

Inhalt

Digitalisierung und Internationale Politische Ökonomie	7
<i>Andreas Busch</i>	

Digitalisierung und Internationale Politische Ökonomie

Andreas Busch

Einleitung und Überblick

Eine der herausragenden Entwicklungen in der globalen Wirtschaft der letzten etwa drei Jahrzehnte ist ihre Digitalisierung und mit ihr die zentrale Rolle, die Daten einnehmen. Das ist, angesichts der längst zum Standard gewordenen Nutzung des Internet auch durch Privatpersonen, eine weit geteilte Alltagserfahrung. Erst Zahlen über die Nutzung von digitalen Daten machen aber deutlich, in einem wie stark steigenden Maß diese in der digitalen Ökonomie eine zunehmend wichtige Rolle spielen. So steigt das Datenvolumen des globalen *Internet Protocol (IP) traffic* anhaltend erheblich an: in der kurzen Zeit zwischen 2017 und 2022 kam es zu einer *Verdreifachung* des Volumens; der weltweite IP-Verkehr wird *allein im Jahr 2022* den gesamten bis 2016 stattgefundenen Internet-Verkehr übersteigen, und die Zahl der mit dem Internet verbundenen Geräte wird 2023 etwa das Dreifache (!) der Weltbevölkerung betragen (UNCTAD 2021: 16f.). Auch in der Unternehmenswelt haben diese Änderungen tiefe Spuren hinterlassen. Waren (nach Marktkapitalisierung) vor 25 Jahren die fünf größten Unternehmen noch in als traditionell industriell zu kennzeichnenden Bereichen tätig (General Electric; Royal Dutch Shell; The Coca-Cola Company; Nippon Telegraph & Telephone und ExxonMobile), so zeigt die entsprechende Liste für Ende 2020 eine fast völlige Dominanz von Unternehmen aus der digitalen Ökonomie (Apple; Microsoft; Alphabet (Google); Amazon und Tesla). Darin spiegelt sich die massive Ausweitung digitaler Angebote hinsichtlich Zahl der Nutzer und Dauer der Nutzung: 2019 haben zwischen 70 und 95 Prozent der Erwachsenen in OECD-Ländern das Internet genutzt, und zwischen 2014 und 2019 ist die tägliche Nutzung im Schnitt um 30 Minuten gestiegen (OECD 2020: 13f.). Auch wenn es zwischen Ländern und Bevölkerungsgruppen fortbestehende Unterschiede gibt, so ist die Nutzung von Daten schon seit längerem ein Treiber ökonomischer Aktivität (vgl. Busch 2019: 28ff.) und mittlerweile so groß, dass 34 OECD-Länder eine Nationale Digitalstrategie haben, um Politikkoordination auf höchster Regierungsebene sicherzustellen (OECD 2020: 13).

Gleichzeitig haben digitale Daten jedoch eine Reihe von Besonderheiten, die ihre Einbeziehung in die ökonomische Analyse erschweren. So legt eine genauere Betrachtung nahe, dass sie anders als gewöhnliche Güter und Dienstleistungen behandelt werden sollten. Denn die datengetriebene digitale Wirtschaft stellt auch Konzepte wie „Eigentum“ und „Souveränität“ in Frage. Es kommt in diesem Bereich mehr darauf an, wer welche Rechte auf Zugang, Verfügung und Nutzung von Daten hat als auf das Eigentum an ihnen (UNCTAD 2021: xvii). Und es gibt Spannungen zwischen dem territorial basierten Konzept nationaler Souveränität sowie dem grenzenlosen digitalen Raum, in dem Daten zirkulieren (ebd.; s.a. schon Busch/Plümper 1999). Weiter erschwerend kommt hinzu, dass keine offiziellen Statistiken existieren, es keine allgemein anerkannten Definitionen für Daten gibt und die Ansätze hinsichtlich des Feldes zwischen den wichtigsten geopolitischen Akteuren deutlich differieren (s.u.).

Diese Schwierigkeiten mögen dazu beigetragen haben, dass in der akademischen Analyse der Internationalen Politischen Ökonomie das Thema der Digitalen Politischen Ökonomie bisher relativ wenig behandelt worden ist (vgl. Farrell/Newman 2019: xiii). Dies wird etwa deutlich, wenn man auf Werke blickt, deren Ziel die Zusammenfassung des Standes des Feldes ist. Das 2009 erschienene und von Mark Blyth herausgegebene „Routledge Handbook of International Political Economy“ sieht das Feld als „global conversation“ und fokussiert weniger auf spezifische Themen als auf die jeweiligen Perspektiven an unterschiedlichen Orten – Nordamerika, Großbritannien, Asien und „elsewhere“.¹ Auch das Handbuch zur „International Political Economy“ von Phillips/Weaver (2011) richtet den Blick v.a. auf „debating the past, present and future“ mit ähnlichen theoretischen Schwerpunkten und betreibt hauptsächlich Introspektion angesichts eines als zersplitternd empfundenen Feldes (übrigens kommt im gesamten Werk das Wort „digital“ nicht einmal vor). Das neueste Werk in diesem Feld (das von Ernesto Vivares (2020) herausgegebene Handbuch der „Global Political Economy“) widmet sich ebenfalls mit großer Ausführlichkeit den fachinternen Debatten und Abgrenzungen, enthält aber auch einen ausführlichen Teil zu „new research arenas“. In diesem wird auch das Thema „cyberpolitics“ aufgegriffen, allerdings ausschließlich mit Blick auf den „Global South“ und dem Ziel der Erstellung einer

1 Siehe das Inhaltsverzeichnis in Blyth (2009: v-vi). Der starke Theoriefokus erinnert an ein anderes Handbuch aus dem Bereich Internationale Beziehungen, in dem 19 von 44 Kapiteln sich „major theoretical perspectives“ widmen (Reus-Smit/Snidal 2008).

Forschungsagenda (Vila Seoane/Saguier 2020). Das ist bedauerlich, gehört der „Global South“ doch zu den Teilen der Welt, in denen das Thema der Digitalisierung eher marginal ist (ebd.: 714). Da der Bereich der datengetriebenen digitalen Wirtschaft jedoch durch starke Konzentration auf die USA und China gekennzeichnet ist (vgl. UNCTAD 2021: xv), nimmt der erwähnte Beitrag somit eine sehr enge Perspektive ein. Überblicksliteratur im angesprochenen Themenbereich, so können wir schließen, findet sich also in zusammenfassenden Werken zur Internationalen Politischen Ökonomie bis jetzt nicht.

Der folgende Beitrag kann dies schon aus Platzgründen ebenfalls nicht leisten. Was er anstrebt, ist, durch einen Überblick über die wichtigsten Fragen und Themen in diesem Bereich einen Beitrag zu mehr Aufmerksamkeit für das Thema Digitale Politische Ökonomie zu leisten – v.a. durch Verweis auf Besonderheiten der politischen Ökonomie des Internet, die Auswirkungen der Digitalisierung auf den Wandel von Machtbeziehungen und die zentrale Rolle von (staatlicher) Regulierung. Besonders interessant ist dabei die formelle und informelle Setzung neuer Standards, die diesen zunehmend wichtigen Bereich der sich globalisierenden Wirtschaft steuern – und eventuell auch Gründe für einen Prozess der „De-Globalisierung“ (vgl. Stone 2019; Walter 2021 sowie den Beitrag von Stefan Schirm in diesem Band) liefern könnte – analog zur von manchen Akteuren angestrebten Rückführung globaler Lieferketten, deren mangelnde Resilienz im Verlauf der COVID19-Pandemie deutlich wurde. Algorithmisches Regieren, das Thema Cybersicherheit sowie die Frage nach den Chancen für internationale Verhandlungen und *institution building* in diesem Bereich runden die Palette der betrachteten Themen ab.

Politische Ökonomie des Internet

Neben der eingangs beschriebenen und (wenn auch regional differenziert) quantitativ zunehmenden Digitalisierung der globalen Ökonomie hat dieser Prozess auch eine qualitative Komponente. Es geht also nicht nur um ein „mehr“, sondern auch um ein „anders“. Zwei Aspekte sollen im folgenden dabei in den Vordergrund gestellt werden: die Veränderung ökonomischer Mechanismen, die digitaler Ökonomie zum Teil eigen sind sowie die Veränderungen von Machtbeziehungen, die das Anwachsen dieses Wirtschaftsbereichs (nicht nur für die Wirtschaft) mit sich brachte und bringt.

Ökonomische Veränderungen

Die Digitalisierung hat die Verwandlung der hochentwickelten Volkswirtschaften in informationsbasierte Ökonomien stark beschleunigt. Die Benennungen der Berichte der *United Nations Conference on Trade and Development* (UNCTAD) sind in dieser Hinsicht instruktiv: Sprach man zu Beginn des Jahrhunderts noch von „E-Commerce and Development“, so ging es bald um die „Information Economy“; seit 2019 trägt der entsprechende Bericht den Namen „Digital Economy Report“ (UNCTAD 2021). Diese Entwicklung, v.a. des Informations- und Kommunikationssektors (ICT) ist so umfassend, dass für sie bereits der Begriff der „4. Revolution“ (Floridi 2014) geprägt worden ist.

In ökonomischer Hinsicht gehört die verlustfreie Reproduzierbarkeit zu den Kerneigenschaften von Digitalisierung und digitalen Daten. Durch sie werden die für die herkömmliche Wirtschaft prägenden Eigenschaften von Knappheit der Ressourcen und Technologien (Smelser/Swedberg 2005: 5) in der digitalen Ökonomie teilweise aufgehoben. Dies hat erhebliche Folgen z.B. in Bereichen wie Mediennutzung, Urheberrecht oder Softwareproduktion: Digitale Güter werden durch Nutzung nicht weniger und nutzen sich nicht ab, sie können vielmehr durch Kooperation sogar im Wert wachsen. Knappheiten gibt es in diesem Bereich dennoch – aber in neuen Feldern, etwa der Aufmerksamkeit (Jungherr/Schroeder 2021: 8).²

Ein weiteres Merkmal vieler digitaler Märkte sind sogenannte *Netzwerkeffekte*. Sie kennzeichnet, dass das gesamte System umso mehr Nutzen für jeden Teilnehmer generiert, je mehr an ihm teilnehmen, es somit „positive Feedback-Effekte“ gibt und in ihnen deshalb eine Tendenz zu „natürlichen Monopolen“ besteht (Schneider 2001: 121ff.; Busch 2019: 37f.). Ähnlich wie bei den Transfers von durch Netzwerkeffekte gekennzeichneten, oft ursprünglich staatlichen Industrien (Bahn, Telekommunikation) in den privaten Sektor in den 1980er Jahren besteht auch im Fall der Digitalisierung die Lösung zur Sicherung von Wettbewerb in verstärkter staatlicher Regulierung. Dies wird am Beispiel Datenschutz weiter unten im Beitrag ausführlicher diskutiert.

Digitalisierung hat zudem zu starken Preissenkungen beigetragen: Zwischen 1950 und 2010 ist der Preis einer gegebenen Menge Computerleistung, gemessen in konstanten US-Dollar, etwa um den Faktor $3 \cdot 10^9$ gefallen (vgl. die Darstellung bei Floridi 2010: 8). Das hierdurch illustrierte hohe Innovationstempo hat zu einer Veränderung von Unterneh-

2 Siehe zu diesem Phänomen bereits Simon (1971: 40) oder Benkler (2006: 107).

mensstrukturen in diesem Bereich beigetragen, in der die nach Börsenbewertung führenden Firmen drastisch weniger Mitarbeiter haben, als das während der Hochzeit des Industriekapitalismus der Fall war. Das damit zusammenhängende *Outsourcing* der Produktion (im Fall von physischen Produkten) an hinsichtlich der Lohnkosten günstigere Standorte hat sowohl die Internationalisierung der Wirtschaft begünstigt als auch eine Abhängigkeit von entsprechenden Lieferketten – vor allem aus China – verstärkt (UNCTAD 2018: 3f.).

Veränderte Machtbeziehungen

Die Digitalisierung der Ökonomie hat (natürlich) auch Auswirkungen auf die Machtverteilung sowohl innerhalb von Volkswirtschaften wie zwischen diesen gehabt. Die akademische Analyse dieser Entwicklung ist sicher noch nicht abgeschlossen, aber eine Reihe von Aspekten lässt sich bereits hervorheben.

Am weitreichendsten ist wahrscheinlich die Diagnose der Entstehung eines „surveillance capitalism“, die die amerikanische Sozialpsychologin und Ökonomin Shoshana Zuboff (2015: 85f.; 2019) vorgelegt hat. Für sie ist das von Firmen wie Google durch Speicherung und Analyse von Verhaltensdaten entwickelte Modell der Wertsteigerung von Anzeigenpreisen zentral. Es führe zur Kommodifizierung von Verhalten, Anreizstrukturen zur Verhaltensänderung und einer neuen Akkumulationslogik, da die Nutzer rasch eine Abhängigkeit von den neuen Informations- und Kommunikationswerkzeugen entwickelt hätten. Andere Autoren (wie Culpepper/Thelen 2019; Kuehn/Salter 2020) fokussieren auf das Phänomen der „platform power“, die von wenigen Firmen (wie Google, Amazon, airbnb oder Facebook) ausgeübt werde, und analysieren deren Bündnis mit Konsumenten bzw. deren Machtübertragung in den Bereich der Politik.

Wo immer man genau den Schwerpunkt legt: Die Digitalisierung hat nicht nur neue wirtschaftliche Macht entstehen lassen, sondern diese eng mit politischer Macht verknüpft. Dies wird deutlich, wenn Digitalmilliardäre wie Jeffrey Bezos sich führende Medien wie die *Washington Post* kaufen, aber vor allem durch die Verbindung von digitalen *social media* und politischer Kommunikation. Kommunikationsplattformen wie Facebook oder Twitter haben sich zu wichtigen Foren gesellschaftlicher Debatten entwickelt – und sie können Einfluss auf diese nehmen, sei es durch inhaltliche Steuerung via Löschung bestimmter Nachrichten, durch Ausschluss von ihrer Nutzung (wie im Fall des ehemaligen US-Präsidenten Donald Trump) oder durch das „Abschalten“ ganzer Länder (wie im Fall

Russlands aus Anlass des Ukrainekriegs). Ob diese Kommunikationsplattformen wegen solchen Einflusses kritisiert werden sollten oder ob ihnen von staatlicher Seite auch noch von Überwachung ihrer Nutzer aufgebürdet werden sollte (wie etwa im deutschen *Netzwerkdurchsetzungsgesetz*), wird kontrovers diskutiert. Zweifellos ist hier asymmetrische Kommunikationsmacht entstanden, gegen die sich (v.a. autoritäre) Staaten durch den Versuch zur Wehr setzen, auf ihrem Territorium diese Kommunikation einzuschränken. Waren bisher die attraktiven „Sender“-Medien durchweg westlicher Provenienz und strahlten in den Rest der Welt aus, so muss dies keineswegs so bleiben. Die Popularität des in China beheimateten Kurzvideo-Dienstes *TikTok* ist ein Beispiel, dass sich Sender-Empfänger-Ströme in Zukunft durchaus umdrehen können – eventuell sogar eines Tages gefolgt von entsprechenden Sperrbemühungen.

Sowohl aus ökonomischen wie aus inhaltlichen Gründen ist der Prozess der Digitalisierung von zunehmender Regulierung begleitet. Waren die Gründer des Internet noch der Überzeugung gewesen, das neue Medium sei aus prinzipiellen und in seinem technischen Design verorteten Gründen nicht regulierbar („the Net interprets censorship as damage and routes around it“, lautete ein Glaubenssatz aus dessen frühen Zeiten), so führte seine stark wachsende wirtschaftliche und politische Bedeutung bald zu einer Situation, in der nur noch die Frage des Ausmaßes sowie des Modus der Regulierung (Selbstregulierung, Ko-Regulierung oder gesetzliche Regulierung, vgl. Levi-Faur 2011), aber nicht mehr der Grundsatz in Frage standen (Busch 2019: 36ff.).

Regulierung von Daten

Zentral für die weiter oben beschriebene Digitalisierungsprozesse, die transnational Wirtschaft und Gesellschaft prägen, sind Daten und ihr Austausch. Auch wenn es Probleme bei der genauen Definition und Messung von Daten und Datenverkehr gibt, sollen personenbezogene Daten und ihre Regulierung im folgenden Abschnitt im Mittelpunkt der Diskussion stehen. Dafür gibt es eine Reihe von guten Gründen: Zum einen handelt es sich um ein seit langem etabliertes Politikfeld, das bereits früh (in den 1990er Jahren) von der nationalen auf die supranationale Ebene wanderte.³ Zum zweiten sind personenbezogene Daten zentral für die Ausbildung

3 Das Politikfeld ist im deutschen Sprachraum als „Datenschutz“ bekannt, was etwas paradox ist, da ja nicht die Daten, sondern die Personen, auf die sie sich beziehen,

und Ausbreitung des digitalen Kapitalismus bzw. „Überwachungskapitalismus“ (Zuboff 2019). Und schließlich gibt es in diesem Bereich signifikante Entwicklungen, Konflikte und Vereinbarungen auf der internationalen Ebene zu berichten.

Die Ursprünge der Regulierung von Privatheit speisen sich aus ganz unterschiedlichen Quellen. Da ist zum einen die Ebene von Menschenrechten, die für jedermann ein allgemeines Recht auf Achtung des Privat- und Familienlebens, der Wohnung und der Korrespondenz postuliert – so die Formulierung in Artikel 8 der Europäischen Menschenrechtskonvention von 1950. Die Festlegung dieses für die Identität und Autonomie des Einzelnen konstitutiven Rechts führte, befördert durch die Entwicklung moderner IT- und Kommunikationstechnik, schon in den 1960er und 1970er Jahren zur Ausweitung auf diese Gebiete (vgl. Busch 2011: 229). Impulse auf nationaler Ebene entwickelten sich aus dem Umfeld der Indienstnahme von Computern in der staatlichen Verwaltung ab den frühen 1970er Jahren. Damals wurde damit begonnen, aus Gründen der Rationalisierung Verzeichnisse etwa von Steuerzahlern und Einwohnern in Datenbanken auf Großrechnern zu erstellen (vgl. Bennett 1992: 46ff.). Auch wenn die Zwecke primär statistischer Natur waren, so kamen doch Bedenken auf, dass solche Daten eventuell von staatlicher Seite für andere Zwecke missbraucht werden könnten; Gesetzgebungsvorhaben (zuerst in Schweden und der Bundesrepublik) waren die Folge – und mit ihnen die Einrichtung von Behörden und Beauftragten zum Datenschutz, die ihrerseits eine wichtige Rolle bei der Ausbreitung des Gedankens von Datenschutz und Datenregulierung spielten (Bennett 2008; Newman 2011). Eine dritte Quelle waren Bestrebungen, aus Gründen der Wirtschaftlichkeit des internationalen Handels Harmonisierungen zwischen nationalen Regeln im Bereich des Datenschutzes anzustreben. Hier spielten bereits in den 1970er Jahren internationale Organisationen wie die OECD eine koordinierende Rolle. Über Expertengruppen wurde versucht, unterschiedliche nationale Ansätze zusammenzuführen, was sich als schwierig erwies. 1981 kam es zur Verabschiedung der „Guidelines on the Protection of Privacy and Transborder Flows of Personal Data“ (OECD 1981), die acht spezifische „Grundprinzipien“ für den Datenschutz umfassten und explizit „Mindeststandards“ darstellen sollten. Zwar waren diese nicht rechtlich bindend (und einige Mitgliedsstaaten bevorzugten statt Gesetzgebung die

geschützt werden sollen. Im Englischen wird deshalb zumeist (und passender) der Ausdruck „privacy“ („Privatheit“) benutzt. Im folgenden werden diese Begriffe abwechselnd und synonym benutzt.

eingeräumte Möglichkeit der Selbstregulierung), doch erwiesen sie sich als einflussreich insbesondere für die Gesetzgebung zum Datenschutz außerhalb Europas (vgl. Busch 2011: 230).

Alle diese Entwicklungen fanden statt zu einer Zeit, in der das Ausmaß an Vernetzung von Computern noch sehr gering (und zumeist auf den Bereich der Forschung beschränkt) war und Computer fast ausschließlich professionell (d.h. in Firmen und staatlichen Verwaltungen) eingesetzt wurden. Die Entwicklung und Verbreitung von *Personal Computers* begann in den 1980er Jahren erst sehr zaghaf, und ihre Vernetzung nahm erst in den späten 1990er Jahren mit dem Ausbau und der Popularisierung des Internet Fahrt auf. Mit der Verbreitung von Smartphones ab den 2010er Jahren wurde der mobile Zugang zum Internet die meistgenutzte Form der Vernetzung (vgl. zu Details der Entwicklung Cortada 2012; Busch 2019).

Ähnlich wie bei den Beweggründen für den Datenschutz kann man auch bei der Analyse von Daten verschiedene Ansätze unterscheiden. So kann man beispielsweise die Unterscheidung von Daten als privates Gut, als öffentliches Gut, als Allmendegut oder als durch Treuhandschaft verwaltetes Gut vornehmen (Schneider 2019). Doch ist diese Unterscheidung in Idealtypen eher zur normativen Diskussion als zur Analyse der Wirklichkeit geeignet. Für die Untersuchung realer Prozesse ist ein Fokus auf interessengeleitetes Handeln vielversprechender, da auf diese Weise Konflikte deutlich werden. Unterscheidet man im Hinblick auf personenbezogene Daten zwischen 1.) ökonomischen Interessen, 2.) Sicherheitsinteressen und 3.) Bürgerrechtsinteressen, so wird deutlich, dass unterschiedliche Akteure dieselben Themen durch unterschiedliche *frames* und mit unterschiedlichen Interessen betrachten (Busch 2012a: 424ff.; Busch 2012b: 324ff.). Auch wird durch eine solche Blickweise erklärbar, dass sich (aufgrund differierender Machtressourcen) in verschiedenen Fallstudien zum selben Themenfeld unterschiedliche Dynamiken und Ergebnisse zeigen können. Blickt man auf Staaten als Akteure in diesem Politikfeld, so zeigen sich die drei wichtigsten Akteure (die USA, China und die Europäische Union) im Hinblick auf ihre datenbezogene Politik als durch unterschiedliche Regulierungslogiken gekennzeichnet: steht bei den Vereinigten Staaten die Kontrolle der Daten durch den privaten Sektor im Mittelpunkt, so ist dies im Fall Chinas die Datenkontrolle durch den Staat. Für die Europäische Union steht im Zentrum die Kontrolle der Daten durch das betroffene Individuum auf Basis von Grundrechten und Werten (UNCTAD 2021: xviii, 108, 111ff.).

Als vor gut 30 Jahren die ersten vergleichenden Untersuchungen im Bereich Datenschutz durchgeführt wurden, erwarteten Experten eine bal-

dige Angleichung der Regelungen. Der Grund lag in einer ganzen Reihe von Einflussfaktoren, die alle in Richtung Konvergenz wirken würden: Da war zum einen die gemeinsame technologische Entwicklung, die überall dieselben Lösungen plausibel erscheinen lassen würde; die Tendenz zur Emulation von Lösungen durch Kontakte in transnationalen Elitennetzwerken, die Harmonisierung in Organisationen wie der Europäischen Gemeinschaft und schließlich Druck durch das wachsende Gewicht derer, die solche Regeln eingeführt haben und mit denen man im wirtschaftlichen Austausch bleiben möchte (Bennett 1992: 247-250). Diese Erwartungen entsprachen einer damals verbreiteten Erwartung genereller Politikkonvergenz im Rahmen des Prozesses der Globalisierung. Mechanismen der Außenhandelsökonomie unter Bedingungen offener (Kapital-)Märkte einerseits und Überlegungen hinsichtlich des Wettbewerbs um Investitionskapital zwischen Standorten andererseits ließen weitgehende Angleichungen in den meisten Politikfeldern erwarten (Busch 2003: 22-27). Freilich hat die Globalisierungsforschung seitdem gezeigt, dass diese Konvergenzprozesse oft keineswegs zu vollständigen oder auch nur weitgehenden Annäherungen geführt haben. Vielmehr haben Prozesse der Pfadabhängigkeit und institutionelle Beharrungskräfte ebenso wie unterschiedliche Interessen weiter für zum Teil deutliche Unterschiede in den Politikprofilen geführt.

Das lässt sich auch im Bereich des Datenschutzes zeigen, wo es eine komplexe Kombination aus Konvergenz und Divergenz zwischen unterschiedlichen Jurisdiktionen gibt. Konvergenz hat es insofern gegeben, als Regulierungen zum Datenschutz (zumindest in allen fortgeschrittenen Volkswirtschaften) zum Standard gehören. So hat sich die Zahl der Staaten, die gesetzliche Regulierungen in diesem Bereich haben, massiv erhöht: von 43 Mitte der 2000er Jahre auf 120 am Ende des Jahres 2016 (Bennett/Raab 2020: 451). Und zugleich ist aus einer geographisch im Bereich der OECD-Staaten konzentrierten Gruppe mit dem Hinzustoßen von Ländern in Asien, Afrika und Lateinamerika ein globales Phänomen geworden (ebd.). Neben dieser Konvergenz gibt es aber weiter relevante Differenzen, die von fortbestehender Divergenz zeugen. Sie betreffen nicht nur den Werkzeugkasten der eingesetzten Politikinstrumente, sondern auch unterschiedliche fundamentale Ansätze der Regulierung. Die deutlichste Unterscheidung ist hier wohl zwischen dem in Europa dominanten *approach* und dem in den Vereinigten Staaten verfolgten zu konstatieren (vgl. Busch 2011: 233): Während Privatheit und Datenschutz in der EU als Menschenrecht bzw. Grundrecht gefasst wird, das dem Individuum konstitutiv zusteht (und für dessen Einhaltung folglich der Staat zu sorgen hat), wird beides in den USA als *property right* angesehen, also ein Besitz-

gut, über das jeder Einzelne frei verfügen kann – und auf das er folglich auch (aus freiem Willen und ggfs. gegen Kompensation) verzichten kann. Dass für ein so klassifiziertes Gut der freie Markt als effektivster Durchsetzungsmechanismus angesehen wird, erstaunt dann nicht weiter. Die Abwesenheit umfassender gesetzlicher Regeln und die Fokussierung auf nur punktuelle Gesetzgebung in diesem Themengebiet sind die logische Folge.

Mit zunehmender Wichtigkeit des Themas internationaler Datenverkehr zeichnete sich bereits in den 1980er Jahren ab, dass es in diesem Bereich zu Konflikten über den Atlantik kommen könnte. Beide Seiten verdächtigten einander, auf Geltung ihrer jeweiligen Regeln nur zum eigenen Vorteil zu bestehen: Die EU-Seite verdächtigte die USA, mit ihrer Präferenz für unbehinderten internationalen Datenaustausch vor allem den Vorsprung der eigenen IT-Industrie verteidigen zu wollen, während umgekehrt die Amerikaner mutmaßten, hinter dem Bestehen der Europäer auf Regeln zum Datenschutz verberge sich in Wirklichkeit der Wunsch nach Protektionismus (Bennett 1992: 136f.). Das absehbar starke Wachstum in diesem Bereich machte dies zu einem strategischen Thema, denn die internationale Durchsetzung des eigenen Regulierungsmodells würde für die siegreiche Seite einen bedeutenden Vorteil darstellen.

Zu einer ersten Zuspitzung kam es nach der Verabschiedung der EU-Datenschutzrichtlinie im Jahr 1995, die im Zusammenhang mit der Vollendung des Binnenmarktes einheitliche Regeln nach innen und eine klare Abgrenzung nach außen schuf (Heisenberg 2005). Erst nach einer längeren, konfrontativen Episode, in der zunächst beide Seiten auf ihren jeweiligen Positionen beharrten und von der jeweils anderen Seite die Übernahme des eigenen Ansatzes erwarteten (also auf Seiten der EU die Schaffung einer allgemeinen Datenschutzgesetzgebung durch die USA; von amerikanischer Seite die Akzeptanz des Vertrauens auf unabhängige, private Zertifizierungsstellen durch die Europäer) fand man zu einem Kompromiss. Das sogenannte „Safe Harbor“-Verfahren tauschte Verpflichtungen der USA hinsichtlich Informationspflichten, Auskunftsrechten und Rechtsschutz gegen eine Erklärung der EU-Kommission, dass dadurch ein „angemessenes Schutzniveau“ im Sinne der Datenschutzrichtlinie gegeben sei (Busch 2012a: 414-417). Doch bereits kurze Zeit später kam es in der Folge der Terroranschläge vom 11. September 2001 zu einem weiteren Konflikt. Das Verlangen der USA, aus Gründen der Terrorismusbekämpfung bereits vor Abflug Zugriff auf die von den Fluglinien gespeicherten persönlichen Daten der in die Vereinigten Staaten fliegenden Passagiere zu erhalten, verstieß gegen EU-Datenschutzregeln. In diesem regulativen Konflikt drohte die eine Seite mit dem Entzug der Landrechte, die andere mit

empfindlichen Geldstrafen für die Fluglinien. Auch in diesem Fall gab es nach langen Verhandlungen eine Einigung mit detaillierter Festlegung, welche Daten übermittelt werden könnten.⁴ Und nur kurze Zeit später, im Juni 2006, entbrannte ein weiterer Disput über Datenschutz zwischen EU und USA: Durch Recherchen der *New York Times* wurde bekannt, dass die amerikanische Justiz sich im Rahmen ihres *Terrorist Finance Tracking Program* (TFTP) Zugriff auf die Daten der in Belgien beheimateten Finanzdienstleistungs-Kooperative SWIFT verschafft hatte, die praktisch den gesamten internationalen Zahlungsverkehr durch ein Mitteilungssystem ermöglicht. Sowohl personenbezogene wie strategische Unternehmensdaten waren also jahrelang ohne Wissen der Betroffenen über das in den USA beheimatete Backup-Rechenzentrum der Genossenschaft von der US-Regierung mitgelesen worden.

Die hier nur kurz beschriebenen Konflikte zeigen, dass es in diesem Bereich nicht nur um eigene Präferenzen der Akteure geht, sondern auch um die Durchsetzung von ökonomischen und politischen Machtinteressen. Die frühe Dominanz der US-IT-Industrie (auch und gerade im Bereich digital verfügbarer Inhalte) hatte im Konflikt der 1990er Jahre eine relativ symmetrische Interessenlage geschaffen und beide Seiten zum Kompromiss geführt: Während die amerikanische Seite ihren Vorsprung in wirtschaftliche Profite verwandeln und den Zugang zum Wachstumsmarkt EU nicht verlieren wollte, war die europäische daran interessiert, nicht vom Zugang zu den digitalen Daten aus den USA abgeschnitten zu werden. Beide späteren Konflikte wiesen keine entsprechend symmetrische Interessenlage auf, vielmehr konnten die USA hier weitgehend einseitig ihre Interessen hinsichtlich der Bekämpfung von Terrorismus durchsetzen, ohne dass ihnen gravierende wirtschaftliche Nachteile gedroht hätten.

Regulierung als Quelle von Macht

Die IT-Industrie der Europäischen Union hat sich später und weniger stark entwickelt als dies in den USA der Fall war. Zudem mussten sich die Europäer in verschiedenen Konflikten den Präferenzen der USA im Bereich Datenschutz beugen, wie eben gesehen. Angesichts dieser scheinbaren Po-

4 Auf die weiteren Stadien in diesem Konflikt (Positionswechsel der EU-Kommission nach terroristischen Vorfällen in Europa sowie der in einem Urteil des EuGH mündende, daran anschließende Konflikt zwischen Europäischem Parlament und Kommission) wird hier nicht eingegangen, da es für das hier vorgebrachte Argument nicht relevant ist. Siehe dazu aber im Detail Busch (2012a: 418–433).

sition der Schwäche muss es überraschen, dass die europäischen Normen in diesem Bereich dennoch ziemlich einhellig als weltweit führend und auf dem Weg zu einem globalen Standard angesehen werden. Die im Mai 2018 (als Nachfolgerin der EU-Datenschutzrichtlinie von 1995) in Kraft getretene *Datenschutz-Grundverordnung* (DSGVO) oder (auf Englisch) *General Data Protection Regulation* (GDPR) wurde bereits bei ihrem Inkrafttreten als kommende globale Norm gewürdigt (Gordon/Ram 2018). Spätere wissenschaftliche Untersuchungen haben diese Einschätzung auf der Basis praktischer Erfahrungen bestätigt: So ist die Rede von einem „privacy law not for the EU, but for the world“ (Schwartz 2019: 771), von einem „gold standard for the world“ (Schuenemann/Windwehr 2021: 864) bzw. von „widely viewed as setting a new global standard for the protection of data privacy“ (Krishnamurthy 2020: 26).

Warum eine Regulierung, die einen besonders hohen Schutzstandard für Individuen einführt, die Regulierungsbehörden mit erheblichen Eingriffsmöglichkeiten ausstattet, die Nutzern wie Unternehmen beim Datentransfer erhebliche Mühen (und letzteren auch Kosten) abverlangt, erscheint zunächst kontraintuitiv. Häufig wird ja erwartet, dass sich bei internationalem regulativem Wettbewerb die laxesten Regeln durchsetzen, weil sie die geringsten Kosten auferlegen und daher die entsprechende Jurisdiktion einen Vorteil erlangt.⁵ Wie kann man dann erklären, dass sich in diesem Bereich stattdessen die schärfste Regulierung durchsetzt, zumal der internationale Datenverkehr ja aufgrund der Abwesenheit physischer Barrieren besonders grenzenlos erscheint?

Drei Faktoren können zur Erklärung dieses scheinbaren Rätsels vorgebracht werden: ökonomische Skaleneffekte für Länder und Unternehmen, legislative Emulation durch andere Staaten und schließlich die Qualität und Handhabung der Regelsetzung. Für den ersten Effekt ist das wirtschaftliche Gewicht des EU-Binnenmarktes ein wichtiger, aber nicht entscheidender Faktor. Ginge es allein nach der Zahl der Konsumenten, wäre die EU zwar ein wichtiger Spieler, aber nicht notwendig entscheidend. Allerdings müssen alle Länder, die Handelsabkommen mit der EU abschließen wollen, die Einhaltung der DSGVO für den Handel mit der EU zusichern; für diese stellt eine Ausweitung der Regelgeltung auf das eigene Territorium daher eine Investition in den Zugang zum Datenmarkt der EU dar. Auch für multinationale Unternehmen kann es durchaus

⁵ Die entsprechende Literatur spricht von „race to the bottom“. Allerdings gibt es auch „race to the top“-Dynamiken. Grundlegend für die Analyse ist Vogel (1986) mit den Konzepten „Delaware effect“ und „California effect“.

attraktiv sein, ihre Produkte nach dem relativ anspruchsvollsten Standard auszurichten, um Vorteile durch einheitliche Produktion zu erlangen und so insgesamt Kosten zu sparen.⁶ Das bereits erwähnte *outsourcing* von Produktion in der globalisierten Wirtschaft verstärkt diesen Anreiz zusätzlich. Der zweite Effekt besteht darin, dass mit der DSGVO eine umfassende Datenschutz-Gesetzgebung vorliegt, die zu imitieren für andere Länder attraktiv sein kann und die sich vorteilhaft von den nur sektoralen Datenschutzregeln in den USA abhebt. Das ist nicht nur ein theoretischer Effekt, sondern man kann ihn empirisch nachweisen: So waren etwa eine Reihe lateinamerikanischer Länder bereits von der EU-Richtlinie aus dem Jahr 1995 zum Erlass ähnlicher Gesetze inspiriert worden. Und im Jahr 2018 hatten bereits 67 von 120 Ländern außerhalb der EU GDPR-ähnliche Gesetze erlassen (UNCTAD 2021: 113). Der dritte Effekt besteht in einer Ausweitung des Effekts der Marktgröße und in seiner Ergänzung um den Faktor regulatorischer Qualität. Wichtig ist demzufolge nicht nur die Setzung von Regeln, sondern auch deren Durchsetzung und Verbreitung. Schon früh wurde das Argument vorgebracht, dass es neben Marktgröße auch auf kompetente Regulierungsinstitutionen ankomme (Bach/Newman 2007: 827). Anhand des Beispiels Datenschutz konnten die Autoren zeigen, warum es der EU trotz amerikanischer Marktüberlegenheit gelang, hier zum de facto-Standardsetzer zu werden: man verfügte zwar nur über einen „second-class market“, verbinde diesen aber mit „first-class regulatory institutions“ (ebd.: 835). Dass diese Dominanz politikfeldspezifisch und nicht generalisierbar sei (siehe als Kontrast den Bereich der Finanzmarktregulierung), ist ein Faktum, das weitere Forschung bestätigt hat, die unter dem Stichwort „Brüssel-Effekt“ bekannt wurde (Bradford 2012, 2020). Dieser (explizit auf David Vogels bahnbrechendem Konzept des *California effect* aufbauende) ~~Effekt~~ ergibt sich aus einer Kombination von Marktgröße, Regulierungskapazität und politischem Willen zu strikter Regelsetzung, sofern die Regulierungsziele keine Ausweichmöglichkeiten haben (es sich also z.B. um Konsumentenmärkte handelt) und Unternehmen mehr Vorteile von einheitlichen Produkten als von je nach Jurisdiktion unterschiedlichen haben (vgl. Bradford 2020: Kap. 2).

Mechanismus

Märkte der digitalen Ökonomie sind, insbesondere im Bereich der Informations- und Kommunikationstechnologie, auf globales *branding* ausgelegt. Unternehmen wie *Google*, *Facebook* und *Twitter*, aber auch *Apple*

⁶ Facebook-CEO Mark Zuckerberg kündigte das etwa bei einer Anhörung vor dem US-Kongress an, vgl. <https://www.theverge.com/2018/4/11/17224492/zuckerberg-facebook-congress-gdpr-data-protection> (letzter Zugriff 15.3.2022).

oder *Microsoft* beziehen einen erheblichen Teil ihrer Attraktivität aus einem weltweit einheitlichen Auftritt. Das lässt, aufbauend auf den Analysen über die Erfolgsgründe des „Brüssel-Effekts“, weitere Erfolge des europäischen Vertrauens auf „regulatory leadership“ (UNCTAD 2021: 113) erwarten – im Gegensatz zur „technological leadership“ der USA und Chinas. Forderungen nach und Debatten über „digitale Souveränität“ (siehe als Überblick Pohle 2020 sowie ausführlicher für den deutschen Fall Lambach/Oppermann 2022) erscheinen von daher weniger unbegründet, als das auf den ersten Blick der Fall sein mag. Und dass die Europäische Union sich in diesem Bereich sehr wahrscheinlich weiter als hochrelevanter Akteur positionieren wird, zeigen neuere Entwicklungen zum Zeitpunkt des Abschlusses dieses Manuskripts im März 2022: In der mit den USA getroffenen Einigung über die Nachfolgeregelung für das vom EuGH gekippte *Privacy Shield* (die ihrerseits eine Verschärfung des *Safe Harbor*-Abkommens war) gelang es der EU, das Schutzniveau noch einmal zu erhöhen und Klagerechte für Europäer in den USA zu verbessern.⁷ Und mit dem im Oktober 2022 in Kraft tretenden *Digital Markets Act* könnte es der EU gelingen, ihre regulatorische Macht noch weiter auszudehnen, indem Vorschriften für Interoperabilität digitaler Dienste mit Verboten für das *bundling* von Diensten und antikompetitives Verhalten kombiniert und mit erheblichen Strafen im Fall des Verstoßes geahndet werden. Dass monopolistisch auftretenden digitalen Geschäftsmodellen eine Kraft entgegentritt, die mit ihren Regeln Wettbewerb zu fördern und Konsumentenrechte zu sichern versucht, wird auch von unzweifelhaft marktwirtschaftlich gesonnenen Kräften wie dem *editorial board* der *Financial Times* begrüßt.⁸

Zusammenfassend ist zu sagen, dass die – verglichen mit den USA und China – relative Erfolglosigkeit Europas hinsichtlich der Existenz großer Unternehmen im digitalen *business* sich als Voraussetzung für den Erfolg bei der Setzung von global wirkenden Regeln erweist. Und dass Konsumenten zwar eine wichtige Rolle auf diesen Märkten spielen, sie aber – anders als von Culpepper/Thelen (2019) vermutet – nicht nur im Bündnis mit großen Produzenten deren Interessen stärken, sondern (entsprechenden politischen Willen vorausgesetzt) auch ihre eigenen Interessen befördern können.

7 Vgl. den Bericht der FAZ vom 26.3.2022 „Lösung für transatlantischen Datenverkehr“, zugänglich unter <https://www.faz.net/aktuell/wirtschaft/eu-und-usa-erzielen-einigung-ueber-transatlantischen-datenverkehr-17910092.html>.

8 Vgl. den Kommentar „The EU tries to loosen Big Tech’s grip“, *Financial Times*, 27. März 2022 (<https://www.ft.com/content/def9de58-a9b7-4ed2-a05f-565c55814570>).

Algorithmisches Regieren

Im letzten Teil dieses Aufsatzes soll (in aus Platzgründen notwendiger Kürze) noch auf zwei wichtige inhaltliche Bereiche eingegangen werden, bevor mit einer Überlegung zu strukturellen Eigenheiten dieses Bereichs ein kurzer Rück- und Ausblick den Beitrag beschließt.

Die Nutzung von Algorithmen bzw. *Künstlicher Intelligenz* (KI) sowie umfangreicher Datensätze („Big Data“) kann neue Möglichkeiten im Handeln von Regierungen und Verwaltungen eröffnen. Dass durch die Nutzung dieser Technologien die Erfassung von Fakten in Echtzeit ebenso wie quasi ein Blick in die Zukunft und vor allem die erfolgreiche Bearbeitung zahlreicher Probleme in einem frühen Stadium (von frühzeitiger Unterstützung für schwache Schüler und Bekämpfung von Krebs über effektive Bekämpfung des Klimawandels und richtige Priorisierung von Überprüfungen öffentlicher Gebäude) ermöglichen würde, ist eine seit langem gehegte Hoffnung (Mayer-Schönberger/Cukier 2013: 193, 195). Die Erwartung einer Dominanz der Fakten reichte bis zu Befürchtungen, dadurch könnte die Essenz von Politik gefährdet sein. Denn ein „algorithmischer Leviathan“ (König 2020) könnte durch vermittelnde Entscheidungsfindung über völlig neue Möglichkeiten der Bearbeitung gesellschaftlicher Komplexität verfügen. Andererseits sei ein solches System aus sich heraus nicht in der Lage, neue Gesichtspunkte aufzunehmen und mit Kritik konstruktiv umzugehen, und nur durch einen politischen Prozess sei Legitimation für den Einsatz solcher Verfahren zu erzielen (ebd.: 481).

Tatsächliche Einsatzformen von KI in der öffentlichen Verwaltung fallen im Vergleich mit solchen grundsätzlichen Überlegungen weitaus prosaischer aus. Themen wie *predictive policing*, Identifikation und Authentifizierung von Personen, Verkehrslenkung oder erleichterte Kommunikation mit Bürgern über *chat bots* (Djeffal 2020) erwecken eher den Eindruck gradueller als fundamentaler Veränderungen. In der Literatur herrscht denn auch Einigkeit, dass der Einsatz fortgeschrittener Techniken in diesem Gebiet (wie Big Data zum Verständnis und zur Beeinflussung des Verhaltens von Kunden) bisher hauptsächlich im privatwirtschaftlichen und weniger im staatlichen Bereich vorkommen (Haunss/Ulbricht 2020). Am weitesten fortgeschritten ist dies im Bereich der Sicherheit – etwa bei Flugreisenden, die mit Verfahren der Mustererkennung auf Terrorismus- bzw. Schwerkriminalitäts-Risiken untersucht werden (ebd.: 46). Ein Einsatz für die Regulierung von Lebensbereichen (wie durch die *social credit*-Systeme in China) findet in Demokratien nicht statt.

KI kann in Demokratien für den politischen Prozess und für das Regierungshandeln sowohl Vor- wie Nachteile schaffen (König/Wenzelburger

2020): In positiver Hinsicht kann sie zu besserer Verarbeitung der Informationen über Präferenzen der Bürger und weniger Informationsüberlastung sorgen; kann besser informiertes Entscheiden ebenso wie bessere Kontrolle demokratischer Entscheidungen sicherstellen und so insgesamt für bessere öffentliche Dienstleistungen sorgen. Andererseits können dieselben Technologien auch für fragmentiertere Gesellschaften, Verbreitung von *fake news* und die Manipulation des Mediensystems sorgen, durch einseitige Informationsvorteile zur Bevorzugung spezieller Interessen und die Erosion politischer Debatten beitragen und intransparentes Verwaltungshandeln befördern. Allein durch das Design solcher KI-Systeme kann nicht bestimmt werden, welches der beiden Szenarien Realität wird – dazu kommt es zentral auf die öffentliche politische Kontrolle der entsprechenden Entscheidungen an (ebd.: 9).

der

Der (relativ zurückhaltende und wohl auch deshalb bisher wenig kontroverse) Einsatz von KI und algorithmischem Regieren in nationalen staatlichen Verwaltungen steht in einem bemerkenswerten Kontrast zur Einschätzung im Bereich internationaler Konkurrenz. Hier wird dieses Thema als zentral für die geopolitische Rivalität zwischen den USA und China angesehen und als entscheidend für die Auseinandersetzung zwischen Demokratien und Autokratien (Buchanan/Imbrie 2022: 133). Noch hätten die Demokratien in diesem Bereich insgesamt einen Vorsprung, doch sei die Erkenntnis, dass man dem Thema entsprechende Ressourcen widmen müsse, noch zu wenig verbreitet. Ob die Verschärfung der internationalen Situation ~~im Frühjahr 2022~~ hier zu entsprechend veränderten Haltungen führen wird, bleibt abzuwarten.

durch den Ukrainekrieg

Cybersicherheit

Kurz soll auch noch auf die damit verbundene Thematik der Cybersicherheit eingegangen werden. Denn ebenso wie durch die immer enger werdenden Vernetzungen der globalen Informations- und Kommunikationstechnologien die Chancen für engere Verbindungen in ökonomischer, sozialer und kultureller Hinsicht zunehmen, steigt auch die Verwundbarkeit durch Angriffe auf diese Vernetzungen. Diese können kriegerische, kriminelle oder terroristische Motive haben, mit unterschiedlichen Formen technischer Raffinesse unternommen werden (siehe Rohs 2019 für einen gegliederten Überblick) und unterschiedlich schwere Folgen haben. Vom Zusammenbruch lebenswichtiger Infrastrukturen (wie Strom- oder Wasserversorgungen) über schwere ökonomische Probleme (bei Attacken z.B. auf Zahlungssysteme) bis zur Verhinderung oder Verzögerung wichti-

ger staatlicher Vorhaben (etwa im Fall des bisher wohl bekanntesten Falles einer Cyberattacke, dem *Stuxnet-Virus*, der das Atomprogramm des Iran sabotierte, vgl. Deibert 2012) reichen tatsächlich stattgefundene oder mögliche Angriffsformen. Ob man aus der Analyse, bisherige Cyberattacken erfüllten nicht die Definition eines Cyberkrieges, tatsächlich plausibel folgern kann, es werde einen solchen auch in Zukunft nicht geben (Rid 2012), wird allerdings erst der Verlauf der Zeit zeigen können. Zwar sind genaue Terminologien immer wichtig, und man muss zwischen einzelnen Attacken, unterstützenden Aktionen und einem generellen Krieg unterscheiden. Eine klare Klassifikation, wann man von „Cyberterrorismus“ und wann von etwas darüber hinausgehendem spricht, hat sich jedoch noch nicht etabliert.

Schon seit längerem wird diskutiert, welcher Zusammenhang zwischen der dezentralen technischen Form des Internet, seiner unhierarchischen Governanceform und der mangelnden Sicherheit im Internet besteht (Mueller u. a. 2013). Da an diese Organisationsform jedoch kurz- und mittelfristig kaum etwas zu ändern sein dürfte, konzentrieren sich staatliche und supranationale Akteure vor allem auf Bearbeitung des Problems durch die Erarbeitung gesetzlicher Regelungen und die Schaffung kompetenter Organisationen zur Abwehr diesbezüglicher Gefährdungen. Sowohl auf der Ebene der EU wie der Bundesrepublik sind unlängst beispielsweise Richtlinien und Gesetze formuliert und verabschiedet worden, und organisatorische Veränderungen zu ihrer Implementation werden an verschiedenen Stellen sowohl der staatlichen Verwaltung wie der Bundeswehr vorgenommen (Schuenemann/Windwehr 2021: 206f.). In der akademischen Diskussion scheint die Bedrohungswahrnehmung hingegen weniger akut zu sein – die primäre Perspektive auf diese Prozesse reflektiert kritisch über Probleme der „Versicherheitlichung“ (*securitization*) und die sich in ihr manifestierende Durchsetzung der Prioritäten von Teilen des Sicherheitsstaates gegenüber der Gesellschaft (vgl. Hansen/Nissenbaum 2009; Busch 2015).

Ausblick

Die dem Prozess der rasch zunehmenden Digitalisierung innewohnende Transformation von Wirtschaftssystemen ist vielfältig, aber im Bereich der Internationalen Politischen Ökonomie noch wenig systematisch erforscht. Dabei bieten sich viele Aspekte an – vom Wandel der Unternehmensstrukturen über Veränderungen internationaler Lieferketten in der Produktion bis zur drastischen Steigerung von Innovationsprozessen und

dem Entstehen neuer Wertschöpfungsquellen zeigen sich in der digitalisierten Ökonomie erhebliche Veränderungen gegenüber der noch vor wenigen Jahren dominierenden Industrieökonomie. Deutlich wird jedenfalls, dass Information und Informations- und Kommunikationstechnologie ein Machtfaktor geworden sind, den jeder berücksichtigen muss, der die Dynamik globaler Politik verstehen will. In den Worten zweier führender Forscher auf diesem Gebiet: „Information has joined oil, tanks, and money as a key currency of international affairs. States, firms, and substate actors among others leverage it to influence economic interactions and coerce adversaries. It provides the basis for business models that drive economies“ (Farrell/Newman 2019: 173).

Dass die Regeln für diese digitale Weltwirtschaft aus multilateralen, internationalen Verhandlungen hervorgehen, ist wohl eher unwahrscheinlich. Die Chance, eine Harmonisierung von Regeln beim ersten datenbezogenen Thema – dem Datenschutz – durch internationale Organisationen zu erlangen, wurde schon früh als schwach eingeschätzt (Bygrave 2004: 347f.). Dass solche Verhandlungen, zumal bei breiter Beteiligung, extrem aufwendig und langdauernd sind, hat nicht zuletzt der in den Jahren nach 2002 stattfindende (und kaum Ergebnisse hervorbringende) Prozess des *World Summit on the Information Society* (WSIS) gezeigt. In mehreren Runden beschäftigten sich Tausende von Delegierten aus 175 Ländern ausführlich mit allgemeinen Verhandlungen über die Natur und die Gestaltung des Internet; mit Problemen der digitalen politischen Ökonomie befasste man sich gar nicht (vgl. Breindl 2019: 93ff.). Auch wenn Internationale Organisationen wie die UNCTAD wiederholt Plädoyers für ein „global data governance framework“ und eine neue Form von Institutionalisierung dafür – idealerweise natürlich unter dem Dach der Vereinten Nationen („the most inclusive international forum in terms of country representation“) – hielten (UNCTAD 2021: xix, xx): Die relevanten Konflikte und Kompromisse, so wurde weiter oben deutlich, wurden in bilateraler Runde oder kleineren Foren direkt betroffener und interessierter Akteuren ausgefochten und ausgehandelt. Es ist kaum zu erwarten, dass sich hieran in Zukunft viel ändern wird, auch wenn eine geographische Ausweitung auf relevante Akteure insbesondere in Asien wahrscheinlich erscheint. Aber internationales *institution building* erscheint heute nicht wahrscheinlicher als das vor zwanzig Jahren der Fall war.

Literatur

- Bach, David/Newman, Abraham L. (2007) The European Regulatory State and Global Public Policy: Micro-institutions, Macro-influence. *Journal of European Public Policy* 14, 827–846.
- Benkler, Yochai (2006) *The wealth of networks: How social production transforms markets and freedom*. New Haven; Conn.: Yale University Press.
- Bennett, Colin J. (1992) *Regulating privacy: Data protection and public policy in Europe and the United States*. Ithaca: Cornell University Press.
- Bennett, Colin J. (2008) *The privacy advocates: Resisting the spread of surveillance*. Cambridge; Mass.: MIT Press.
- Bennett, Colin J./Raab, Charles D. (2020) Revisiting the Governance of Privacy: Contemporary policy instruments in global perspective. *Regulation & Governance* 14, 447–464.
- Blyth, Mark (2009) *Routledge Handbook of International Political Economy (IPE): IPE as a Global Conversation*. London [u.a.]: Routledge.
- Bradford, Anu (2012) The Brussels Effect. *Northwestern University Law Review* 107, 1–68.
- Bradford, Anu (2020) *The Brussels Effect: How the European Union Rules the World*. New York, NY: Oxford University Press, USA.
- Breindl, Yana (2019) Internet Governance: Von der Selbstregulierung zu hybriden Regulierungsmodellen. In: Busch, Andreas/Breindl, Yana/Jakobi, Tobias (Hrsg.): *Netropolitik: Ein einführender Überblick*, Wiesbaden: Springer VS, 81–102.
- Buchanan, Ben/Imbrie, Andrew (2022) *The New Fire: War, Peace, and Democracy in the Age of AI*. Cambridge (MA): MIT Press.
- Busch, Andreas (2003) *Staat und Globalisierung: Das Politikfeld Bankenregulierung im internationalen Vergleich*. Wiesbaden: Westdeutscher Verlag.
- Busch, Andreas (2011) The Regulation of Privacy. In: Levi-Faur, David (Hrsg.): *Handbook on the Politics of Regulation*, Cheltenham UK; Northampton MA: Edward Elgar, 227–240.
- Busch, Andreas (2012a) Die Regulierung transatlantischer Datenströme: zwischen Diktat und Blockade? In: Busch, Andreas/Hofmann, Jeanette (Hrsg.): *Politik und die Regulierung von Information*, Baden-Baden: Nomos, 408–440.
- Busch, Andreas (2012b) The regulation of transborder data traffic: Disputes across the Atlantic. *Security and Human Rights* 23, 313–330.
- Busch, Andreas (2015) The Changing Architecture of the National Security State. In: Leibfried, Stephan/Huber, Evelyne/Lange, Matthew/Levy, Jonah/u. a. (Hrsg.): *The Oxford Handbook of Transformations of the State*, Oxford: Oxford University Press, 547–564.
- Busch, Andreas (2019) Untersuchungsgegenstand Internet. In: Busch, Andreas/Breindl, Yana/Jakobi, Tobias (Hrsg.): *Netropolitik: Ein einführender Überblick*, Wiesbaden: Springer VS, 17–51.

- Busch, Andreas/Plümper, Thomas (Hrsg.) (1999) *Nationaler Staat und internationale Wirtschaft: Anmerkungen zum Thema Globalisierung*. Baden-Baden: Nomos.
- Bygrave, Lee A. (2004) Privacy Protection in a Global Context – A Comparative Overview. *Scandinavian Studies in Law* 47, 319–348.
- Cortada, James W. (2012) *The digital flood: The diffusion of information technology across the U.S., Europe, and Asia*. Oxford: Oxford Univ. Press.
- Culpepper, Pepper D./Thelen, Kathleen (2019) Are We All Amazon Primed? Consumers and the Politics of Platform Power. *Comparative Political Studies* 53, 288–318.
- Deibert, Ronald (2012) The Growing Dark Side of Cyberspace (...and What To Do About It). *Penn State Journal of Law & International Affairs* 1, 260–274.
- Djeffal, Christian (2020) Künstliche Intelligenz. In: Klenk, Tanja/Nullmeier, Frank/Wewer, Göttrik (Hrsg.): *Handbuch Digitalisierung in Staat und Verwaltung*, Wiesbaden: Springer VS, 51–62.
- Farrell, Henry/Newman, Abraham L. (2019) *Of privacy and power: The transatlantic struggle over freedom and security*. Princeton NJ: Princeton University Press.
- Floridi, Luciano (2010) *Information: A very short introduction*. Oxford: Oxford Univ. Press.
- Floridi, Luciano (2014) *The 4th revolution: How the infosphere is reshaping human reality*. Oxford: Oxford Univ. Press.
- Gordon, Sarah/Ram, Aliya (2018) Information wars: How Europe became the world's data police. *Financial Times*.
- Hansen, Lene/Nissenbaum, Helen (2009) Digital disaster, cyber security, and the Copenhagen School. *International studies quarterly* 53, 1155–1175.
- Haunss, Sebastian/Ulbricht, Lena (2020) Staatliche Regulierung durch Big Data und Algorithmen. In: Klenk, Tanja/Nullmeier, Frank/Wewer, Göttrik (Hrsg.): *Handbuch Digitalisierung in Staat und Verwaltung*, Wiesbaden: Springer VS, 41–49.
- Heisenberg, Dorothee (2005) *Negotiating Privacy: The European Union, the United States, and Personal Data Protection*. Boulder (CO): Lynne Rienner Publishers.
- Jungherr, Andreas/Schroeder, Ralph (2021) *Digital Transformations of the Public Arena*. Cambridge University Press.
- König, Pascal D. (2020) Dissecting the Algorithmic Leviathan: On the Socio-Political Anatomy of Algorithmic Governance. *Philosophy & Technology* 33, 467–485.
- König, Pascal D./Wenzelburger, Georg (2020) Opportunity for renewal or disruptive force? How artificial intelligence alters democratic politics. In: *Government Information Quarterly* 37, 101489.
- Krishnamurthy, Vivek (2020) A Tale of Two Privacy Laws: The GDPR and the International Right to Privacy. In: *AJIL Unbound*.

- Kuehn, Kathleen M./Salter, Leon A. (2020) Assessing Digital Threats to Democracy, and Workable Solutions: A Review of the Recent Literature. *International Journal of Communication* 14, 2589–2610.
- Lambach, Daniel/Oppermann, Kai (2022) Narratives of digital sovereignty in German political discourse. *Governance*, 1–17 (doi: 10.1111/gove.12690).
- Levi-Faur, David (2011) Regulation and regulatory governance. In: Levi-Faur, David (Hrsg.): *Handbook on the Politics of Regulation*, Cheltenham UK; Northampton MA: Edward Elgar, 3–21.
- Mayer-Schönberger, Viktor/Cukier, Kenneth (2013) *Big data: A revolution that will transform how we live, work and think*. London: Murray.
- Mueller, Milton/Schmidt, Andreas/Kuerbis, Brenden (2013) Internet security and networked governance in international relations. *International Studies Review* 15, 86–104.
- Newman, Abraham L. (2011) Watching the Watchers: Transgovernmental Implementation of Data Privacy Policy in Europe. *Journal of Comparative Policy Analysis: Research and Practice* 13, 181–194.
- OECD (1981) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Paris, Washington DC: Organisation for Economic Co-operation; Development.
- OECD (2020) *OECD Digital Economy Outlook 2020*. Paris: OECD Publishing.
- Phillips, Nicola/Weaver, Catherine E. (Hrsg.) (2011) *International political economy: Debating the past, present and future*. London [u.a.]: Routledge.
- Pohle, Julia (2020) Digitale Souveränität. In: Klenk, Tanja/Nullmeier, Frank/Wewer, Göttrik (Hrsg.): *Handbuch Digitalisierung in Staat und Verwaltung*, Wiesbaden: Springer VS, 241–253.
- Reus-Smit, Christian/Snidal, Duncan (Hrsg.) (2008) *The Oxford handbook of international relations*. Oxford: Oxford Univ. Press.
- Rid, Thomas (2012) Cyber War Will Not Take Place. *Journal of Strategic Studies* 35, 5–32.
- Rohs, Bastian (2019) Sicherheit im Internet: Cybercrime, Cyberterror und Cyberwar. In: Busch, Andreas/Breindl, Yana/Jakobi, Tobias (Hrsg.): *Netropolitik: Ein einführender Überblick*, Wiesbaden: Springer VS, 303–332.
- Schneider, Ingrid (2019) Regulierungsansätze in der Datenökonomie. In: *Aus Politik und Zeitgeschichte* 24-26, 35–41.
- Schneider, Volker (2001) *Die Transformation der Telekommunikation: Vom Staatsmonopol zum globalen Markt (1800 - 2000)*. Frankfurt/Main: Campus-Verl.
- Schuenemann, Wolf J./Windwehr, Jana (2021) Towards a ‘gold standard for the world?’ The European General Data Protection Regulation between supranational and national norm entrepreneurship. *Journal of European Integration* 43, 859–874.
- Schwartz, Paul M. (2019) Global data privacy: the EU way. *New York University Law Review* 94, 771–818.

- Simon, Herbert A. (1971) Designing Organizations for an Information-Rich World. In: Greenberger, Martin (Hrsg.): Computers, communications, and the public interest, Baltimore: Johns Hopkins University Press, 38–52.
- Smelser, Neil J./Swedberg, Richard (Hrsg.) (2005) The Handbook of Economic Sociology. Princeton NJ; Oxford; New York: Princeton University Press / Russell Sage Foundation.
- Stone, Diane (2019) Making Global Policy. Cambridge: Cambridge University Press.
- UNCTAD (2018) Information Economy Report: 2017: Digitalization, Trade and Development. Information Economy Report.
- UNCTAD (2021) Digital Economy Report 2020: Cross-Border Data Flows and Development - for Whom the Data Flow. Geneva: United Nations.
- Vila Seoane, Maximiliano/Saguier, Marcelo (2020) Cyberpolitics and IPE: Towards a research agenda in the Global South. In: Vivares, Ernesto (Hrsg.): The Routledge Handbook to Global Political Economy: Conversations and Inquiries, New York: Routledge, 702–718.
- Vivares, Ernesto (Hrsg.) (2020) The Routledge Handbook to Global Political Economy: Conversations and Inquiries. New York: Routledge.
- Vogel, David (1986) National Styles of Regulation: Environmental Policy in Great Britain and the United States. Ithaca: Cornell University Press.
- Walter, Stefanie (2021) The Backlash Against Globalization. *Annual Review of Political Science* 24, 421–442.
- Zuboff, Shoshana (2015) Big other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology* 30, 75–89.
- Zuboff, Shoshana (2019) The age of surveillance capitalism: The fight for the future at the new frontier of power. London: Profile Books.