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

Max Tretter

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

1. Einleitung

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

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

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

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

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

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

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

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

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

2. Methoden

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

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

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

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

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

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

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

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

3. Ergebnisse

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

3.1 Zentrale Akteur*innen und Kontexte »digitaler Souveränität«

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

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

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

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

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

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

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

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

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

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

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

3.2 Formen der digitalen Kontrollausübung im Kontext »digitaler Souveränität«

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

Ausbau der digitalen Infrastruktur

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

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

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

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

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

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

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

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

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

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

»Digitale Kontrolle« durch Gesetzgebung

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

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

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

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

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

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

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

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

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

»Digitale Kontrolle« durch Zensur, Friction und Flooding

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

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

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

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

Kontrolle durch digitale Grenzziehung

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

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

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

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

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

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

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

4. Diskussion

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

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

4.1 Zusammenwirken der verschiedenen Formen digitaler Kontrollausübung

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

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

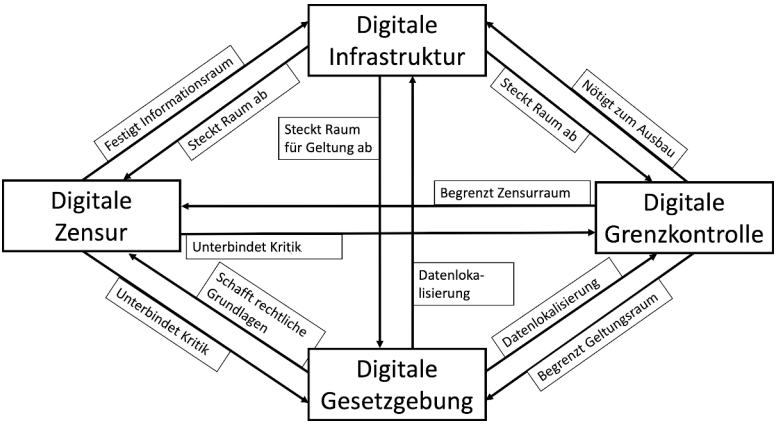
Gleichzeitig deutet Ristolainen (ebd.) an, dass die verschiedenen Formen »digitaler Kontrolle« zusammenwirken, wenn er aufzeigt, dass jede *Ausübung* »digitaler Kontrolle« in instrumenteller Weise (»through«, »by«) gleichsam andere Formen »digitaler Kontrolle« *ermöglichen* und *fördern* kann. Diesen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

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

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

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

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



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

4.2 Limitationen der Untersuchung

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

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

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

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

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

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

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

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

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

4.3 Ethische Einschätzung

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

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

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

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

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

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

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

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

5. Fazit

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

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

Literaturverzeichnis

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

Jurnal Politik Internasional 21 (2), S. 262, https://doi.org/10.7454/global.v21i2.412.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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