Deutschlands Rolle in Europas digitaler Ordnungsmacht: Gestaltung eines globalen Technologie-Regelwerks im Sinne Europas

Barker, Tyson; Hagebölling, David

Veröffentlichungsversion / Published Version
Sammelwerksbeitrag / collection article

Deutsche Gesellschaft für Auswärtige Politik e. V.

Oktober 2022

DGAP BERICHT

Deutschlands Rolle in Europas digitaler Ordnungsmacht

Gestaltung eines globalen Technologie-Regelwerks im Sinne Europas

Tyson Barker
Leiter, Programm Technologie und Außenpolitik

Dr. David Hagebölling
Associate Fellow, Programm Technologie und Außenpolitik

KAPITELÜBERSICHT

Zentrale Erkenntnisse

1 Die Stärken und zuweilen auch die Grenzen des deutschen Einflusses auf die Regulierung digitaler Technologien lassen sich anhand von vier Elementen aufzeigen:

- Deutschland antizipiert die Regulierung digitaler Technologien durch die EU und versucht, vollendete Tatsachen zu schaffen.
- Deutschland nimmt überdurchschnittlich großen Einfluss auf die formalen Entscheidungsphasen der EU-Regulierungspolitik im Digitalbereich.
- Deutschland nutzt gleichzeitig die EU als Sprungbrett, um auf weltweite regulatorische Normen Einfluss zu nehmen.
- Deutschland entdeckt die Bedeutung der deutschen Privatwirtschaft und der mit ihr assoziierten technischen Normungsgremien zur Prägung globaler technischer Vorschriften allmählich wieder.

2 Als EU-Mitgliedstaat engagiert sich Deutschland in drei wichtigen Bereichen der Datenverwaltung und Cybersicherheit: digitale Identitäten und offene Daten, rechtmäßiger Zugang zu elektronischen Messaging-Diensten und Regeln für die Nutzung souveräner Cloud-Dienste.

3 Die weitgehend erfolgreiche Rolle Deutschlands als wichtiger Impulsgeber für den regulatorischen Ansatz der EU im Bereich der digitalen Technologien, und damit als Triebfeder des „Brüssel-Effekts" bei der Gestaltung der globalen Märkte, wird hierzulande wenig anerkannt oder verstanden. Die Diskrepanz zwischen Regulierung, Technologie und internationalem Kontext zeigt sich in Bereichen wie Datenschutz, Inhaltsmoderation und Marktmacht von Online-Plattformen. Selbst substanzielle Debatten zur Regulierung von Quantencomputing, Metaverse (AR/VR) und 6G lassen in Deutschland noch auf sich warten.

4 Deutschland muss seinen Ansatz im Bereich der Digital-Regulierung ändern, um dem dynamischen und universellen Charakter aufkommender digitaler Technologien besser zu entsprechen – insbesondere in einem zunehmend angespannten internationalen Umfeld, in dem technische Regeln eine Komponente geopolitischer Macht darstellen. Dazu gehört: *erstens*, dass die politischen Zielkonflikte, die mit den Entscheidungen zur Regulierung digitaler Technologien verbunden sind, direkt adressiert werden; *zweitens*, dass die Überprüfungen und Auslaufklauseln in diesem Bereich ausgeweitet werden, um Flexibilität zu fördern; und *drittens*, dass Möglichkeiten zur Durchsetzung von Regeln unter Einbeziehung der Zivilgesellschaft, von Unternehmen und anderen nichtstaatlichen Akteuren stärker genutzt werden. Deutschland muss auch das Engagement seiner außen- und sicherheitspolitischen Gemeinschaft in der EU-Technologiediplomatie und bei der globalen Durchsetzung von Regeln verstärken.

Einleitung

Deutschland ist eine wichtige – vielleicht sogar die wichtigste – Kraft bei der Gestaltung des EU-Regulierungsansatzes für digitale Technologien, welcher eine wichtige Grundlage für Europas Macht im geopolitischen Technologie-Wettbewerb bildet. Deutschland steht im Mittelpunkt der ehrgeizigen Bemühungen der EU, Digital-Regulierung mit Menschenrechten, Rechtsstaatlichkeit und Demokratie zu verbinden. Diese Regulierung von Plattformen, Algorithmen und Daten ist im EU-Gesetz über digitale Dienste (Digital Services Act, DSA), im Gesetz über digitale Märkte (Digital Market Act, DMA), im Daten-Governance-Gesetz (Digital Governance Act, DGA), im Gesetz über künstliche Intelligenz (Artificial Intelligence Act, AI Act), im Datengesetz (Data Act) und im EU Cloud Rulebook festgelegt.[1] Deutschlands zentrale Rolle bei der Gestaltung dieser Regeln bedeutet, dass es der EU nur dann gelingen wird, ihr Regelwerk zu aktualisieren, wenn auch Deutschland seine Denkansätze an die neuen Gegebenheiten anpasst. Das bedeutet unter anderem, dass die Bundesregierung anerkennen muss, dass Regulierung zu einer geopolitisch bedeutsamen Komponente geworden ist, andere Staaten ein teils abweichendes Gleichgewicht zwischen Regulierung und Innovation wählen und somit manchmal Vorteile aus den Kosten ziehen, die der EU als re-

1 Tyson Barker, „2021 Is the Year the Internet Gets Rewritten", Foreign Policy, 19. Januar 2021: https://foreignpolicy.com/2021/01/19/2021-is-the-year-the-internet-gets-rewritten/ (abgerufen am 1. Juni 2022).

gulatorische Vorreiterin entstehen. Während Europa die nächste Welle der Daten-Governance in der Cloud, im Edge Computing und im Internet der Dinge (IoT) in Angriff nimmt, haben Deutschland und damit auch die EU die Chance, einen Rechtsrahmen zu schaffen, der europäische Werte und die globale Wettbewerbsfähigkeit fördert.

Status quo

Deutschland ist auf nationaler und vor allem auf EU-Ebene ein selbstbewusster, beharrlicher und kompetenter Akteur bei der Ausgestaltung digitaler Ordnungspolitik. Deutschland kennt die Hebel der Regulierungsmacht im Bereich der digitalen Technologien in Brüssel und hat über verschiedene Kanäle – Bund und Länder, Privatsektor und die deutsche Zivilgesellschaft – die Möglichkeit, das europäische Regelwerk so zu gestalten, dass es mit einem ordoliberalen, regelzentrierten Ansatz für digitale Souveränität vereinbar ist. Hinsichtlich der Strahlkraft dieses Ansatzes für die Regulierung digitaler Technologien weltweit, bleibt das deutsche Bewusstsein jedoch nach wie vor wenig ausgeprägt. Die Stärken und zuweilen auch die Grenzen der deutschen Einflussnahme auf die Regulierung digitaler Technologien lassen sich anhand von vier Elementen aufzeigen.

Erstens versucht Deutschland immer wieder, die Entwicklung der EU-Regulierung in Hinblick auf die digitale Sphäre zu antizipieren und diesbezügliche Debatten in Brüssel auf seine eigenen Bedürfnisse hin auszurichten, und das vermutlich mehr als jeder andere Mitgliedstaat. Die EU ihrerseits neigt wiederum dazu, die deutsche Debatte zu verfolgen, um den Weg für eine reibungslose rechtliche Verankerung ihrer eigenen Prioritäten zu ebnen. Folglich sind deutsche Rechtstraditionen (z. B. beim Festlegen des Datenschutzes als Grundlage für die Datenschutz-Grundverordnung (DSGVO))[2] und ordoliberales Denken (z. B. die Skepsis gegenüber Kartellen und digitaler Marktkonzentration) auf EU-Ebene sehr einflussreich. Gleichzeitig befindet sich Deutschland in einer Art Echokammer und ist der Ansicht, dass seine eigenen Prioritäten auch auf europäischer Ebene Vorrang haben – und nicht etwa die grenzüberschreitende Liberalisierung digitaler Dienste mit gleichgesinnten Nicht-EU-Staaten oder ein stärkerer regulatorischer Fokus auf die Cyberrisiken der von staatlich kontrollierten, chinesischen Unternehmen entwickelten IKT-Infrastruktur.

Natürlich spiegelt das EU-Regelwerk nicht immer die deutschen Prioritäten wider, und andere Akteure – etwa die Europäische Kommission, das Europäische Parlament, der Privatsektor, einschließlich US-Technologieunternehmen, und andere Mitgliedstaaten wie Frankreich und die technikbegeisterten nordischen und baltischen Staaten sowie Irland – beeinflussen in der Regel den Übergang von der EU-Debatte zur Gesetzgebung. Ein Beispiel dafür sind die Widersprüche zwischen dem DMA und der zehnten Novelle des deutschen Gesetzes gegen Wettbewerbsbeschränkungen. Gleiches trifft auch auf die Widersprüche zwischen der DSA-Regelung bezüglich illegaler Inhalte und dem deutsche Netzwerkdurchsetzungsgesetz (NetzDG) zu. Dennoch ist die deutsche Vorwegnahme der rechtlichen Debatten in der EU in fast jeder Hinsicht von Berlins digitaler Technologiepolitik geprägt – von der Prüfung ausländischer Direktinvestitionen (FDI/ADI) bis hin zur Sorgfaltspflicht im Bereich der Technologielieferketten.[3] So hat die deutsche Datenethikkommission (DEK) 2017 einen Rahmen für KI-Risikokategorien und -bewertung entworfen, der sich im KI-Whitepaper der EU 2020 und im Entwurf des EU AI Act wiederfindet.[4] Das deutsche IT-Sicherheitsgesetz 2.0 und Gaia-X haben jeweils die EU-Diskussion über die Richtlinie zur Netz- und Informationssicherheit 2 (NIS 2) und das europäische Cybersicherheit-Zertifizierungssystem für Cloud-Dienste (EUCS) angestoßen.

Zweitens ist Deutschland auch als größter Mitgliedstaat der EU in der digitalen Ordnungspolitik überrepräsentiert. Deutsche besetzen Schlüsselpositionen als Beamtinnen und Beamten in der Europäischen Kommission, als gut positionierte Administratorinnen und Administratoren des Europäischen Rates und als Mitglieder des Europäischen Parlaments (MdEP), die als Berichterstatterinnen und Berichter-

2 Informationelle Selbstbestimmung.

3 Bundesministerium für Arbeit und Soziales, „CSR-Supply Chain Act", (22. Juli 2021): https://www.csr-in-deutschland.de/EN/Business-Human-Rights/Supply-Chain-Act/supply-chain-act.html (abgerufen am 1. Juni 2022).

4 Tyson Barker, „The Digital Technology Environment and Europe's Capacity to Act", DGAP Report No. 7, Deutsche Gesellschaft für Auswärtige Politik (November 2021), S. 23: https://dgap.org/sites/default/files/article_pdfs/Mercator%20Study%20Tech_Highres.pdf (abgerufen am 1. Juni 2022).

statter für wichtige Gesetzespakete[5] und als einflussreiche Ausschussvorsitzende[6] dienen sowie als wichtige Mitarbeiterinnen und Mitarbeiter des Parlamentssekretariats. Obwohl viele dieser Offiziellen ein breites ideologisches Spektrum repräsentieren, bewahren sie sich eine deutsche politische Sensibilität. Nur Frankreich kann mit Deutschland mithalten, was den Einsatz von Personal zur Gestaltung der digitalen Ordnungspolitik der EU angeht, insbesondere in der Kommission (z. B. DG CONNECT) und in wichtigen Aufsichtsbehörden wie dem Gremium Europäischer Regulierungsstellen für elektronische Kommunikation (GEREK).

Zuweilen spiegeln diese Beamtinnen und Beamten sowie Vertreterinnen und Vertreter die Interessen deutscher Institutionen wider, einschließlich wichtiger deutscher Unternehmen.[7] Dies ist an sich kein Problem, sondern eher ein natürlicher Nebeneffekt, der auf das komplexe Zusammenwirken der deutschen Europapolitik in Brüssel und des politischen Diskurses der deutschen Wirtschaft zurückzuführen ist. Unternehmen können Deutschlands Stellung im Digitalbereich stärken. Ohne ausreichendes Gegengewicht besteht jedoch das Risiko, dass sie den deutschen Einfluss auf eng gesteckte Unternehmensziele umlenken. Und, was noch problematischer ist: Dies könnte zu gemeinsamen unternehmensstrategischen Schwachstellen führen. Dazu gehört auch eine erhöhte Anfälligkeit gegenüber möglichen Vergeltungsmaßnahmen Chinas für behördliche Prüfungen der Datenverarbeitungs- und Cybersicherheitspraktiken chinesischer Unternehmen, die in der EU tätig sind. Unternehmen in Australien, Kanada und dem Vereinigten Königreich, Deutschlands Verbündete außerhalb der EU, sind darüber weniger besorgt, da sie nicht so stark vom chinesischen Markt abhängig sind. Aufgrund der Marktabhängigkeit von China ist Deutschland gezwungen, ein Gleichgewicht zwischen seinem Bedarf an chinesischen Verbraucherinnen und Verbrauchern und seinem Engagement für seine eigenen Werte im Bereich der digitalen Technologien zu finden.

Internationale und geopolitische Belange prägen zwar die deutsche und europäische digitale Ordnungspolitik, doch sind diese auch noch immer von früheren Erfahrungen mit den USA und Misstrauen in Bezug auf Datenschutz und Spionage geprägt. Seit den Enthüllungen rund um die National Security Agency (NSA) durch den Whistleblower Edward Snowden 2013 richten sich die deutschen Bedenken hinsichtlich des Datenschutzes vor allem auf die USA. Jüngste EU-Initiativen – insbesondere der DSA, DMA und Vorschläge bezüglich Cloud – betreffen aufgrund ihrer Marktdominanz hauptsächlich amerikanische Technologieunternehmen. Aber der Grad, zu dem dies als Mittel zur Einschränkung des technologischen Einflusses der USA wahrgenommen wird, kann Fragen aufwerfen. Die unverhältnismäßige Konzentration auf die USA entspricht nicht den heutigen geopolitischen Bedrohungen (Box 1). Der ko-regulatorische Ansatz und die weitreichenden Durchsetzungsbefugnisse der Kommission gemäß DSA und DMA schaffen in beiden Fällen die nötige Flexibilität, um den neuen Risiken in den sich ständig verändernden Online-Informationsökosystemen und der Dynamik der Marktmacht der Plattformen Rechnung zu tragen. Sobald DSA und DMA in Kraft treten, wird sich konkret zeigen, inwieweit diese für die Plattformlandschaft des Jahres 2023, und nicht des Jahres 2015, geeignet sind.

Drittens ist die EU für Deutschland und andere Mitgliedstaaten ein Sprungbrett, um weltweit auf Regulierung Einfluss zu nehmen. Bei globalen Technologieunternehmen wurde die Datenschutz-Grundverordnung der EU bekanntlich zur Referenz für Datenschutz, und das auch in Ländern außerhalb der EU. Vier Jahre nach Inkrafttreten der DSGVO nutzen Länder wie Argentinien, Südkorea, Japan und Kenia sowie subnationale Regierungen wie die von Kalifornien mit ihrem California Privacy Rights Act (CPRA) die DSGVO als Grundlage für ihre eigenen Datenschutzbestimmungen. Selbst der wachsende Druck auf Washington, ein föderales US-Datenschutzgesetz zu erlassen, geht zum Teil von Europa aus. Und das Schrems-II-Urteil aus dem Jahr 2020, mit dem der Europäische Gerichtshof das Privacy Shield-Abkommen aus dem Jahr 2016 für die transatlantische Übermittlung personenbezogener Daten für unwirksam erklärte, zwang die USA dazu, erhebliche Änderungen vorzunehmen, um Beschwerden aus Europa nachzukommen und Kontrollen der Datenerfassung durch Geheimdienste zu verschärfen. Die EU hat als Vorreiterin in Sachen Regulierung die globale Regulierungslandschaft in Richtung ihres Modells geprägt. Das ist für Deutschlands Anliegen zwar vorteilhaft, birgt aber auch Nachteile. Viele Nicht-EU-Staaten und die meisten EU-Mitgliedstaaten tun sich schwer damit, die Bestimmungen der Datenschutz-Grundverordnung

5 Zum Beispiel von DSGVO, DMA und der NIS-Richtlinie.
6 Zum Beispiel von dem Ausschuss für Binnenmarkt und Verbraucherschutz und dem Ausschuss für internationalen Handel.
7 Wie zum Beispiel Deutsche Telekom, SAP, Infineon, Bosch, Axel Springer und Bertelsmann.

DEUTSCHLANDS STARKER USA-FOKUS

Die transatlantischen Technologiebeziehungen sind nach wie vor die Hauptschlagader der digitalen Welt. Die Unterseekabel, die den Nordatlantik durchqueren, übertragen 55 Prozent mehr Daten als die transpazifischen Unterseekabel. Allerdings verschieben sich die globalen digitalen Aktivitäten, wie auch wirtschaftlichen Aktivitäten, von den USA in den indopazifischen Raum und in den globalen Süden, auch wenn Deutschland bei der Durchsetzung von Vorschriften weiterhin stark auf den Atlantik ausgerichtet ist.

Die Datenstrategie Deutschlands vom Januar 2021 konzentrierte sich stark auf Gaia-X als Mittel zur Emanzipation Europas von US-Cloud-Diensten (und den Bestimmungen des Gesetzes Clarifying Lawful Overseas Use of Data (CLOUD), das US-Behörden den Zugriff auf bestimmte Daten in anderen Ländern ermöglicht), zum Teil durch den Einsatz von Open-Source-Software wie OpenStack. Der aktuelle deutsche Diskurs über Datenlokalisierung, Plattformabhängigkeit und Verschlüsselung wird nach wie vor von den Enthüllungen rund um die NSA, die Wahl des ehemaligen US-Präsidenten Donald Trump im Jahr 2016 und dem Cambridge-Analytica-Skandal im Jahr 2017 überschattet.

Die Bemühungen der EU um die Durchsetzung von Rechtsvorschriften konzentrieren sich ebenfalls hauptsächlich auf den euro-atlantischen Raum. Die Durchsetzung der DSGVO durch die 17 deutschen Datenschutzbehörden (DSB) richtet sich nach wie vor primär gegen US-Dienstleister und -Plattformen. Dies war angesichts der dominierenden Rolle der US-amerikanischen digitalen Dienste auf dem europäischen Markt in den letzten zehn Jahren gerechtfertigt. Der Fokus auf die Überprüfung von US-Technologieunternehmen steht jedoch im Gegensatz zu der mangelnden Prüfung von systematischen Verstößen durch Unternehmen aus Staaten mit Angemessenheitsbeschluss wie dem Vereinigten Königreich, Kanada und Japan und sogar durch europäische Unternehmen selbst. Am interessantesten ist vielleicht die verhältnismäßig unzureichende Prüfung systematischer Verstöße, insbesondere in Bezug auf Anforderungen für rechtmäßigen Zugriff, durch autoritäre Staaten wie China und Russland.

Es gibt jedoch einige Anzeichen dafür, dass der Fokus langsam von den USA abrückt. Der Entwurf der EU für eine KI-Verordnung, der von der deutschen EU-Ratspräsidentschaft 2020 und der Datenethikkommission der Bundesregierung mit erarbeitet wurde, schenkt den chinesischen Praktiken größere Aufmerksamkeit als frühere ähnliche EU-Verordnungen. Die strengsten Bestimmungen des Kommissions-Entwurfs betreffen das Sozialkreditsystem, welches die Verordnung verbietet, und die biometrische Fernidentifizierung in Echtzeit, die nur Strafverfolgungsbehörden in streng definierten Situationen nutzen dürfen. Diese Maßnahmen beziehen sich implizit auf das Vorgehen Chinas. Die Förderung konformen Verhaltens ist seit langem kennzeichnendes Element der chinesischen Gesellschaft, aber die KI-gestützte biometrische Identifizierung in Kombination mit umfassender Videoüberwachung und einem Sozialkreditsystem bildet ein mächtiges und gefährliches Instrument zur sozialen Kontrolle.

einzuhalten, was freie Datenflüsse erschwert. Darüber hinaus stehen der EU andere, potenziell vielversprechendere Wege offen, um ein international anwendbares Regelwerk zu erarbeiten.

Die EU und gleichgesinnte Staaten wie Australien, Kanada und das Vereinigte Königreich haben einen (zwischenstaatlichen) Regulierungsdiskurs in Bereichen begonnen, die über den Datenschutz hinausgehen. Zu diesen Bereichen gehören Inhaltsmoderation, Plattform-Governance, die Marktmacht einzelner Unternehmen, Datenschutz und risikobasierte KI-Ansätze. Dies ist jedoch ein mühsames Unterfangen, da Unterschiede in den internen Gesetzgebungsverfahren, den Regulierungskompetenzen, den föderalen Strukturen und den verfassungsrechtlichen Grenzen zu unterschiedlichen Ergebnissen führen.

Gleichzeitig hat China gelernt, die Regulierungsprinzipien der EU zu kopieren, um weit weniger

hochgesinnte Ziele zu verfolgen. Chinas Diskurs über die Marktmacht der Technologieriesen und Datenschutz spiegelt die Debatte in Deutschland und Europa, doch mit dem Ziel, internationale Kritik zu beschwichtigen und gleichzeitig die absolutistische Macht der Kommunistischen Partei zu festigen. Das chinesische Anti-Sanktionsgesetz von 2021, das exterritoriale Sanktionen innerhalb des Landes außer Kraft setzt, wurde dem EU-Recht nachempfunden.[8] Chinesische Vorschriften zum Schutz personenbezogener Daten (einschließlich der Globalen Initiative für Datensicherheit 2020),[9] zum Wettbewerb, zu Algorithmen und zuletzt zur Content-Governance mit „positiver Energie“[10] lehnen sich an europäische Überlegungen an und übernehmen mitunter sogar den Wortlaut des Unionsrechts. Dennoch zielen diese Bemühungen darauf ab, den chinesischen Technologiesektor und andere Akteure in den Dienst parteistaatlicher Interessen zu stellen.

Viertens wäre Europas Gestaltungsmacht ohne Deutschlands Einfluss und den seines Privatsektors in globalen technischen Normungsgremien viel geringer. Das Deutsche Institut für Normung e.V. (DIN), die Deutsche Kommission Elektrotechnik Elektronik Informationstechnik e.V. (DKE) und der Verband der Elektrotechnik Elektronik Informationstechnik e.V. (VDE) bilden einen Kern nationaler Gremien, deren Arbeit in ihre europäischen und internationalen Pendants einfließt. Deutschland ist eines von sechs ständigen Mitgliedern des Rates der Internationalen Organisation für Normung (ISO) und stellt 18 Prozent der ISO-Sekretariate, 19 Prozent der Sekretariate der Internationalen Elektrotechnischen Kommission (IEC) und 29 Prozent der IEC-Arbeitsgruppenvorsitzenden.[11] Es stellt auch Kandidaten für Schlüsselpositionen auf, wie zum Beispiel für den Posten des Direktors des Sektors für Telekommunikationsnormung der Internationalen Fernmeldeunion (ITU) im Jahr 2022.[12]

Aber so wie sich Deutschland manchmal des großen Einflusses seines Privatsektors auf die europäische Regulierung nicht bewusst ist, so hat es den relativen Rückgang seines Einflusses – und folglich desjenigen der EU – bei der internationalen Standardsetzung nur langsam erkannt. Die Rolle des deutschen Privatsektors ist geschrumpft, seitdem insbesondere chinesische Staatsunternehmen und dem Staat nahestehende Unternehmen die Kontrolle über wichtige technische Arbeitsgruppen erlangt und Musternormen eingebracht haben.[13] Chinas Drängen auf regionale Standardsetzungsvereinbarungen im Rahmen seiner Seidenstraßeninitiative könnte auch zu Lock-in-Effekten für Drittländer führen, die zu einem merkantilistischen digitalen internationalen System neigen, das China und den digital gestützten Autoritarismus begünstigt. Dies ist Teil eines umfassenderen Plans, den Henry Kissinger als Chinas „geduldige Anhäufung relativer Vorteile“ bezeichnet hat.[14] Deutschland hat, wie der Rest Europas, erst spät erkannt, dass die technische Normung mit geopolitischen Risiken behaftet ist, und dies zu einer Zeit, in der die Beteiligung des deutschen Privatsektors in internationalen Normungsgremien bereits zurückgegangen ist

Aktueller politischer Ansatz

Die derzeitige Debatte der Bundesregierung über die Regulierung digitaler Technologien konzentriert sich auf eine Reihe von Fragen der Daten-Governance und der Cybersicherheit im Zusammenhang mit der nahtlosen digitalen Interaktion mit der öffentlichen Verwaltung, dem rechtmäßigen Zugang zu elektronischen Messaging-Diensten und Regeln für die Nutzung souveräner Cloud-Dienste. Damit ändert sich der Schwerpunkt im Vergleich zu den jüngsten EU-

8 Kelly Austin et al., „China’s ‚Blocking Statute‘ – New Chinese Rules to Counter the Application of Extraterritorial Foreign Laws“ Gibson Dunn, 13. Januar 2021: https://www.gibsondunn.com/chinas-blocking-statute-new-chinese-rules-to-counter-the-application-of-extraterritorial-foreign-laws/ (abgerufen am 1. Juni 2022).

9 Botschaft der Volksrepublik China in den Vereinigten Staaten von Amerika, „Global Initiative on Data Security“, 8. September 2020: https://www.mfa.gov.cn/ce/ceus//eng/zgyw/t1812951.htm (abgerufen am 1. Juni 2022).

10 Maria Siow, „Positive energy: the darker side of China’s social media catchphrase“, South China Morning Post, 21. Juni 2020: https://www.scmp.com/week-asia/people/article/3089846/positive-energy-darker-side-chinas-social-media-catchphrase (abgerufen 1. Juni 2022).

11 Deutsches Institut für Normung, „DIN“, 4. August 2022: https://www.iso.org/member/1511.html (abgerufen am 10. August 2022).

12 Internationale Fernmeldeunion, „Elections“, (2022): https://www.itu.int/pp22/en/elections/candidates/ (abgerufen am 1. Juni 2022).

13 Tim Rühlig, „Technical standardisation, China and the future international order. A European perspective“, E-Paper, Heinrich Böll Stiftung Brussels (Februar 2020): https://eu.boell.org/sites/default/files/2020-03/HBS-Techn%20Stand-A4%20web-030320.pdf (abgerufen am 1. Juni 2022).

14 Tom McTague, „Joe Biden Has a Europe Problem“, The Atlantic, 21. Januar 2021: https://www.theatlantic.com/international/archive/2021/01/joe-biden-europe/617753/ (abgerufen am 1. Juni 2022).

Regulierungswellen insofern, als dass Datenschutz erheblich stärker als Aspekt von Cybersicherheit und weniger in Bezug auf staatliche und staatsnahe private Akteure eingeordnet wird. Dies könnte Gelegenheit für eine Neukalibrierung der Rolle Deutschlands auf europäischer Ebene bieten, um die demokratischen Grundsätze der Daten-Governance – und zwar auf flexible Weise und im Einklang mit dem deutschen Verständnis von digitaler Souveränität – zu definieren. Was genau unternimmt Deutschland also?

EIN DIGITAL BEFÄHIGTER STAAT

Erstens konzentrieren sich die deutschen Bemühungen auf der Nachfrageseite auf die Einführung sektorübergreifender und sicherer elektronischer digitaler Identitäten (eIDs), die auf den Erfahrungen der nordischen und baltischen EU-Mitgliedstaaten sowie der Ukraine basieren, die eIDs bereits eingeführt haben.[15] Das deutsche eID-Karte-Gesetz ist im September 2021 in Kraft getreten und hat die rechtliche Grundlage für digitale Identifikation über Smartphones mit sicherer und durch die Bundesdruckerei unterstützter Authentifizierungstechnologie geschaffen. Die Regierung hatte für Ende 2021 erste digitale ID-Dienste versprochen, die jedoch bisher nicht verfügbar sind. Auch bezüglich digitaler Führerscheine, ID-Wallets und Smart eIDs bestehen noch immer Probleme.[16] Auf der Angebotsseite verpflichtet das Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (OZG) aus dem Jahr 2017 Bund, Länder und Kommunen dazu, ihre Verwaltungsdienste bis Ende 2022 digital anzubieten – eine Frist, die die Regierungen auf allen politischen Ebenen wahrscheinlich nicht werden einhalten können.[17] Ziel des OZG ist es, Behördenportale miteinander zu verbinden, damit Unternehmen sowie Bürgerinnen und Bürger mit einem einzigen Benutzerkonto auf Online-Dienste zugreifen können.[18] Dabei besteht die Gefahr, dass bürokratische Verzögerungen bei der Umsetzung, mangelnde Koordination zwischen den Behörden und letztlich eine uneinheitliche und ungleichmäßige Datenverfügbarkeit auch zu einer suboptimalen Nutzung durch Forscherinnen und Forscher sowie den privaten Sektor führen.

RECHTMÄSSIGER ZUGRIFF AUF ONLINE-KOMMUNIKATION

Eine weitere erwähnenswerte Maßnahme ist der Versuch der deutschen Bundesregierung, Bedingungen festzulegen, unter denen Strafverfolgungsbehörden Messaging-Dienste dazu verpflichten können, Zugriff auf verschlüsselte Kommunikation zu gewähren – ein anhaltender Konfliktpunkt zwischen der Strafverfolgung und Ende-zu-Ende-Verschlüsselung. Dies steht seit der Veröffentlichung des FBI-Dokuments „Lawful Access“ vom Januar 2021 auch in der EU auf der Agenda: Aus diesem geht hervor, welche Daten Strafverfolgungsbehörden von verschiedenen Messenger-Diensten erhalten können.[19] Anbieter wie Apple, Signal und Telegram wehren sich weiterhin dagegen.[20]

Letztes Jahr kündigte die Europäische Kommission selbst einen Gesetzesentwurf zur „Chat-Kontrolle“ an, der schnell wieder von der Tagesordnung verschwand; möglicherweise aufgrund der massiven Proteste von mehr als 30 Organisationen aus der Zivilgesellschaft.[21] Doch im Mai 2022 legte die Kommission einen Vorschlag „zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern“ vor.[22] Da-

15 Das Bundesministerium für Wirtschaft und Klimaschutz schätzt, dass entwickelte Volkswirtschaften mit einer gut funktionierenden Infrastruktur für digitale Identitäten ihr Bruttoinlandsprodukt um 3 bis 4 Prozent steigern können. Bundesministerium für Wirtschaft und Klimaschutz, „Im Fokus: Sichere digitale Identitäten“, (Oktober 2021): https://www.bmwk.de/Redaktion/DE/Schlaglichter-der-Wirtschaftspolitik/2021/11/05-im-fokus-digitale-identitäten.html (abgerufen am 1. Juni 2022).

16 Viola Heeger, „Digitale Identitäten: Deutschland im Verzug“, Tagesspiegel Background Digitalisierung & KI, 20. December 2021: https://background.tagesspiegel.de/digitalisierung/digitale-identitaeten-deutschland-im-verzug (abgerufen am 1. Juni 2022).

17 Bundesministerium des Innern und für Heimat, „Onlinezugangsgesetz (OZG)“, (2022): https://www.bmi.bund.de/DE/themen/moderne-verwaltung/verwaltungsmodernisierung/onlinezugangsgesetz/onlinezugangsgesetz-node.html (abgerufen am 1. Juni 2022).

18 Auf europäischer Ebene enthält die eIDAS-Verordnung (Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt, mit der die Richtlinie 1999/93/EG aufgehoben wurde) europaweit verbindliche Regelungen in den Bereichen „elektronische Identifizierung“ und „elektronische Vertrauensdienste“. Die Verordnung schafft einen einheitlichen Rahmen für die grenzüberschreitende Nutzung nationaler elektronischer Identifizierungsmaßnahmen und damit auch für die Nutzung des deutschen Online-Ausweises und der Vertrauensdienste.

19 Martin Holland, „FBI über Messenger: An welche Daten von WhatsApp & Co. US-Strafverfolger kommen“, Heise Online, 2. Dezember 2021: https://www.heise.de/news/FBI-ueber-Messenger-An-welche-Daten-von-WhatsApp-Co-US-Strafverfolger-kommen-6282456.html?wt_mc=rss.red.ho.ho.atom.beitrag.beitrag (abgerufen 1. Juni 2022).

20 Der iMessage-Dienst von Apple bietet eine Ende-zu-Ende-Verschlüsselung und gibt Nutzerdaten nur auf Vorladung heraus, und Chat-Informationen sind nur verfügbar, wenn sie in iCloud gesichert wurden. Telegram kann mögliche IP-Adressen und Telefonnummern bereitstellen. Signal veröffentlicht nur Datum und Uhrzeit der letzten Nachricht. Bei WhatsApp, dem weltweit beliebtesten Messenger-Dienst, können die Ermittler jedoch auf Nutzerdaten, gesperrte Konten, Kontakte und Nachrichtenziele zugreifen.

21 Thomas Rudl und Markus Reuter, „Warum die Chatkontrolle so gefährlich ist“, Netzpolitik, 4. November 2021: https://netzpolitik.org/2021/eu-kommission-warum-die-chatkontrolle-so-gefaehrlich-ist/ (abgerufen am 1. Juni 2022).

22 Europäische Kommission, „Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse“, COM(2022)209 final, (Mai 2022): https://eur-lex.europa.eu/resource.html?uri=cellar:13e33abf-d209-11ec-a95f-01aa75ed71a1.0001.02/DOC_1&format=PDF (abgerufen 1. Juni 2022).

mit sollen insbesondere Anbieter interpersoneller Kommunikation in die Pflicht genommen werden, „Material über sexuellen Kindesmissbrauch aufzudecken, zu melden, zu sperren und aus ihren Diensten zu entfernen".[23] Dies könnte Nachrichten- und Hosting-Dienste wie WhatsApp und Signal dazu verpflichten, ihre Verschlüsselungsverfahren zu schwächen oder andere umstrittene Lösungen einzuführen, wie zum Beispiel Hash-Abgleiche oder das Scannen der Geräte von Endnutzerinnen und Endnutzern („Client-Side-Scanning" oder CSS).[24] Kritikerinnen und Kritiker behaupten, dass der Vorschlag die demokratischen Grundsätze untergrabe, indem er alle europäischen Bürgerinnen und Bürger unter Verdacht stelle und die Vertraulichkeit und Sicherheit des Internets unterminiere.

SOUVERÄNE CLOUD-DIENSTE UND INDUSTRIEDATEN

Die politischen Bemühungen in Deutschland und der EU kreisen um die Schaffung einer Cloud-Infrastruktur, die auf europäischen Regeln basiert und durch eine föderierte europäische Dateninfrastruktur ergänzt wird, die die Marktdominanz der Hyperscaler mit ihren enormen Datenverarbeitungskapazitäten durch Interoperabilitäts- und Portabilitätsanforderungen einschränken kann. Das Ziel ist letztlich, eine wettbewerbsfähige Cloud-Umgebung nach europäischen Regeln zu schaffen, die eine Grundlage für die Infrastruktur für das industrielle Internet und das Internet der Dinge bildet.

Ob dieser von Deutschland geleitete Cloud-Ansatz am Ende der eigenen ordoliberalen, regelzentrierten Vorstellung von digitaler Souveränität Nachdruck verleihen wird, bleibt unklar. Gaia-X, ein industriegetriebenes Spin-off einer deutsch-französischen Regierungsinitiative, ist eine Option für eine interoperable Cloud-Standardarchitektur für Europa und vielleicht auch darüber hinaus. Doch die Ausrichtung von Gaia-X auf eine regelbasierte digitale Souveränität sowie die Einbeziehung US-amerikanischer und chinesischer Akteure in die Governance, hat die Erwartungen einiger europäischer Akteure – auch in Frankreich – nicht erfüllt. Dies hat einige europäische Akteure dazu veranlasst, konkurrierende Initiativen wie die European Cloud Industrial Alliance (EUCLIDIA) und das EUCS zu gründen. Diese stützen sich auf das französische Cloud-Zertifizierungssystem SecNumCloud, das die öffentliche Verwaltung von außereuropäischen Cloud-Anbietern abschirmen soll. Trotz der Ankündigung verwandter Dienste wie einer föderierten Cloud-Infrastruktur-Architektur (Structura-X) und sektorspezifischer Kooperationen in den Bereichen Mobilität (Catena-X), Landwirtschaft (AgriGaia) und Finanzwesen (EuroDat) scheint Gaia-X mit den Mängeln früherer ähnlicher Bemühungen zu kämpfen: geringe Akzeptanz, unsichere private Nachfrage und schwindende politische Unterstützung in Deutschland.

Unterdessen nehmen die Diskussionen über die Datenlokalisierung in Deutschland zu. Internationale Datenströme sind nach wie vor umstritten und spiegeln Deutschlands Ambivalenz in Bezug auf den Wert und Nutzen von Datenzugang wider. Neben einigen Vertreterinnen und Vertretern der deutschen Regierung, Politikerinnen und Politikern, Rechtsexpertinnen und Rechtsexperten sowie NGOs in Deutschland gibt es auch in Frankreich Stimmen, die infrage stellen, ob US-Cloud-Anbieter sensible Daten überhaupt speichern sollten. Ihre Bedenken betreffen die Ungewissheit über den Datenschutz bei der transatlantischen Datenübermittlung nach dem Schrems-II-Urteil und die Ermächtigung der US-Strafverfolgungsbehörden im Rahmen des US CLOUD Act auf Daten zuzugreifen, die auf Servern von US-Cloud-Anbietern in Europa gespeichert sind.[25]

Deutschland erwägt daher Regeln für die Cloud-Nutzung in der Verwaltung und in sensiblen Bereichen, da die EU ein Cloud-Zertifizierungsverfahren einführen möchte, das Fragen bezüglich Datenlokalisierung berücksichtigt. Deutschland schloss sich Frankreich, Italien und Spanien an – gegen die Niederlande, Schweden und Irland – und unterstützte die „Souveränitätsanforderungen" im EUCS und dem Gaia-X-Labelling-Framework, die im Wesentlichen Datenlokalisierung als Anforderung unterstützen. Die höchsten Sicherheitsstufen von EUCS und Gaia-X, nämlich „Hoch" und „Stufe 3", würden die Auswahl an Providern einschränken und die EU möglicherweise von Hyperscalern wie Amazon, Microsoft und Google, die ihren Sitz in den Vereinigten Staaten

23 Ebd., S. 2.

24 Stefan Krempl, „Chatkontrolle: Informatiker und IT-Verbände gegen EU-weite Massenüberwachung", Heise Online, 29. März 2022: https://www.heise.de/news/Chatkontrolle-Informatiker-und-IT-Verbaende-gegen-EU-weite-Massenueberwachung-6656545.html (abgerufen am 1. Juni 2022).

25 Einige haben sogar den Grad der Kontrolle durch die chinesische Firewall als positives Modell für ein europäisches Internet angeführt. Nick Sohnemann et al., „New Developments in Digital Services", Europäisches Parliament, Fachabteilung Wirtschaft, Wissenschaft und Lebensqualität der Generaldirektion Interne Politikbereiche der Union (Mai 2020): https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648784/IPOL_STU(2020)648784_EN.pdf (abgerufen am 11. März 2021).

haben, sowie von europäischen Unternehmen mit amerikanischer Präsenz, darunter die Deutsche Telekom, SAP und Bertelsmann, abschneiden. Obwohl diese Zertifizierungssysteme derzeit noch freiwillig sind, wird davon ausgegangen, dass sie in Zukunft in irgendeiner Form für die Erbringung öffentlicher Dienstleistungen in der EU erforderlich sein werden – mit schwerwiegenden Auswirkungen auf die Datennutzung in digitalen Lieferketten. Digitale Smart-City-, Gesundheits- und Bildungsdienste gehören zu den Bereichen, die davon betroffen sein werden.

DEUTSCHLANDS GEOPOLITISCHE SCHWACHPUNKTE IN DER REGULIERUNG

Während sich die deutsche Politik in den Bereichen digitale Identität, Cybersicherheit, Strafverfolgung und Cloud-Governance weiterentwickelt, sind drei Schwachpunkte offensichtlich. Diese können Deutschlands Fähigkeit und die der EU, Governance und Innovation in Einklang zu bringen sowie ihre Gestaltungskraft zu maximieren, beeinträchtigen.

Erstens wird die weitgehend erfolgreiche Rolle Deutschlands als wichtiger Impulsgeber für den regulatorischen Ansatz der EU im Bereich der digitalen Technologien – und damit als Triebfeder des „Brüssel-Effekts" bei der Prägung globaler Märkte – in Deutschland selbst kaum anerkannt oder verstanden. Vielmehr ist die deutsche Technologiediskussion nach innen gerichtet und beachtet kaum, welchen Einfluss Deutschland auf die EU und die Welt haben. Die Politik überlässt es oft den Technokraten, reaktiv nationale Präferenzen auf europäische Ebene zu heben. Die Debatte neigt auch dazu, die potenziell globalen Auswirkungen deutscher Regularien auszublenden, und es gelingt ihr nicht, die deutschen Vorbehalte in Bezug auf Digitalisierung und Datenflüsse, die weiterhin im EU-Recht zum Ausdruck kommen, konsequent zu adressieren.

Zweitens gibt es nach wie vor geopolitische Herausforderungen im Zusammenhang mit der Umsetzung und Durchsetzung bestehender Regularien, insbesondere der DSGVO, des DSA und des DMA, was eine Diskrepanz zwischen Vorschriften und dem Kontext, in dem sie festgelegt wurden, widerspiegelt. Der überwiegend euro-atlantische Fokus deutscher und europäischer Rechtsdurchsetzung entspricht dem internationalen digitalen Status quo zwischen 2012 und 2015. Seitdem sind chinesische und russische staatsnahe Akteure zu bedeutenden Anbietern von Cloud-Diensten, Plattformdiensten, geschlossenen Messaging-Systemen und intelligenter Infrastrukturtechnologie geworden. Auch das Internet der Dinge hat an globaler Bedeutung gewonnen. Die Durchsetzung der Rechtsvorschriften konnte nicht Schritt halten, was in Deutschland und Europa zu Schwachstellen in der Digital-Governance geführt hat.

Drittens kommt die Gestaltung von Regeln für neue Technologien in Deutschland regelmäßig nur langsam zustande, obwohl das Land in der Lage ist, die EU-Debatte zu antizipieren. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat erstmals ein Grundschutz-Profil für die Cybersicherheit von LEO-Satelliten-Netzwerken herausgegeben, die als Grundlage für Modellstandards der Europäischen Weltraumorganisation dienen sollen.[26] Und die öffentlich finanzierte Forschung und Entwicklung im Bereich der Quantenverschlüsselung wird dazu beitragen, Standards für die Post-Quanten-Kryptografie zu entwickeln, auch in Zusammenarbeit mit Partnern wie dem US National Institute of Standards and Technology (NIST).[27] Nichtsdestotrotz gibt es zwischen technologischer Entwicklung und Governance in Deutschland, Europa und gleichgesinnten Staaten nach wie vor eine ausgeprägte Diskrepanz. Dies ist für das von Deutschland und Europa gewünschte strategische Regulierungsumfeld kaum förderlich. Da die Marktgröße Deutschlands und der EU im Vergleich zum Rest der Welt schrumpft, nimmt auch ihre Regulierungsmacht ab. Mittelfristig wird der wachsende Einfluss der Nachfrage in Indien und im globalen Süden ihre Rolle bei der Festlegung globaler Regeln, Normen und ihre Marktmacht neu definieren.

Handlungs-empfehlungen

Drei Faktoren sind ausschlaggebend dafür, ob die Bundesregierung in der Lage sein wird, die globale Regelsetzung zu beeinflussen: die Kohärenz ihrer

26 Catherine Stupp, "Germany Offers Model for Space-Industry Cybersecurity Standards," The Wall Street Journal, 17. August 2022: https://www.wsj.com/articles/germany-offers-model-for-space-industry-cybersecurity-standards-11660728604 (abgerufen am 12. September 2022)

27 Barbara-Henrika Alfing, "Bochum researchers win worldwide post-quantum cryptography competition", Ruhr Universität Bochum, 6. Juli 2022: https://news.rub.de/english/press-releases/2022-07-06-future-proof-data-encryption-bochum-researchers-win-worldwide-post-quantumcryptography-competition (abgerufen am 12. September 2022)

Vision, die Beständigkeit bei der Regeldurchsetzung in Deutschland und in der EU sowie die Fähigkeit, Vorschriften zu erlassen, die die europäische Innovationsfähigkeit (auch für neue kritische Technologien) bewahren und stärken, ohne protektionistischen Tendenzen Vorschub zu leisten. Um deutsche Regeln und Normen in einen konsequenteren geostrategischen Ansatz einzubetten, sollte die Bundesregierung:

Politische Abwägungen im Zusammenhang mit digitalpolitischen Entscheidungen adressieren. Bei den schwierigsten Aspekten der Digital-Regulierung stehen wichtige deutsche Prioritäten wie Datenschutz und Sicherheit oft im Widerspruch zueinander. Dies zwingt politische Entscheidungsträgerinnen und -träger dazu, Ziele gegeneinander abzuwägen. Debatten über Themen wie Datenschutz, Strafverfolgung und nationale Sicherheit sollten den Gesamtkontext berücksichtigen, eine transparente Aufsicht ermöglichen und auf dem Grundsatz aufbauen, dass Aktivitäten, die offline illegal sind, dies auch online sind.

Musterklauseln und -module erarbeiten, die in Regularien von Partnerländern integriert werden können. Es könnte ein Verzeichnis von Open-Source-Regeln geschaffen werden, das den Prozess für außereuropäische Partner beschleunigt, wenn es darum geht, Angemessenheit mit der EU in Bezug auf den Austausch personenbezogener und industrieller Daten, die IoT-Sicherheit und die Moderation von Inhalten zu erreichen und die oben erwähnten Herausforderungen mit der DSGVO zu bewältigen. Musterklauseln und -module sollten so gestaltet werden, dass ihrem Missbrauch durch autoritäre Regierungen zur Rechtfertigung von Massenüberwachung, Zensur und Datendiebstahl entgegengewirkt wird. Die Bundesregierung sollte auch die Fähigkeit anderer europäischer Staaten unterstützen, ihre eigenen Vorschriften zu erlassen; die EU wiederum könnte Partnerländern helfen, deren Auswirkungen zu evaluieren.

Geopolitische Folgenabschätzungen für Entwürfe deutscher und europäischer Digital-Regulierung durchführen. Wie wir dargelegt haben, könnten Maßnahmen von Deutschland und der EU unbeabsichtigt digitalem Autoritarismus Vorschub leisten oder unerwünschte globale Trends wie Datenlokalisierung, Zensur, Schwächung von Cybersicherheit oder Internetfragmentierung begünstigen. Autoritäre Staaten wie China und Russland haben bereits gezeigt, dass sie bereit sind, solche unbeabsichtigten Folgen auszunutzen, indem sie Regeln spiegeln und kombinieren, um Massenüberwachung, Zensur und digitale Kontrolle über ihre Bürgerinnen und Bürger zu rechtfertigen. Eine aufmerksame Bewertung der Auswirkungen der deutschen und der EU-Technologiepolitik außerhalb Europas könnte solchem Missbrauch entgegenwirken.

Dem zunehmenden Staatszentrismus bei der europäischen technischen Standardsetzung entgegentreten. Der internationale Einfluss europäischer Organisationen wie des Europäischen Komitees für Normung (CEN), des Europäischen Komitees für elektrotechnische Normung (CENELEC) und des Europäischen Instituts für Telekommunikationsnormen (ETSI) beruht weitgehend auf ihrer Offenheit für private Akteure, einschließlich außereuropäischer Unternehmen. Es geht nicht darum, technische Standardsetzung einfach dem Privatsektor zu überlassen. Die Bundesregierung sollte jedoch ein großes Interesse daran haben, die Führungsrolle des Privatsektors mit den staatlichen und europäischen Interessen in Einklang zu bringen. Sie muss die Bemühungen anführen, den pluralistischen Charakter der europäischen Normung zu erhalten. Wenn sich das Gleichgewicht zu sehr zugunsten des Staates verschiebt, besteht die Gefahr, dass die Leistungsfähigkeit Deutschlands und Europas in diesem Bereich beeinträchtigt wird. Außerdem könnte dies einen ungewollten Präzedenzfall für autoritäre Regime schaffen.

Die Kapazitäten des privaten Sektors in der technischen Standardsetzung stärken. Die Bundesregierung sollte steuerliche Anreize und einen Mechanismus für staatliche Förderung deutscher Unternehmen, Start-ups und Verbände schaffen, damit sie in Normungsgremien mitwirken, Vorsitze übernehmen, neue einschlägige Normen entwickeln und mit gleichgesinnten Staaten zusammenarbeiten. Finanzielle Unterstützung könnte durch Zuschüsse des Bundesministeriums für Wirtschaft und Klimaschutz (BMWK) und des Bundesministeriums für Digitales und Verkehr (BMDV) erfolgen.

Die europäische Cloud-Zertifizierung und die Gaia-X-Architektur in die globalen Cloud-Governance-Bemühungen einbetten. Da Industriedaten zu einer neuen Front in der globalen Technologieregulierung werden könnten, sollte die Bundesregierung nach Wegen suchen, das Datenraummodell Gaia-X zu internationalisieren, um außereuropäische Partner, insbesondere die Vereinigten Staaten, einzubeziehen. Der EU-USA Trade and Technology Council (TTC) könnte demokratische Datenräume für Industriedaten auf der Grundlage der Gaia-X-Architektur in nationalen Hubs in gleichgesinnten außereuropäischen Ländern entwickeln. Die deutsche G7-Präsident-

schaft, die sich in ihrer Endphase befindet, wäre eine Möglichkeit, die gemeinsame Arbeit für freie Datenflüsse auf Grundlage einer vertrauenswürdigen europäischen Regulierung und Architektur für die Speicherung, Verarbeitung und Übertragung von Daten in Gang zu setzen. Japan könnte diese Arbeit während seiner G7-Präsidentschaft 2023 fortsetzen. Schließlich könnte Deutschland den Aufbau von Kapazitäten in den Global Gateway-Partnerländern zur Nutzung europäischer Cloud Computing-Architekturen unterstützen, um die Interoperabilität zu erhöhen und die Menschenrechte zu wahren. Dieses Vorhaben stünde im Einklang mit dem Versprechen der Regierung, die digitale Souveränität im globalen Süden zu stärken.

Digital-Regulierung und technische Standardsetzung in die Zeitenwende und die Nationale Sicherheitsstrategie integrieren. Die Bundesregierung muss sich intensiver mit den Auswirkungen der Regulierung digitaler Technologien auf Deutschlands nationale Sicherheit und Verteidigungsindustrie befassen. Sie muss sicherstellen, dass Deutschland in der Lage ist, Technologien mit doppeltem Verwendungszweck in vergleichbarer Weise zu übernehmen und einzusetzen wie andere Länder, etwa Frankreich, Kanada, Japan und das Vereinigte Königreich. Dies erfordert mehr Flexibilität bei der Berücksichtigung der nationalen Sicherheitsinteressen. Die Bestimmungen des Gesetzes über künstliche Intelligenz könnten beispielsweise Anwendungen von Deep Learning verbieten, die von den Streitkräften anderer Staaten genutzt werden. Die vom deutschen Wettbewerbsrecht und der DMA vorgeschriebene Entflechtung digitaler Dienste wird auch unbeabsichtigte Folgen für die Fähigkeit von Unternehmen haben, ihre Cybersicherheit zu stärken. Die politischen Verantwortlichen in Deutschland müssen ihre Regulierungsmaßnahmen im Bereich der Technologie besser mit nationalen, EU- und NATO-Sicherheitsinteressen in Einklang bringen. Sie haben dies erfolgreich getan, als sie im IT-Sicherheitsgesetz 2.0 aus dem Jahr 2021 Kriterien für vertrauenswürdige Telekommunikationsausrüstung aufstellten.

Das Engagement der deutschen außen- und sicherheitspolitischen Gemeinschaft bei der Gestaltung und Durchsetzung von Regulierungsvereinbarungen erhöhen. Die deutschen Nachrichtendienste, die Außenpolitik, die Strafverfolgungs- und die Verteidigungsbehörden haben alle Anteil an der Durchsetzung nationaler Technologievorschriften. Während die USA eine stärkere Einbeziehung von Datenschützern in die Rahmengespräche fördern sollten, sollte die deutsche Regierung erkennen, dass es für diese Behörden an der Zeit ist, mehr Gewicht zu bekommen. Die post-Privacy Shield Transatlantic Data Privacy Framework-Ära (TDPF) wird eine erste Chance dafür bieten. Das deutsche Außenministerium und die nationalen Sicherheitsbehörden haben ein unmittelbares Interesse an der Aufrechterhaltung einer offenen Datenbrücke zwischen der EU und den USA, die gleichzeitig privaten Akteuren den Zugang zu US-Gerichten sowie einklagbare Rechte und Beschränkungen für die wahllose Erhebung personenbezogener Daten zusichert. Sie müssen eine Führungsrolle übernehmen, um sicherzustellen, dass das TDPF eine dauerhafte Lösung ist, angesichts der Gelegenheit, die es bietet, klare Regelungen für einen freien euro-atlantischen Datenverkehr zu schaffen.

Multistakeholder-Ansatz unter Einbeziehung von Zivilgesellschaft, Unternehmen und anderen nichtstaatlichen Akteuren ermöglichen. Deutschland und Europa haben begonnen, neue Modelle für die Regulierung von Technologien zu entwickeln. Die bisherige Regulierung war hochgradig reglementiert und entsprach damit den Entwicklungspfaden industrieller Technologien, die in Fabrikhallen zum Einsatz kamen. Die Regulierung der digitalen Sphäre muss jedoch agil, auf dem Ökosystem basierend und auf die Schaffung von Anreizen ausgerichtet sein. In Anlehnung an das DSA/DMA-Modell muss sie ein Geflecht von Beziehungen, Zuständigkeiten und Aufsichtsfunktionen umfassen, das schneller Alarm schlagen kann, wenn regulatorische Schwachstellen erkennbar werden. Diese flexiblen Strukturen ermöglichen eine ständige und gleichzeitig kompromissfähige Aufsicht.

Evaluierungen und Auslaufklauseln in der digitalen Regulierung ausweiten, um Flexibilität zu fördern. Angesichts der Geschwindigkeit des Wandels digitaler Technologien ist regulatorische und rechtliche Flexibilität zentral. Evaluierungen und Auslaufklauseln würden die Regulierungsbehörden dazu zwingen, die Wirksamkeit und Relevanz von Vorschriften zu prüfen. Solche Klauseln würden auch die Kohärenz mit der Regulierung in anderen Demokratien fördern. Das bereits erwähnte Beispiel der Datenschutz-Grundverordnung zeigt die Notwendigkeit solcher Bemühungen, die mit dem Gebot der Gewährleistung von Rechtssicherheit und der Bedeutung von Reformen für eine zukunftssichere Regulierung in Einklang stehen.

DEUTSCHE UND EU-REGULIERUNG DIGITALER TECHNOLOGIEN (2015-HEUTE)

Deutsche Initiative	Zielsetzungen	EU-Initiative	Zielsetzungen
2015 **IT-Sicherheits-gesetz**	• führende Standards für IT-Systemsicherheit setzen • digitale Infrastrukturen schützen, insbesondere in kritischen Technologie-Bereichen (kritische Infrastrukturen/KRITIS) • eine neue Warnpflicht in der Telekommunikationsbranche einführen	2016 **NIS-Richtlinie (NIS Directive)**	• eine nationale Aufsicht über kritische Infrastruktursektoren und kritische Anbieter digitaler Dienste mandatieren • Anforderungen an die Cybersicherheitsfähigkeiten der Mitgliedstaaten festlegen, einschließlich Cybersicherheitsstrategien und Computer Security Incident Response Teams (CSIRTS) • grenzübergreifende Zusammenarbeit fördern
2017 **Netzwerkdurchsetzungsgesetz (NetzDG)**	• Rahmenwerke für die Moderation von strafbaren Inhalten wie Hassreden und Fake News definieren • Meldepflichten und Sanktionen für Online-Plattformen festlegen	2020 **Gesetz über digitale Dienste (Digital Services Act, DSA) – Entwurf**	• die EU-weiten Rechtsvorschriften in Bezug auf digitale Plattformen reformieren • Standards für die Moderation von Inhalten, Werbung und Algorithmen setzen • Verpflichtungen, einschließlich Melde- und Aktionsverfahren, bei rechtswidrigen Inhalten definieren
2017 **Datenethikkommission**	• ethische Richtlinien zur Datenpolitik entwickeln • einen Rahmen für den Umgang mit Algorithmen, KI und digitaler Innovation bereitstellen • Fragen zur Datenethik klären • einen Ansatz zur Überwindung sozialer Konflikte in der Datenpolitik definieren	2021 **Gesetz über künstliche Intelligenz (AI Act) – Entwurf** (basierend auf dem KI Whitepaper der Europäischen Kommission von 2020)	• einen „menschenzentrierten" Rechtsrahmen für vertrauenswürdige KI entwerfen • Auseinandersetzung mit den Risiken, die mit bestimmten Anwendungen von KI verbunden sind • das Vertrauen der Nutzerinnen und Nutzer in KI-basierte Lösungen stärken und Unternehmen bei deren Entwicklung fördern
2018 **Nationale Forschungsdaten-infrastruktur (NFDI)**	• Datenbestände im In- und Ausland vernetzen • Wissenschafts- und Forschungsdaten systematisch entwickeln, nachhaltig speichern und zugänglich machen	2018 **European Open Science Cloud (EOSC)**	• ein offenes, multidisziplinäres Umfeld für europäische Forscherinnen und Forscher, Innovatorinnen und Innovatoren, Unternehmen sowie Bürgerinnen und Bürger schaffen • eine erstklassige Dateninfrastruktur, Hochgeschwindigkeitsverbindungen und leistungsstarke Computer für die europäische Wissenschaft, Industrie und öffentliche Einrichtungen bereitstellen
2019 **Gaia-X-Initiative**	• einen gemeinsamen Rahmen für Software-Governance entwickeln, mit dem Ziel, die digitale Souveränität Europas zu gewährleisten • ein gemeinsames Regelwerk implementieren, das auf bestehende Technologie-Stacks angewendet werden kann • Transparenz, Kontrollierbarkeit, Übertragbarkeit und Interoperabilität von Daten und Diensten erreichen	2021 **Allianz für Industriedaten, Edge und Cloud**	• die Position der EU-Industrie im Bereich der Cloud- und Edge-Technologien stärken • die Anforderungen von EU-Unternehmen und öffentlichen Verwaltungen erfüllen, die sensible Daten verarbeiten • die Entwicklung und Bereitstellung von Cloud- und Edge-Kapazitäten der nächsten Generation für den öffentlichen und privaten Sektor fördern • Important Project of Common European Interest for Next Generation Cloud Infrastructure and Services (IPCEI-CIS) trägt zur Überprüfung der EU-Industriestrategie bei
2019 **Blockchain-Strategie der Bundesregierung**	• die Möglichkeiten, die die Blockchain bietet, nutzen und ihr Potenzial für die digitale Transformation mobilisieren • fünf Handlungsfelder: Blockchain im Finanzsektor; Finanzierung von Projekten und Reallaboren; klare und sichere Rahmenbedingungen; digitale Verwaltungsdienstleistungen; Wissen, Vernetzung und Zusammenarbeit		
2021 **Datenstrategie der Bundesregierung**	• die innovative und verantwortungsvolle Nutzung von Daten fördern • Datenkompetenz und eine Datenkultur entwickeln • die Dateninfrastruktur effektiv und nachhaltig gestalten • eine tragfähige staatliche Dateninfrastruktur aufbauen und die Datenkompetenz der Beamtinnen und Beamten stärken	2022 **Datengesetz**	• Fairness durch Regeln für die Nutzung der von IoT-Geräten erzeugten Daten sicherstellen • einen Rahmen zur Förderung des Datenaustauschs zwischen Unternehmen und staatlichen Stellen entwickeln • Business-to-Business-Datenübermittlung unterstützen • den Rahmen für die integrierte Planung und Berichterstattung (IPR) im Hinblick auf eine weitere Verbesserung des Datenzugangs und der Datennutzung evaluieren
		2020 **Daten-Governance-Gesetz – Entwurf**	• das Vertrauen in Datenübermittlung stärken • die Mechanismen für den Datenaustausch zwischen den einzelnen Sektoren und der EU stärken, die Datenverfügbarkeit verbessern und technische Hindernisse für die Wiederverwendung von Daten überwinden
		2021 **EU Cloud Code of Conduct**	• zu einem Umfeld des Vertrauens und der Transparenz auf dem europäischen Cloud-Computing-Markt beitragen • den Prozess zur Risikobewertung von Cloud-Service-Anbietern (CSPs) für Cloud-Kunden vereinfachen
2021 **IT-Sicherheitsgesetz 2.0**	• Sicherheitslücken zum Schutz kritischer Infrastrukturen (KRITIS) schließen • die Kompetenzen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ausweiten, um eine stärkere Zusammenarbeit mit den Strafverfolgungsbehörden zu ermöglichen	2021 **Reform der NIS-Richtlinie**	• das NIS-Mandat ausweiten, um Fragmentierungs- und Umsetzungsprobleme zu adressieren • den Informationsaustausch, die Meldepflicht und die Sanktionsregelungen innerhalb der EU koordinieren • strengere Anforderungen für kritische Infrastrukturen, z. B. für die Sicherheit von Lieferketten, einführen

Quelle: Eigene Darstellung

Deutsche Initiative	Zielsetzungen	EU-Initiative	Zielsetzungen
2021 **Telekommunikation-Telemedien-Datenschutzgesetz (TTDSG)**	• die bisher im Telekommunikationsgesetz (TKG) und im Telemediengesetz enthaltenen Vorschriften zum Schutz des Fernmeldegeheimnisses und von Daten in einem neuen Stammgesetz zusammenführen • bestehende Bestimmungen an die europäische Datenschutzgrundverordnung und an neue Definitionen im Telekommunikationsgesetz anpassen	2017 **E-Privacy-Richtlinie – Entwurf**	• Datenschutzregeln für neue Akteure wie WhatsApp, Facebook Messenger und Skype durchsetzen • den EU-Datenschutz standardisieren • Kommunikationsinhalte und Metadaten schützen • die Cookie-Zustimmungsregelung vereinfachen • Benutzerinnen und Benutzer effektiver vor Spam schützen
		2020 **Daten-Governance-Gesetz – Entwurf**	• den sicheren Austausch sensibler Daten, die sich im Besitz • öffentlicher Einrichtungen befinden, ermöglichen, und den Datenaustausch durch öffentliche Akteure regeln • das Vertrauen zu Datenmittlern steigern • die Mechanismen für den EU-weiten Datenaustausch stärken
2021 **10. Novelle des Gesetzes gegen Wettbewerbsbeschränkungen (GWB)**	• das Bundeskartellamt (BKartA) dazu befähigen, präventive Maßnahmen zur Eindämmung der Marktmacht großer digitaler Plattformen zu ergreifen • Änderungen in Bezug auf kartellrechtliche Ermittlungsverfahren, Kronzeugenregelung und Kartellschadensersatzansprüche einführen	2020 **Gesetz über digitale Märkte (Digital Market Act, DMA**	• unlautere Geschäftspraktiken digitaler Gatekeeper eindämmen • ein faires Geschäftsumfeld für Unternehmen schaffen, die von Gatekeepern abhängig sind • freiere Innovation durch Technologie-Start-ups ermöglichen • unfaire Bedingungen beseitigen, die die technologische Entwicklung einschränken • die Auswahl an Dienstleistungsunternehmen für Kunden ausweiten
2021 **Novelle des Telekommunikationsgesetzes (TKG)**	• einen maßgeschneiderten und zukunftsweisenden Rechtsrahmen für den deutschen Telekommunikationsmarkt schaffen • die Rechte von Endnutzerinnen und -nutzern stärken • den Ausbau von Glasfaser- und Mobilfunknetzen beschleunigen	2018 **Richtlinie (EU) 2018/1972:** über den europäischen Kodex für die elektronische Kommunikation	• den Rahmen für die Regulierung elektronischer Kommunikationsnetze und -dienste konsolidieren und reformieren
2020 **Gesetzentwurf zur Umsetzung von Richtlinie (EU) 2018/1972**	• Netze mit sehr hoher Kapazität und ihre Nutzung ausbauen • nachhaltigen und wirksamen Wettbewerb und die Interoperabilität von Telekommunikationsdiensten gewährleisten • Zugänglichkeit und Sicherheit von Netzen und Diensten sicherstellen • die Interessen der Endnutzerinnen und -nutzer stärken		
2021 **17. Novelle der Außenwirtschaftsverordnung (AWG)**	• Im Rahmen der AWG kritische Infrastrukturen und Schlüsseltechnologien umfassend vor ausländischen Investitionen schützen • anzeigepflichtigen Erwerb auf neue Branchen im sektorübergreifenden Screening ausweiten • die relevanten Schwellenwerte für Meldepflichten senken • das sektorspezifische Screening ausweiten • die Fristen für sektorübergreifende und -spezifische Prüfungen standardisieren	2019 **Verordnung zur Schaffung eines Rahmens für die Überprüfung ausländischer Direktinvestitionen in der Union**	• die strategischen Interessen Europas wahren bei gleichzeitiger Offenhaltung des EU-Marktes für Investitionen • europäische Bedenken hinsichtlich der Auswirkungen ausländischer Übernahmen berücksichtigen • die Meldung bestehender nationaler Mechanismen zur Investitionsüberwachung an die Europäische Kommission (EK) regulieren • formelle Kontaktstellen und sichere Kanäle in jedem Mitgliedstaat und innerhalb der EK für den Informationsaustausch einrichten • Verfahren entwickeln, die es den Mitgliedstaaten und der EK ermöglichen, rasch auf Bedenken hinsichtlich ausländischer Direktinvestitionen zu reagieren
		2021 **Richtlinie (EU) 2021/821** über eine Unionsregelung für die Kontrolle der Ausfuhr, der Vermittlung, der technischen Unterstützung der Durchfuhr und der Verbringung betreffender Güter mit doppeltem Verwendungszweck	• den bisherigen Rechtsrahmen zur Modernisierung der EU-Ausfuhrkontrollregelung für Güter mit doppeltem Verwendungszweck aktualisieren • eine Regelung für die Kontrolle der Ausfuhr, der Vermittlung, der technischen Unterstützung der Durchfuhr und der Verbringung betreffend Güter mit doppeltem Verwendungszweck schaffen • Güter mit doppeltem Verwendungszweck wirksam kontrollieren, wenn sie aus der EU ausgeführt oder durch die EU durchgeführt werden • neue Catch-All-Kontrollen implementieren • nationale Kontrolllisten erstellen und neue Kontrollen für technische Unterstützung einführen – auch für die militärische Endverwendung • mehr Informationsaustausch und Transparenz gewährleisten
2017 **Open-Data-Gesetz**	• Bundesbehörden verpflichten, unbearbeitete Daten, die bei der Erfüllung öffentlich-rechtlicher Aufgaben oder durch Dritte gewonnen wurden, in öffentlich zugänglichen Netzen zu veröffentlichen • eine gesetzliche Grundlage für die Beschaffung von Daten aller öffentlichen Behörden schaffen, die der Aufsicht der Bundesregierung unterliegen	2019 **Open-Data-Richtlinie**	• die Datenwirtschaft in der EU durch Erhöhung des Umfangs der in öffentlichem Besitz befindlichen und öffentlich finanzierten Daten stärken, die zur Weiterverwendung zur Verfügung stehen • öffentliche Stellen verpflichten, Daten nach Möglichkeit zur Wiederverwendung zur Verfügung zu stellen • Echtzeit-Zugang zu dynamischen Daten mit geeigneten technischen Mitteln bereitstellen • das Angebot an wertvollen öffentlichen Daten zur Weiterverwendung erhöhen, auch von öffentlichen Unternehmen • das Entstehen neuer Formen von Ausschließlichkeitsbindungen bekämpfen

DGAP

Advancing foreign policy. Since 1955.

Rauchstraße 17/18
10787 Berlin
Tel. +49 30 254231-0
info@dgap.org
www.dgap.org
@dgapev

Die Deutsche Gesellschaft für Auswärtige Politik e.V. (DGAP) forscht und berät zu aktuellen Themen der deutschen und europäischen Außenpolitik. Dieser Text spiegelt die Meinung der Autorinnen und Autoren wider, nicht die der DGAP.

Die DGAP ist gefördert vom Auswärtigen Amt aufgrund eines Beschlusses des Deutschen Bundestages.

Herausgeber
Deutsche Gesellschaft für
Auswärtige Politik e.V.

ISSN 2198-5936

Übersetzung executive english

Redaktion Jana Idris

Layout Lara Bührer

Design Konzept WeDo

Fotos Autorinnen und Autoren © DGAP