischen Infrastruktur – eingebunden. Unter anderem aus diesem Grund haben sich kürzlich europäische Unternehmen aus dem Projekt zurückgezogen, das allerdings ohnehin seit seiner Initiierung kaum Fortschritte gemacht hat.

Pohle (ebd.: 6f.) verweist darauf, dass es bei dieser Systemfrage nicht nur um technische Aspekte geht, sondern um die »Suche nach einem normativen Rahmen für die europäische und deutsche Digitalpolitik«, einer »eigenständigen digitalen Ordnungspolitik, die sich an europäischen Wertvorstellungen orientiert.« Hierbei geht es um einen Mittelweg zwischen US-amerikanischem Solutionismus und Überwachungskapitalismus auf der einen sowie dem chinesischen digitalen Überwachungsstaat auf der anderen Seite. Daher spielen trotz des Fokus auf der Wirtschaftspolitik im Rahmen der sicherheitspolitischen Betrachtung auch Fragen von Datenschutz, Privatsphäre und Demokratie eine Rolle.[33] Andere Abhängigkeiten von US-Konzernen werden weiterhin eher am Rande diskutiert. Hierzu gehörten insbesondere Datenschutzfragen im Anwendungsbereich,

29 Diese Investitionen in Innovationen haben allerdings kaum etwas mit der Innovationspolitik eines von Mazzucato (2014: 12) »Unternehmerstaat« genannten, intervenierenden Staats zu tun, der »die Wissensökonomie nicht nur fördert, sondern sie mit mutigen Visionen und gezielten Investitionen aktiv schaffen kann.« Dies wird nicht nur an den hierfür von ihr genutzten Begrifflichkeiten von »radikalen, revolutionären Innovationen« und »radikalen Investitionen« unter »extreme[r] Unsicherheit« deutlich (ebd.: 13). Hierbei geht es um mehr als staatliche Fördergelder, öffentliche Innovationsanreize oder den Zusammenhang, dass staatliche Investitionen häufig zusätzliche private Investitionen induzieren. Der Unternehmerstaat erschafft vor allem »die Vision, die Mission und den Plan« (ebd.: 20). Die besondere Rolle des Staates zeigt sich bei Investitionen, die zu Innovationen führen, deren Gewinn für die Allgemeinheit – im Sinne von öffentlichen Gütern – anfällt.

30 Hierzu gehört etwa die 2021 aktualisierte europäische KI-Strategie [*Coordinated Plan on Artificial Intelligence*] (Com/2018/795 final; Com/2021/205 final) (vgl. Europäische Kommission 2021a).

31 So soll etwa mit dem Data Governance Act (DGA) (COM/2020/767 final) im Rahmen der EU-Datenstrategie auf europäischer Ebene ein digitaler Binnenmarkt für Daten geschaffen werden, der unter anderem eine gemeinsame Nutzung von Daten zwischen Unternehmen, öffentlicher Hand, Zivilgesellschaft, Wissenschaft und Privatpersonen vereinfachen und regeln soll (vgl. Europäische Kommission 2020c).

32 Im aktuellen Vision & Strategy Dokument wird Gaia-X nur noch als »open software layer of control, governance, and the implementation of a common set of policies and rules to be applied to any existing cloud/edge technology stack to obtain transparency, sovereignty and interoperability across data and services« beschrieben (Bonfiglio 2021: 2). Damit würde »a framework to configure sovereignty from a digital and technical perspective«, das jedoch keine »political or economic interpretation of sovereignty« umfasst (ebd.: 3).

33 So soll etwa der Digital Services Act (DSA) (COM/2020/825 final) die Felder Datenschutz, Illegale Inhalte und Datengestützte Geschäftsmodelle im Bereich digitaler Dienstleistungen und Plattformregulierung miteinander verbinden (vgl. Europäische Kommission 2020c).

etwa bezogen auf Microsofts Dominanz bei PC-Betriebssystemen und Officeanwendungen (bei Bildungseinrichtungen und in der Verwaltung) oder im Zuge der Coronapandemie bei Videokonferenzlösungen (Zoom, Microsoft Teams).

Wenn man sich von diesem augenscheinlichen politischen Fokus auf sicherheits- und wirtschaftspolitische Aspekte löst, wird eine sehr viel breitere Nutzung des Begriffes der digitalen Souveränität ersichtlich.[34] Die Prominenz des Begriffes trug nicht zu seiner Schärfung bei. Vielmehr findet eine beständige Ausweitung seines Einzugsbereichs statt. Für eine erste Annäherung an eine Systematik des Begriffs digitale Souveränität kann Thiel (2019) herangezogen werden. Er identifiziert drei wissenschaftliche Debattenstränge: zum einen »Souveränität und Territorialität«, worunter die Entgrenzung durch das Internet, Kontrolle über Infrastruktur, Fragen der Rechtsdurchsetzung und die Sicherheitsdimension (Cyberwar) sowie als Antwort aus Steuerungsperspektive Internet Governance und Multi-Stakeholder Governance fallen. Im Strang der »Souveränität und Herrschaftsansprüche« geht es um die global agierenden Digitalunternehmen, die als private Herrschaftsakteure und Datenmachtmonopole staatliche Souveränität infrage stellen – und aus Steuerungsperspektive zu einer »Hybridisierung« führen, wenn staatliche Durchsetzungsmacht private Akteure nutzt oder gar auf diese angewiesen ist (ebd.: 53). Der dritte Strang der »Souveränität und demokratischen Selbstbestimmung« rückt dagegen nicht den Staat, sondern die Bürger:innen und damit individuelle und kollektive Selbstbestimmung in den Fokus.

Dieser *inhalts*bezogenen Dreiteilung lässt sich eine *akteurs- beziehungsweise ebenenbezogene* Dreiteilung gegenüberstellen. Während Erstere die Felder aufzeigt, *wo* Souveränität erreicht werden soll, fragt Letztere danach, *wer* souverän sein soll, beziehungsweise um *wessen* Souveränität es geht. Hilfreich ist hierbei die unter anderem von Pohle (2020b: 15ff.) aufgemachte Unterteilung in drei Ebenen: *staatlich* (Makroebene) (wobei hier noch einmal die nationale von der supranationalen Ebene unterschieden werden kann), *wirtschaftlich* (Mesoebene) und *individuell* (Mikroebene).[35] Diese Unterteilung lenkt darüber hinaus den Blick auch auf die Schnittstellen zwischen den Ebenen. Hierbei stellt sich dann die Frage nach (In-)Kompatibilitäten zwischen der digitalen Souveränität der Einzelebenen. So stellen die Grundrechte zunächst einmal Abwehrrechte der Bürger:innen (Mikroebene) gegenüber dem Staat (Makroebene) dar, insofern steht hier die digitale

34 Pohle (2021: 7) erkennt drei Tendenzen in der Entwicklung der Debatte und Nutzung des Begriffs: Diese differenziert sich konzeptionell aus, erhält eine stärker normative Prägung und entwickelt sich über ein allein auf den Staat bezogenes Verständnis von Souveränität hinaus. Insbesondere gerät die Zivilgesellschaft stärker in den Blick. Neben den Aspekt der staatlichen Souveränität im Sinne von *Autonomie* tritt daher die individuelle Souveränität im Sinne der *Selbstbestimmung* in digitalen Belangen.

35 Diese Einteilung ist deckungsgleich mit der Dreiteilung in Staatssouveränität, Marktsouveränität und Bürger:innensouveränität. Falk und Schroeder (2022: 4f.) dagegen sprechen auf der Mesoebene von der *kollektiven* statt der *wirtschaftlichen* Dimension. Ebenso unterteilen Glasze et al. (2022a: 8) zwischen Staat, Subjekt und nicht-staatlichen Organisationen. Diese Einteilung bringt jedoch die Schwierigkeit mit sich, dass auf der kollektiven Mesoebene sowohl Unternehmen als auch Bürger:innenrechtsorganisationen verortet werden müssten, wobei die von Letzteren vertretenen Souveränitätsinteressen jedoch eigentlich auf die individuelle Mikroebene abzielen.

Souveränität des Einzelnen möglicherweise in einem Spannungsverhältnis zu staatlichen Interessen, wie es sich etwa in den Debatten um den Umgang mit Gesundheitsdaten (siehe Kapitel V.1.3.4) oder die Datenschutzgrundverordnung (DSGVO) zeigt.

Gleiches gilt aber auch für die Mikro- und Mesoebene. Auch hier kann, wie das Beispiel Beschäftigtendatenschutz verdeutlicht, die digitale Souveränität des Unternehmens (Mesoebene) – im Sinne der selbstbestimmten Erhebung und Verfügung über (Produktions-)Daten – im Widerspruch oder zumindest Spannungsverhältnis zur digitalen Souveränität der Beschäftigten (Mikroebene) stehen. Noch viel deutlicher wird es an der von Zuboff (2018) als Überwachungskapitalismus bezeichneten Ausbeutung individueller Verhaltensdaten durch Digitalkonzerne, bei der diese ihrer Souveränität über ihre Plattform auf Kosten der Souveränität der Plattformnutzer:innen ausnutzen (siehe Kapitel IV.4.2). Andererseits geht eine Wahlmöglichkeit der genutzten Hard- und Software von Beschäftigten (etwa »*bring your own device*«; byod), als eine Form von individueller digitaler Souveränität, zulasten der Souveränität des Unternehmens (insbesondere in Sicherheitsaspekten). Aber auch wenn eine theoretische Wahlmöglichkeit besteht, kann diese in der Realität stark beschnitten oder quasi nicht vorhanden sein. Im Arbeitsumfeld sind viele auf die Nutzung von Microsoft Office angewiesen (größere Wahrscheinlichkeit für einheitliche Formatierung und problemloser Dateiformataustausch) und können somit nicht selbstbestimmt Open-Source-Alternativen wie beispielsweise LibreOffice nutzen.

Ein Schwerpunkt der Debatte um die digitale Souveränität des Staates wiederum konzentriert sich auf das Verhältnis zwischen der staatlichen Regulierungsfähigkeit (Makroebene) und transnational agierenden Digitalkonzernen (Mesoebene). Bei der technisch-architektonischen Implementierung der Corona-Warn-App bestand staatlicherseits zwar die Wahlmöglichkeit zwischen zwei Konzepten (zentral vs. dezentral). Die theoretischen, zentralen Wahlalternativen wurden jedoch infolge der Vorauswahl des unterstützten Verfahrens durch die maßgeblichen Infrastrukturanbieter (Mobiltelefonbetriebssysteme) Google und Apple obsolet, da damit eine effektive Implementierung aussichtslos wurde. Diese beiden US-Konzerne nutzten ihre digitale Souveränität über die von ihnen gepflegte Infrastruktur also zulasten der Souveränität der Nationalstaaten (siehe Kapitel V.1.4.1). Zugleich hätten im deutschen Fall die staatlichen Akteure (Makroebene), wenn sie sich mit der Umsetzung des von ihnen ursprünglich favorisierten zentralen Konzepts durchgesetzt hätten, die staatliche digitale Souveränität auf Kosten der digitalen Souveränität der Bürger:innen (Mikroebene) über ihre Daten (im Sinne der Datensparsamkeit und des Datenschutzes) durchgesetzt. Somit sind die Handlungsspielräume auf den drei Ebenen niemals deckungsgleich – vielmehr hängen sie vielfach in einem Nullsummenspiel voneinander ab.

Dies wird auch an den von Falk und Schroeder (2022: 4ff.), die digitale Souveränität als Voraussetzung dafür verstehen, Handlungsspielräume zu erkennen und diese eigenständig und selbstbestimmt zu nutzen, verwendeten Kategorien zur Definition von digitaler Souveränität deutlich: *Dürfen* (Entscheidungsbefugnisse sind vorhanden), *Können* (alternative Möglichkeiten stehen zur Auswahl; Entscheidungs- und Handlungskompetenzen sind vorhanden) und *Wollen* (Motivation ist vorhanden). Wenn das Dürfen primär über die (nicht) vorhandenen Entscheidungsbefugnisse definiert wird, dann besteht hier automatisch ein Konkurrenzverhältnis um eben diese Zuständigkeiten und Befugnisse.

Auch für Nationalstaaten und Systemvergleiche ist diese Dreiteilung fruchtbar. So kann China ein erhebliches Maß an staatlicher digitaler Souveränität zugestanden werden, die das Land durch hierarchische Maßnahmen und Instrumente auf der infrastrukturellen bis hin zur individuellen Ebene sicherstellt (von der Great Firewall bis zum Social Credit System). Auch die zuletzt getroffenen Maßnahmen gegen große chinesische Plattformen (wie Tencent) verdeutlichen den absoluten Anspruch und Vorrang staatlicher Souveränität (Makroebene) gegenüber Mark (Mesoebene) und Bürger:innen (Mikroebene). In den USA dagegen konnte sich eine starke digitale Souveränität der Techkonzerne (Mesoebene) sowohl gegenüber dem Staat (Makroebene) als auch den Nutzer:innen (Mikroebene) herausbilden.

An diesen Beispielen wird sehr deutlich, dass die Souveränität von Akteuren auf der einen Ebene häufig die Souveränität von Akteuren auf den anderen Ebenen einschränkt. Die hier sichtbar werdenden Spannungsverhältnisse zwischen den drei Ebenen lassen sich nicht einfach auflösen. Wechselseitig bedingte und beschränkte Handlungsspielräume betreffen zwar auch Akteure einer einzelnen Ebene (etwa welche staatliche Institution die Entscheidungsbefugnisse für einen bestimmten Bereich der Digitalpolitik erhält; siehe Kapitel II.3.2). Insbesondere stellt sich aber die Frage, wie das Souveränitätsniveau (relativ) von Akteuren einer Ebene im Verhältnis zur Souveränität von Akteuren der jeweils anderen Ebenen (relational) austariert wird. Daher lässt sich konstatieren, dass es sich bei der digitalen Souveränität um ein *relatives und relationales Konzept* handelt.

Dieser Aspekt findet sich jedoch in keiner Definition. Vielmehr lesen sich diese häufig so, als würde es gar kein Spannungsverhältnis geben.

> »Digitale Souveränität bedeutet also die kollektive Souveränität als Handlungs- und Gestaltungsfähigkeit des Staates und der Wirtschaft, zugleich aber auch die individuelle Souveränität, verstanden als Autonomie und selbstbestimmte Handlungsfähigkeit des Individuums in einer vernetzten Welt« (Pohle 2021: 8).

Darüber hinaus besteht das Problem, dass sich zwar ein gemeinsamer Kern aus den unterschiedlichen Definitionen herausarbeiten lässt, der sich um Begriffe wie Unabhängigkeit, Autonomie und Selbstbestimmung von Akteuren in der digitalen Welt dreht. Um wessen Souveränität, um welche Herausforderungen und damit auch um welche Ziele es geht, variiert jedoch erheblich.

Die Schwierigkeit beim Konzept der digitalen Souveränität besteht daher darin, dass dieses erst inhaltlich spezifiziert und aufgeladen werden muss. Der Erfolg des Begriffs mag gerade damit zusammenhängen, dass sich darunter jede:r etwas anderes vorstellen kann und er zugleich immer eine positiv besetzte (Ziel-)Perspektive beinhaltet.[36] Wer würde schon für digitale Abhängigkeit plädieren? Bei der Nutzung des Begriffs kann daher die Gefahr negativen Feedbacks oder kontroverser Debatten stark verringert werden.

36 Trotz positiver Perspektive wohnt dem Begriff zugleich eine negative Grundprämisse inne: Wenn digitale Souveränität als erstrebenswertes und erwünschtes Ziel ausgegeben wird, framet dies den Status quo unweigerlich als eine Situation der digitalen Abhängigkeit, aus der es zu entkommen gilt.

Zugleich bleibt digitale Souveränität damit häufig inhaltsleer, zumindest aber unkonkret. Somit handelt es sich weniger um ein Konzept als um eine *Chiffre* oder einen *Kofferbegriff*, angereichert mit wenigen geteilten Grundbegriffen, aber ansonsten offen für unterschiedliche konkrete Vorstellungen und zu erreichende Ziele.

Besonders deutlich wird dies in einer diskursanalytischen Untersuchung der deutschen Debatten um digitale Souveränität,[37] in der Lambach und Oppermann (2022) insgesamt sieben unterschiedliche Narrative identifizieren konnten. Stellenweise überlappen diese sich, teilweise verfolgen sie aber auch gegensätzliche politische Agenden. Am häufigsten (in 39 von 63 Dokumenten) fanden die Autoren das Narrativ der wirtschaftlichen Prosperität vor. In einem Drittel der Dokumente (20) folgte das Sicherheitsnarrativ. Die weiteren Narrative in absteigender Reihenfolge waren: Europäischer Way of Life (18), Datenschutz (15), Moderner Staat (11), Verbraucherschutz (9) und Demokratisches Empowerment (8) (vgl. ebd.: 6).[38] Aufgrund der inhaltlichen Nähe und des häufig gleichzeitigen Vorkommens fassen Lambach und Oppermann (ebd.: 7ff.) das Daten- und Verbraucherschutznarrativ sowie das Narrativ des demokratischen Empowerments unter der Kategorie des individuellen Empowerments zusammen.[39] Die besondere Rolle des Narratives der wirtschaftlichen Prosperität wird nicht nur an der Häufigkeit seines Vorkommens deutlich, sondern auch daran, dass dieses Narrativ als einziges in Kombination mit allen anderen Narrativen (mit einer Wahrscheinlichkeit von 63 %) vorkommt. »Um die nötigen Kräfte für das große Vorhaben der digitalen Transformation zu mobilisieren, Verpflichtungen plausibel zu machen und das Tempo zu erhöhen, braucht es jedoch ein gemeinsames Narrativ«, das eine breite Unterstützung unterschiedlicher Akteure generiert (Falk/Schroeder 2022: 2).

Trotz des heterogenen Verständnisses des Begriffes – insbesondere in der Frage, um wessen Souveränität es geht – aufgrund dessen sich die Narrative unterscheiden, heben Lambach und Oppermann (2022: 14) gleichwohl einen positiven Aspekt besonders hervor:

> »[T]he interpretive flexibility of digital sovereignty makes the concept a poor guide for policymaking. […] Arguably, the main value of digital sovereignty lies not in policy or governance but rather in politics – as a useful tool for organizing political coalitions«.

37 Grundlage der Untersuchung war ein Textkorpus aus 63 zwischen 2010 und 2021 erschienenen Dokumenten von staatlicher, zivilgesellschaftlicher und wirtschaftlicher Seite.

38 Für die englischsprachige Literatur nennt Süß (2022: 5) sechs unterschiedliche Bezugskonzepte der Debatten um digitale Souveränität: die Unabhängigkeit des Cyberspace, digitale Staatssouveränität, die Datensouveränität indigener Völker, die technische Souveränität sozialer Bewegungen sowie den commonsbasierten Souveränitätsansatz.

39 Dieser auf die individuelle Souveränität und digitale Bürger:innenrechte fokussierte Teil der Debatte um digitale Souveränität ist kennzeichnend für den deutschen (im Unterschied zum europäischen) Diskurs und bringt die konfliktträchtigere Dimension zwischen staatlicher und individueller Souveränität mit sich. Bei der Souveränitätsabwägung zwischen Staat und Unternehmen (zugunsten des Staates) sowie Unternehmen und Individuen (zugunsten der Individuen) lässt sich in der Regel ein Konsens auch zwischen Akteuren unterschiedlicher Ebenen einfacher herstellen.

Hieran anschließend ist digitale Souveränität zwar als (wissenschaftliches) Konzept wenig hilfreich, die Chiffre der digitalen Souveränität könnte jedoch eine veritable Vision des Staates im digitalen Zeitalter darstellen.

Auch Falk und Schroeder (2022: 1f.) sehen im Begriff der digitalen Souveränität das Potenzial für einen »politische[n] Leitgedanke[n]«, der dem Mangel an einem »belastbaren strategischen Rahmen« mit »klaren Zielvorgabe[n] […] und kompetente[r] Umsetzungsperspektive« begegnen könnte. Das Konzept der digitalen Souveränität, verstanden als »politisches, wirtschaftliches und gesellschaftliches Leitbild«, bietet »eine normative und strategische Grundorientierung, um in gesellschaftlichen und globalen Deutungskonflikten die Position einer nachhaltigen und demokratischen Digitalpolitik plausibler auszurichten« (ebd.: 10).

Ein solches Narrativ beschreibt die aktuellen Herausforderungen (Warum) und die Vision einer erwünschten Zukunft (Was), skizziert den Weg dorthin (Wie) und treibt die Umsetzung der notwendigen Schritte voran, indem es die relevanten Akteure integriert (Wer). Im Rahmen der Chiffre der digitalen Souveränität ist ein solches Narrativ möglich, da sowohl der Kern der Problemdiagnose als auch die grundsätzliche Richtung der nötigen Veränderungen vielfach eher konkurrierend als konfligierend verlaufen. Insofern liegt diese als Vision eher auf einer Ebene mit dem starken oder schlanken Staat, als dass sie ein klar erkennbares Schema der erwünschten Zukunft visualisieren würde. Viele Details bleiben mithin offen beziehungsweise werden nicht vorgegeben. Damit hat diese Chiffre nicht nur das Potenzial, unterschiedliche Akteure hinter sich zu versammeln, die die Details aus ihrer jeweiligen Interessenlage heraus individuell ausfüllen, sondern bietet auch kommunikatives Interaktionspotenzial.[40] Zugleich ist die Vision der digitalen Souveränität offen und flexibel. Sie lässt sich sowohl an unerwartete Hindernisse auf dem Weg anpassen als auch im Modus von Kooperation, Verhandlung und Konsens – ausreichende Kompromissfähigkeit der relevanten Akteure vorausgesetzt – mit konkreten Zielpunkten und Umsetzungsprozessen hinterlegen. Die digitale Souveränität ist also als analytisches Konzept (aufgrund ihrer Unbestimmtheit) wenig hilfreich, als politische Leitbild für den Staat im digitalen Zeitalter dafür umso mehr. Gleichwohl ist damit der notwendige Schritt von der Vision zur Konkretisierung noch nicht getan.

Am Beispiel der politisch häufig verkürzten Debatte um digitale Souveränität zeigt sich deutlich, dass es alles andere als trivial ist, eine konstruktive und realistische Zukunftsvision zu entfalten, von der sich konkrete Steuerungsziele ableiten lassen, die dann wiederum eine begründete Auswahl an Steuerungsinstrumenten erlauben.[41]

---

40 Lambach und Oppermann (2022: 13) kommen in ihrer Analyse der deutschen Diskurse um digitale Souveränität zu dem Schluss, dass das Konzept nicht *trotz* der Existenz der von ihnen identifizierten sieben Narrative so erfolgreich geworden ist, sondern *wegen* der sich zwar teilweise widersprechenden, aber auch überlappenden und damit aufeinander beziehbaren Narrative: »These narrative qualities of ›digital sovereignty‹ and the interpretive flexibility of the concept make it an attractive focal point for the political projects of actors from many different policy fields and political camps.«

41 Kontraproduktiv sind daher eine Vision, die »vollkommen entkoppelt dasteht und es keine sinnvollen Verbindungslinien vom Hier und Jetzt zum utopischen Übermorgen gibt« (Friesike/Sprondel 2022: 23).

Steuerungsfähigkeit in komplexen Kontexten bedarf jedoch aus mindestens zwei Gründen einer Vision: Zum einen können Zielbestimmungen als einfache Ableitungen von mehreren identifizierten Einzelproblemen (also die einfache Umkehrung ungewollter Zustände als) wicked problems nicht gerecht werden. Zum anderen ergeben sich aus ambiguen Herausforderungen keine zwingenden Perspektiven und damit kein alternativloser Handlungshorizont. Stattdessen ist die Zukunft kontingent, und erwünschte Zukünfte können sich zwischen Akteuren unterscheiden. Wie könnte ein deutsches Leitbild der digitalen Souveränität aussehen, wenn diese konsequent als drittes Modell – in der Tradition des mittleren Weges – neben dem staatlichen Modell Chinas (Makroebene) und dem wirtschaftlichen Modell der USA (Mesoebene) gedacht werden würde?

In einer solchen Perspektive stände die digitale Souveränität der Bürger:innen auf der Mikroebene im Fokus, die von zahlreichen zivilgesellschaftlichen Organisationen insbesondere in die deutsche Debatte um digitale Souveränität eingebracht worden ist *(wollen)*. Für alle anderen Akteure und Ebenen würde gelten: so viel digitale Souveränität wie möglich, ohne dabei diejenige der Bürger:innen zu beschneiden. Dem Staat käme dann, neben der Sicherstellung des Primats der Bürger:innen-Souveränität *(dürfen)*, insbesondere die Aufgabe zu, dafür Sorge zu tragen, dass die Bürger:innen dazu in die Lage versetzte werden, ihre Souveränität auch wahrzunehmen *(können)*. Dies beinhaltet insbesondere die Stärkung der *digital literacy*, damit zwischen bestehenden Wahlmöglichkeiten auch tatsächlich durch selbstbestimmte (und damit mit einem für das Abwägen nötigen Wissen) Entscheidungen eine (begründete) Auswahl getroffen werden kann. Genauso gehört aber auch die Regulierung von Plattformen dazu, damit diese nicht einseitig Auswahlmöglichkeiten vorenthalten oder *dark pattern* zur Lenkung von Nutzer:innen-Entscheidungen verwenden.

Wenn ein solcher Konsens über den Primat digital souveräner Bürger:innen bestehen würde, verschöbe sich auch die ewig gleiche Debatte beispielsweise über Datenschutz vs. Wirtschaftsinteressen. Denn aus einer solchen Konsensperspektive kann aus der *Frontstellung* vermeintlicher Gegensätze – Datenschutz *oder* Datenwirtschaft – eine *Fragestellung* werden: Wie lässt sich Datenwirtschaft mit Datenschutz vereinbaren? So kann ein Nachdenken über wirklich innovative Geschäftsmodelle forciert werden, anstatt die Tendenz zu befördern, Alternativen zu »entwickeln«, bei denen einfach die Modelle US-amerikanischer Unternehmen kopiert werden. Genauso kann gefragt werden, wie die Bereitschaft von Bürger:innen zu Datenspenden gesteigert werden kann, inwiefern Nutzer:innen in der Lage sein sollten, selbst ihr Daten zu vermarkten (und wie man sicherstellen kann, dass sie dies verantwortungsvoll und mit Überblick über die Konsequenzen tun).

Bislang scheinen allerdings weiterhin ökonomische und sicherheitspolitische Erwägungen zu überwiegen. Diese kumulieren in den Feldern der Technologiesouveränität[42] (der nationalen beziehungsweise europäischen Unabhängigkeit etwa bei Schlüsseltechnologien und Mikrochips) sowie einer Datensouveränität, bei der primär deren Potenziale für Innovation und Wachstum (für Wirtschaft, Gesundheit etc.) gehoben

42 Für ein Konzept von Technologiesouveränität siehe etwa Edler et al. (2020).

werden sollen. Und auch in der Sicherheitsdimension werden Kontrolle und Überwachung sowohl nach außen (Schutz kritischer Infrastruktur) als auch nach innen (Staatstrojaner) priorisiert. Es ist daher bezeichnend, wenn es acatech im Impulspapier zum Status quo und zu den Handlungsfeldern digitaler Souveränität ausschließlich um den »globale[n] Wettlauf im industriellen Sektor«, »Innovationsfähigkeit« sowie »neue[] Wertschöpfung« geht und der Fokus auf Technologie und Daten liegt (Kagermann et al. 2021: 8). Die individuelle Dimension demokratischer digitaler Souveränität kommt allenfalls indirekt zum Ausdruck, wenn vereinzelt diffus auf eine Orientierung an europäischen Werten verwiesen wird. Dies spiegelt sich auf Bundesebene auch in aktuellen Strategiedokumenten der Ampelkoalition wider. Das Innenministerium stellte seine digitalpolitischen Ziele und Maßnahmen bis 2025 unter dem Titel »Digitales Deutschland – Souverän. Sicher. Bürgerzentriert« vor, wobei der Begriff »Digitale Souveränität« konkret bei zwei der fünf vom BMI (2022a: 8, 10) fokussierten Themenfeldern auftaucht: bei der Cybersicherheitsarchitektur und bei den interoperablen Infrastrukturen.

Tabelle 9: Häufigkeit von Begriffen zur digitalen Souveränität in der Digitalstrategie 2022 der Ampelkoalition

Souveränitätsbezug in den Handlungsfeldern	Vernetzte und digital souveräne Gesellschaft	Innovative Wirtschaft, Arbeitswelt, Wissenschaft und Forschung	Lernender, digitaler Staat
Bürger:innen/Verbraucher:innnen/ Patient:innen (Datensouveränität)	5		
Nutzer:innen (Datensouveränität)		3	
Technologisch/Infrastruktur		3	1
EU/Binnenmarkt		1	2
(Cyber-)Sicherheit			3
Verwaltung(sdigitalisierung)			5
Übergreifend	2	1	1
Insgesamt	**7**	**8**	**12**

Quelle: BMDV (2022a); eigene Zusammenstellung und Darstellung.

In der im September 2022 von der Ampelkoalition verabschiedeten Digitalstrategie finden sich auf 52 Seiten ganze 48 Mal Begriffe wie »digitale Souveränität« oder »digital souveräne Gesellschaft« (vgl. BMDV 2022a). In den drei Handlungsfeldern der Strategie überwiegt die Nutzung der Begriffe im Kontext von Verwaltung, Sicherheit und Wirtschaft. Zwar spielt das Thema Datensouveränität auch wirtschaftsbezogen eine Rolle, hier allerdings aus der Perspektive auf Nutzer:innen in einer zu stärkenden Datenökonomie. Nur im Handlungsfeld »Vernetzte und digital souveräne Gesellschaft« steht die Souveränität von Bürger:innen, Verbraucher:innen und Patient:innen (auch hier häufig mit dem Fokus auf Datensouveränität) im Mittelpunkt (siehe Tabelle 9). Dabei fand das

Unterkapitel »Digitale Zivilgesellschaft«, das auf Teilhabe und »digitale Souveränität der Gesellschaft« abzielt, erst nach Bekanntwerden des ersten Entwurfs im Juli 2022 noch nachträglich Eingang in die Strategie.

Ein konsistentes, bürger:innenorientiertes digitales Souveränitätsverständnis als deutscher (und europäischer) dritter Weg jenseits der chinesischen Staatssouveränität und der US-amerikanischen Marktsouveränität konnte sich bislang also nicht herausbilden, was auch die nachfolgenden Fallbeispielen zeigen.