

Der geopolitische Kampf um digitale Souveränität: Zur Digital-Governance der EU in der Rivalität zwischen den USA und China und der Wirkung des „Brüssel-Effekts“ im Globalen Süden

Ingrid Schneider

Zusammenfassung

Dieser Beitrag analysiert die europäische Digitalpolitik im Kontext geopolitischer Spannungen, wobei der Fokus auf der Position Europas zwischen den konkurrierenden US-amerikanischen und chinesischen Modellen digitaler Governance liegt. Während die USA einen Laissez-faire-Ansatz verfolgen und China auf staatliche Kontrolle und Überwachung setzt, strebt die Europäische Union einen eigenständigen „Dritten Weg“ mit einem umfassenden regulatorischen Rahmen an, der Menschenrechte, Demokratie und Nachhaltigkeit betont. Durch die Umsetzung der Datenschutz-Grundverordnung (DSGVO) und weiterer Gesetzgebungen will die EU zugleich globale Standards setzen und ihren Einfluss mittels des „Brüssel-Effekts“ ausweiten. Die empirische Studie basiert auf einer vergleichenden Analyse und Feldforschung in den Schwellenländern Mexiko, Brasilien, Indien und Südafrika, in denen die Wirksamkeit europäischer Digitalregulierung und des Brüssel-Effekts im Datenschutz untersucht werden. Die Ergebnisse zeigen, dass Europas regulatorischer Ansatz in Schwellenländern durchaus ein Leitbild bietet und positive Impulse setzen kann, gleichzeitig aber Herausforderungen bei der Durchsetzung der Gesetze bestehen. Die Arbeit beleuchtet, ob das europäische Modell als Referenz für digitale Souveränität in einer multipolaren Welt fungieren kann und zeigt andere Einflussfaktoren auf.

1. Einleitung

Digitalpolitik wird seit einigen Jahren zunehmend unter geopolitischen Vorzeichen betrachtet. Spätestens die zweite Amtszeit von Präsident Donald Trump in den Vereinigten Staaten hat Europa die große Abhängigkeit von digitalen US-Plattform-Unternehmen vor Augen geführt und den Ruf nach technologischer Souveränität weiter gestärkt. Das digitale Zeitalter hat konkurrierende Leitbilder digitaler Governance hervorgebracht, wobei die USA und China als zentrale Akteure jeweils grundlegend unterschiedliche Prinzipien und Praktiken vertreten. Während diese beiden digitalen Supermächte um technologische Dominanz und wirtschaftliche Einflussphären ringen, positioniert sich die Europäische Union (EU) als Akteur mit einem eigenständigen normativen Ordnungsrahmen. Dieser Beitrag untersucht insbesondere am Beispiel des Datenschutzes den Anspruch der EU, als regulatorische Supermacht aufzutreten und für digitale Governance auf

der Basis von Menschenrechten, demokratischen Werten und ethischen Prinzipien ein globales Referenzmodell zu bilden.

Die Konfrontation zwischen dem US-amerikanischen und dem chinesischen Modell digitaler Governance stellt für die EU die Frage nach ihrem eigenen Weg. Die USA befürworten traditionell einen Laissez-faire-Ansatz, bei dem Innovation und Marktfreiheit im Vordergrund stehen, während China ein staatlich kontrolliertes System mit ausgeprägten Überwachungsmechanismen vertritt. Vor diesem Hintergrund bemüht sich die EU, einen „Dritten Weg“ der digitalen Governance zu etablieren, der sich durch einen robusten Regulierungsrahmen wie die Datenschutz-Grundverordnung (DSGVO), den Digital Markets Act (DMA), den Digital Services Act (DSA), den Data Governance Act (DGA), den Data Act sowie den AI Act auszeichnet. Diese Regulierungsmaßnahmen zielen darauf ab, internationale Konkurrenzfähigkeit und Wirtschaftswachstum im EU-Binnenmarkt zu stärken, technologische Innovation zu gestalten, und gleichzeitig Menschenrechte, Rechtsstaatlichkeit und Demokratie zu gewährleisten sowie Nachhaltigkeit zu fördern. Sie wollen auch den Einfluss der EU über ihre Grenzen hinaus ausweiten und den sogenannten „Brüssel-Effekt“ (siehe unten) zur Geltung bringen, mittels dessen die EU weltweit hohe regulative Standards prägen will.

Dieser Aufsatz verfolgt die Forschungsfrage, welche unterschiedlichen Governance-Modelle sich in den untersuchten Staaten entwickelt haben und ob das Streben Europas nach digitaler Souveränität und die EU-Digitalregulierung in Schwellenländern als Referenzmodell wahrgenommen wird. Zunächst wird untersucht, welche digitalen Governance-Modelle USA und China verfolgen und wie das europäische Modell sich davon unterscheidet, und sodann, welche globale Wirkung dieses entfaltet. Ausgehend von Anu Bradfords These des „Brüssel-Effekts“ (Bradford 2019) wird der Einfluss der EU-Regulierung auf Drittstaaten analysiert. Die entsprechende Fallstudie zum Datenschutz untersucht die Gesetzgebung und Durchsetzung von Datenschutz in vier Schwellenländern und bewertet, ob und wie diese effektiv umgesetzt werden. Der Blick auf Schwellenländer erscheint besonders notwendig, da diese zu den Ländern mit den höchsten Internet-Nutzerzahlen gehören. Zudem spielen diese Länder in einer zunehmend multipolaren Welt eine wichtige Rolle bei der Gestaltung der internationalen Digital-Governance.

Methodisch stützt sich die Studie auf einen vergleichenden Ansatz und basiert auf insgesamt 12 Monaten empirischer Feldforschung, die zwischen 2020 und 2025 in Mexiko, Brasilien, Indien und Südafrika durchgeführt

wurde. Die Feldforschung wurde durch jeweils dreimonatige Entsendungen im Rahmen eines EU-Projekts mit dem Titel "Promoting Research on Digitalisation in Emerging Powers and Europe Towards Sustainable Development" (PRODIGEES) ermöglicht. Die Methodik umfasste in erster Linie leitfadengestützte qualitative Interviews mit 120 verschiedenen Akteuren. Dazu gehörten Experteninterviews mit staatlichen und akademischen Fachleuten, Vertreter:innen von Think Tanks, Branchenexperten und Digitalrechtsorganisationen sowie teilnehmende Beobachtung bei Veranstaltungen und eingehende Literatur- und Dokumentenrecherchen. Das Material wurde codiert und mit Methoden der qualitativen Inhaltsanalyse (Mayring 2022) ausgewertet.

2. Regimes digitaler Governance

Der Begriff der digitalen Governance-Regimes (vgl. Jia/Chen 2022; Staab 2024) umfasst die Gesamtheit der politischen Strategien, rechtlichen Regelungen und gestalterischen Rahmenbedingungen, die das Management und den Betrieb digitaler Technologien sowie des Internets bestimmen. Diese Governance-Regimes prägen eine Vielzahl von Themen, angefangen bei Datenschutz und Cybersicherheit bis hin zu Innovation, Wettbewerb und Marktzugang. Die geopolitische Bedeutung der digitalen Governance wird in den unterschiedlichen Ansätzen deutlich, die von den mächtigen globalen Akteuren wie den USA, China und der EU verfolgt werden. Dabei operieren diese Akteure unter jeweils eigenen regulatorischen Modellen, die von spezifischen Motivationen und Herausforderungen geprägt sind. In jüngerer Zeit werden diese Maßnahmen besonders stark hinsichtlich ihrer geopolitischen Implikationen diskutiert.

Die Vereinigten Staaten und China haben sich zu den wichtigsten Rivalen auf der globalen Bühne entwickelt, die beide nach einer technologischen Führungsrolle streben, welche letztlich die globalen Machtverhältnisse neu definieren wird. In Tabelle 1 sind die wesentlichen Unterschiede zwischen diesen beiden digitalen Governance-Regimes vergleichend dargestellt. Sie werden im Folgenden weiter ausgeführt.

Tabelle 1: Vergleich der Digital-Governance-Modelle zwischen den USA und China

	USA	China
Regulatorischer Ansatz	Minimale Regulierung: Zur Förderung des Wachstums der Technologiebranche verfolgt der Staat einen zurückhaltenden Ansatz mit geringer staatlicher Einmischung.	Staatlich kontrollierte Regulierung: Die Regierung übt eine umfassende Aufsicht aus, um die Ausrichtung auf nationale Prioritäten sicherzustellen.
Innovationsfokus	Starke Betonung des Aufrechterhaltens von Technologie-Führerschaft durch die Priorisierung von Innovation gegenüber Regulierung.	Technologie wird als Instrument des wirtschaftlichen Wachstums eingesetzt; die staatliche Aufsicht gewährleistet jedoch die Einhaltung geplanter politischer Vorgaben.
Marktdynamik	Setzt auf Marktkräfte zur Korrektur von Ungleichgewichten und verzichtet auf starke Regulierung, sofern nicht als unbedingt notwendig erachtet.	Die staatliche Intervention spielt eine zentrale Rolle in der Steuerung des Marktes und stellt sicher, dass Technologieunternehmen mit staatlichen Vorgaben konform gehen.
Wirtschaftliche Entwicklung	Marktorientierter Ansatz zur wirtschaftlichen Entwicklung; disruptive Technologieunternehmen sind führend bei Innovation und Expansion.	Ein durch die Regierung gelenkter Technologiesektor unterstützt nationale Wirtschaftsstrategien und Wachstumspläne.
Soziale Kontrolle	Begrenzte direkte staatliche Kontrolle über digitale Plattformen, allerdings teilweise Bedenken bezüglich Desinformation und Kinderschutz. Neuerdings Propagieren von „freedom of speech“ für rechtspopulistische Sprechakte.	Technologie dient als Mittel zur sozialen und politischen Kontrolle und festigt digitalen Autoritarismus mittels Überwachung sowie staatlicher Zensur und Propaganda.
Daten-Governance	Dezentral organisierte Daten-Governance mit einer zentralen Rolle privater Unternehmen; Regularien wie die DSGVO fehlen weitgehend.	Umfangreiche Erfassung und staatliche Kontrolle der Daten von Bürger:innen zur Gewährleistung von Sicherheit und Stabilität.
Globaler Einfluss	Strebt globale Technologiedominanz primär durch privatwirtschaftliche Akteure wie Google, Apple, Meta, Amazon, Microsoft und Open AI an, staatlich unterstützt. Die Einflussnahme von großen Plattformen auf Handelspolitik und internationales Regierungshandeln ist gewachsen.	China propagiert sein Modell digitaler Steuerung weltweit, unter anderem durch Infrastruktur-Initiativen wie die „Digitale Seidenstraße“, Setzung von Standards in internationalen Organisationen, eigene Internet-Foren und exportiert den Ansatz von Cyber-Souveränität und Datenlokalisierung in Partnerländer. Chinesische Unternehmen wie Tiktok, Huawei, Alibaba, Tencent, Baidu, Temu und Shein expandieren weltweit.

2.1 Das US-Modell digitaler Governance

Der Ansatz der USA zur digitalen Governance hat traditionell Marktfreiheit und Innovation in den Vordergrund gerückt. Der regulatorische Rahmen ist vergleichsweise gering, wodurch Technologieunternehmen erhebliche Freiräume zum Wachstum erhalten. Zu den zentralen Komponenten dieses Ökosystems zählen die staatliche Förderung entscheidender Innovationen (Mazzucato 2013), der Zugang zu hohen Risikokapital-Investitionen, das ingenieurwissenschaftliche Fachwissen und die Wissensressourcen der Universitäten sowie ein ausgeprägter Techno-Optimismus, der mit der Vorstellung einhergeht, dass ein „freies Internet“ Freiheit und Demokratie fördert. All dies begünstigt rasches technologisches Fortschreiten und verschafft Start-ups eine schnelle Umsetzung in marktfähige Produkte und Dienstleistungen.

Die USA prägen die internationale Digitalpolitik in erster Linie durch ihre dominanten GAFAM-Plattformen – Google/Alphabet, Apple, Facebook/Meta, Amazon und Microsoft. Sie haben bisher einem libertären Modell den Vorzug gegeben, das marktwirtschaftliche Prinzipien priorisiert. Trotz wachsender öffentlicher Forderungen nach einer stärkeren Regulierung der Tech-Industrie angesichts von Datenschutzverstößen und schädlichen Online-Inhalten wurden regulatorische Interventionen durch intensives Lobbying der Unternehmen weitgehend ausgebremsst. Es erscheint derzeit höchst unwahrscheinlich, dass ein bundesweites Datenschutzgesetz oder umfassende Reformen von Section 230 des Communications Decency Act von 1996 – der Online-Plattformen Haftungsimmunität für gepostete Inhalte gewährt – verabschiedet wird (Cohen 2019). Die Vereinigten Staaten setzen weiterhin auf die Maximierung ihres technologischen Potenzials, insbesondere um ihre Wettbewerbsfähigkeit gegenüber China zu wahren. Nationale Sicherheitsinteressen ermöglichen es der Regierung allerdings, auf Daten von Internetplattformen zuzugreifen (Bradford 2023).

Unter der Regierung von Präsident Biden zeigten sich jedoch spürbare Verschiebungen hin zu stärkerer staatlicher und gerichtlicher Aufsicht, wie die Durchsetzung von Kartellrecht durch die Federal Trade Commission und das Justizministerium sowie Bidens Executive Order zur Künstlichen Intelligenz demonstrierten (Biden 2023). Ein großer Teil dieser Maßnahmen wurde bereits in den ersten Wochen der zweiten Amtszeit von Präsident Trump per Dekret ausgesetzt und eine Abkehr von einer Regulierung der Tech-Konzerne vollzogen. Wie sich bereits bei Trumps Inaugurationsfeier zeigte, betonen die Eigentümer bzw. Geschäftsführer

der größten digitalen Plattform-Unternehmen eine große Nähe zur US-Regierung. Beispielsweise haben Meta und X Anfang Januar 2025 ihre Kooperation mit Fact-Checkern in den USA aufgekündigt und wollen diese durch sogenannte Community-Notes ersetzen. Inzwischen wird gegenüber Drittstaaten eine Verknüpfung von Digitalregulierung mit der Handelspolitik und Zöllen vollzogen, insofern als etwa der EU angedroht wird, eine scharfe Durchsetzung von DSA und DMA würde als „Erpressung“ bewertet und hohe Bußgelder würden mit Zollerhöhungen „vergolten“ (The White House 2025; Glenn/Muggah 2025; AP 2025). Die EU behält sich bisher vor, „alle Karten auszuspielen“ und die Tech-Unternehmen weiterhin strikt zu regulieren (Reid 2025).

Unter Präsident Biden kam es zu verstärkten staatlichen Subventionen und industriepolitischen Maßnahmen, wie etwa durch den CHIPS Act zur Förderung der inländischen Halbleiterproduktion und Forschung sowie durch den Inflation Reduction Act. Mit solchen Initiativen hat die US-Technologiepolitik einen signifikanten Paradigmenwechsel vom traditionellen Laissez-faire-Herangehen hin zu einer stärkeren Förderung nationaler Wettbewerbsfähigkeit und Sicherheit vollzogen (Bradford 2023a). Unter Trump scheint sich das Zusammenspiel von staatlicher Politik und privatwirtschaftlichem Handeln noch zu verstärken, etwa bei der Ankündigung einer neuen KI-Infrastruktur namens „Stargate“, wofür in den kommenden vier Jahren 500 Milliarden Dollar investiert werden sollen (Open.AI 2025) oder bei der Förderung von Elon Musks Satellitenprojekt Starlink in afrikanischen Ländern (Rudl 2025), was die zukünftige weltweite Gestaltung technologischer Entwicklungen prägen wird. Von libertären technologiepolitischen Vordenkern wie Peter Thiel und anderen werden Freiheit und Demokratie sogar zunehmend als Gegensatz konzipiert. Imaginiert werden dahingehend eine weitgehende Reduktion des Staates und sogar ein Verzicht auf demokratische Wahlen zugunsten einer Art von technologiegeführten Fürstentümern (vgl. Golumbia 2024).

2.2 Das chinesische Modell digitaler Governance

Im Gegensatz zu den USA ist das chinesische Modell der digitalen Governance staatlich und top-down geprägt, Technologie wird genutzt für wirtschaftliches Wachstum, soziale Kontrolle, Stabilität und Wahrung der Autorität der Kommunistischen Partei Chinas (KPCh). Die Regierung fördert die Wirtschaft durch Subventionen, Steuervergünstigungen und

Schutz vor ausländischer Konkurrenz. Ziel ist technologische Autarkie, etwa bei KI und Hochtechnologie, unterstützt durch Programme wie „Made in China 2025“ (Holzmann/ Zenglein 2019). Das Internet ist durch die Große Firewall abgeschirmt, was dominante nationale Plattformen wie Baidu, Alibaba und Tencent begünstigt. Die Regierung schafft durch Gesetze wie Cybersecurity und Data Security Law ein strenges Regelwerk, das Kontrolle, Überwachung und Zensur ermöglicht. Diese Maßnahmen dienen dem Schutz der Industrie, der Stabilität und der Wahrung der Autorität der KPCh. Unter dem Motto „Gemeinsamer Wohlstand“ verfolgt China eine inklusive Wachstumsstrategie, wobei der Nutzen für Bürger:innen mit strenger Internetkontrolle und Sanktionen bei Dissens einhergeht (Lilkov 2020).

Während technologische Entwicklungen mit ökonomischer Stoßrichtung staatlich gefördert werden, unterbindet der Staat gleichzeitig gezielt das Entstehen privatwirtschaftlicher Akteure, die seine Autorität gefährden könnten. Einige Eingriffe in jüngerer Zeit – wie das Vorgehen gegen Jack Ma’s Ant Group (2020), die Milliardenstrafe gegen Alibaba (2021) und das Verhindern einer von Tencent unterstützten Fusion – spiegeln eine Neubewertung des staatlichen Umgangs mit dem Privatsektor wider (Bradford 2023a, S. 94ff.).

Das chinesische Modell baut flächendeckend digitale Technologien wie Gesichtserkennung, Big Data und KI zur Überwachung und sozialen Steuerung aus, um Loyalität und gesellschaftlichen Konformismus zu fördern (Lilkov 2020). Chinas Konzept der „Cyber-Souveränität“ umfasst territoriale Datenlokalisierung, bei der alle Daten in China gespeichert und staatlicher Zugriff gesetzlich möglich sind. China propagiert dieses Modell international, insbesondere im Globalen Süden, um geopolitischen Einfluss zu gewinnen (Fischer 2022). Insgesamt steht das chinesische Modell für eine autoritäre Ausrichtung. Der chinesische Technologiesektor profitiert aber auch von marktgetriebener Innovation und Wagniskapital. Dies verdeutlicht, dass politische Freiheit kein notwendiges Erfordernis für technologischen Fortschritt und damit einhergehender wirtschaftlicher Prosperität ist – was verbreitete westliche Annahmen zunehmend herausfordert.

Extern stärkt China seinen Einfluss durch den Export digitaler Infrastruktur im Rahmen der „Digitalen Seidenstraße“, etwa 5G-Technologien durch Huawei, Netzwerklösungen von ZTE sowie Smart-City-Projekte. Dieser Infrastruktur-Export gilt als kostengünstiger Weg zur Entwicklung, birgt aber hohe Schulden- und Abhängigkeitsrisiken, oft durch Kredite,

die mit Rohstoffen gesichert sind. China stärkt zudem seinen Einfluss in internationalen Standardorganisationen der digitalen Governance, wie der International Telecommunication Union (ITU) und der International Organization for Standardization (ISO) sowie bei Online-Zahlungssystemen zur Förderung des Yuan. Das zeigt sich in digitalpolitischen Gremien wie der UN-Open Ended Working Group, dem seit 2014 abgehaltenen Wuzhen Summit und der 2020 gestarteten „Global Data Security Initiative“ (Erie/Streinzi 2021; Recorded Future 2021). Zudem verzeichnet China eine wachsende Präsenz von Plattformen wie TikTok, Alibaba, Tencent, Temu und Shein auf globalen Märkten.

Zusammenfassend verbindet Chinas Ansatz zur digitalen Governance Elemente von digitalem Autoritarismus mit selektiver Adaption regulatorischer Praktiken, die durchaus an die EU angelehnt sind. Ziel ist technologische Überlegenheit, wirtschaftliche Entwicklung und politische Kontrolle. Es gibt Datenschutz- und Wettbewerbsregeln, die große chinesische Tech-Unternehmen einschränken, ähnlich wie in der EU (Bradford 2023a). Gleichzeitig nutzt China Technologie systematisch für Zensur und Überwachung, um Stabilität zu sichern. Ob dieses Modell langfristig nachhaltig ist, ist unklar, da wirtschaftliche Risiken wie Immobilienblasen und Jugendarbeitslosigkeit bestehen, und fraglich ist, ob die Bevölkerung mittels bequemer digitaler Dienste und Wachstum dauerhaft loyal bleibt.

2.3 Die sich zuspitzende Rivalität zwischen den USA und China

Das globale Feld digitaler Governance ist zunehmend geprägt von Spannungen, die Innovationspfade, Regulierungen und internationale Beziehungen beeinflussen. Die digitale Rivalität zwischen den USA und China hat insbesondere durch KI, Konkurrenz um strategische Rohstoffe wie seltene Erden, Hochleistungs-Chips und Datenzentren sowie handelspolitische Spannungen in den letzten Jahren stark zugenommen. Beide Staaten liegen bei der Wertschöpfung aus der Datenwirtschaft an der Weltspitze: Sie beherbergen den Großteil der globalen Hyperscale-Rechenzentren, verfügen über die schnellsten Internetverbindungen, generieren über 94 % der Investitionen in KI-Start-ups und vereinen etwa 90 % der Börsenkapitalisierung der zehn größten Digitalunternehmen auf sich (UNCTAD 2021). Zugleich entstehen dadurch neue Disparitäten und Innovationsgefälle, da physische Faktoren wie Wasser und Energieversorgung, lokales Fachpersonal und der Zugang zu spezialisierten Chips zu entscheidenden Voraussetzungen

der KI-Ökonomie werden (UNCTAD 2024). Drei Unternehmen - Amazon Web Services, Microsoft Azure und Google Cloud - bieten mehr als 65 Prozent der weltweiten Cloud-Dienste an, ein Markt, der 2024 auf über 750 Milliarden US-Dollar geschätzt wurde. 90 Prozent der europäischen Cloud-Infrastruktur wird von US-Unternehmen kontrolliert. Die USA dominieren auch die Dateninfrastruktur; ihre mehr als 5.400 Rechenzentren übertreffen die von Deutschland (529) und Großbritannien (523) ums Zehnfache. Schätzungsweise 70 Prozent des weltweiten Internetverkehrs fließen über Server in den USA (Glenny/ Muggah 2025).

In diesem sich verändernden globalen Kontext stellt sich die Frage, ob Europa und der Globale Süden zwischen diese geopolitischen Fronten geraten sind und sich für eines der beiden konkurrierenden Modelle im internationalen digitalen Wettbewerb entscheiden müssen – oder ob sie, wie etwa von der EU proklamiert, einen eigenen Ansatz zur Digital-Governance und digitalen Souveränität als „Dritten Weg“ etablieren können.

Angesichts der enormen Marktmacht großer Plattformen ergibt sich zudem die Frage, wer tatsächlich die Regeln setzt und wer sich diesen zu unterwerfen hat: Sind große Digitalplattformen eigentlich „Rule-Taker“ oder „Rule-Maker“? Haben sie mittlerweile gar mehr Einfluss auf digitale Geschäftsmodelle, Wertschöpfungsketten und das individuelle wie kollektive Verhalten als Nationalstaaten? In der Praxis fungieren diese Plattformen selbst als regulatorische Akteure – sie beeinflussen über ihre Geschäftsmodelle, technologischen Designs, Algorithmen und die Steuerung dessen, welche Inhalte in Suchmaschinen und sozialen Netzwerken prominent sichtbar sind, maßgeblich das digitale Nutzungsverhalten. In den USA wird dieser Sachverhalt beispielsweise mithilfe der Begriffe „Private Ordering“ oder „Code is Law“ (Lessig) diskutiert (vgl. Cohen 2019), während im Globalen Süden zuweilen von „digitalem Kolonialismus“ gesprochen wird (Belli/Zingales 2017; Dachwitz/Hilbig 2025). Nichtsdestotrotz steht auch die Rückkehr staatlicher Steuerungsansprüche – insbesondere in der Forderung nach technologischer Souveränität und dem Streben nach strategischer Autonomie – zunehmend zur Debatte (CERRE 2024; FES 2024).

3. Das Regulierungsmodell der Europäischen Union für digitale Governance

3.1 Zentrale Regulierungsinitiativen der Europäischen Union

Die EU strebt danach, sich als ambitionierte regulatorische Supermacht zu positionieren und damit einen eigenständigen „Dritten Weg“ zu etablie-

ren, der sie sowohl von den Modellen der Vereinigten Staaten als auch Chinas abgrenzt (Hobbs 2020). Innerhalb der EU mehren sich allerdings Stimmen, die unter dem Motto von „Vereinfachung“, Entbürokratisierung und „Innovationsoffensive“ eine Abkehr von dieser Strategie fordern (European Commission 2024; vgl. Csernaton 2025; von Thun et al. 2025; Schneider 2025). In diesem Spannungsfeld versucht die EU, sich als internationales Referenzmodell für andere Staaten darzustellen. In den vergangenen Legislaturperioden hat die EU eine Reihe umfassender gesetzlicher Regelwerke verabschiedet (zum Überblick siehe Bruegel 2024). Die Datenschutz-Grundverordnung (DSGVO), die 2018 in Kraft trat, hat strenge Maßstäbe für den Datenschutz in der EU gesetzt und sieht bei Verstößen empfindliche Bußgelder vor. Der Digital Markets Act (DMA) zielt darauf ab, fairen Wettbewerb zu gewährleisten, indem er wettbewerbswidrige Praktiken großer Gatekeeper-Plattformen einschränkt. Der Digital Services Act (DSA) fokussiert auf sehr große Online-Plattformen und Suchmaschinen und fördert Transparenz und Sicherheit der Nutzer:innen. Der Data Governance Act (DGA) sowie der Data Act sollen durch mehr Datenzugang die europäische Datenökonomie für kleinere und mittlere Unternehmen erschließen. Die KI-Verordnung schließlich definiert Standards für Künstliche Intelligenz, kategorisiert vier Risikostufen und legt insbesondere für Hochrisikosysteme spezifische Auflagen fest.

Zusammengenommen bilden diese Regulierungen ein robustes Rahmenwerk der digitalen Governance, das die EU als Vorreiterin bei Datenschutz, fairem Marktzugang und nachhaltiger Innovation positioniert (CAIDP 2025; UNCTAD 2021 und 2024). Ziel ist ein *level playing field*, das Wachstum, Wettbewerb und Innovation sowohl im EU-Binnenmarkt als auch global fördert. Gleichzeitig stehen die Mitgliedstaaten vor der Herausforderung, technologische Entwicklung zu unterstützen und zugleich die Grundrechte der Bürger gegenüber staatlichen Sicherheitsinteressen und ausländischer Einflussnahme zu schützen.

Mit ihrer Strategie „Weg in die Digitale Dekade“ hat die Europäische Union ehrgeizige Ziele für die digitale Transformation bis 2030 definiert (European Council 2022a und 2024). Der „Digital Compass“ legt die Vision und Zielvorgaben für die Digitalisierung der EU fest (European Commission 2021), während das entsprechende internationale Politikprogramm das Rahmenwerk für ihre Umsetzung bereitstellt (European Council 2022b).

3.2. Der „Brüssel-Effekt“: Konzept und Implikationen

Der Begriff „Brüssel-Effekt“, wie ihn Anu Bradford (2019) geprägt hat, bezieht sich auf die weitreichenden extraterritorialen Wirkungen der regulatorischen Maßnahmen der Europäischen Union. Er umfasst zwei zentrale Prozesse: Erstens neigen globale digitale Plattformen und Unternehmen dazu, die hohen regulatorischen EU-Standards auch außerhalb Europas freiwillig zu übernehmen. Dies liegt daran, dass es für diese Akteure unpraktisch und zu aufwendig wäre, ihre digitalen Architekturen und Systemdesigns jeweils genau den unterschiedlichen nationalen Regularien anzupassen. Zweitens fungieren die EU-Regelungen zunehmend als Referenzmodelle für die Gesetzgebung in anderen Ländern, die ihre eigenen Rechtsrahmen an die EU-Standards angleichen, um Zugang zu wichtigen Märkten zu erhalten oder internationale Kooperationen zu erleichtern.

Der Brüssel-Effekt stellt daher Bradford zufolge eine Form der unilateralen, globalen Regulierung dar, bei der die Rechtsnormen der EU primär durch Marktmechanismen nach außen hin durchgesetzt werden. Dies sei auf mehrere Faktoren zurückzuführen: Die Größe des EU-Binnenmarktes mit seinen 450 Millionen Konsument:innen ermöglicht es, Einfluss auf ausländische Akteure auszuüben; die beträchtlichen regulatorischen Kapazitäten der EU erlauben eine wirksame Durchsetzung; EU-Vorschriften können den Zugang zu sämtlichen Märkten erleichtern; durch ihre Relevanz im globalen Verbrauchermarkt werden einheitliche Produktstandards bei multinationalen Unternehmen gefördert und regulatorische Kosten minimiert. Zusammengenommen führt dies zu dem, was Bradford als „de-facto-Brüssel-Effekt“ bezeichnet, bei dem es primär die Unternehmen selbst sind, die die hohen EU-Standards nicht nur innerhalb der EU, sondern weltweit implementieren (Bradford 2019, S. 83-84.).

Daneben gibt es den „de jure-Brüssel-Effekt“, bei dem Nicht-EU-Länder formell durch Gesetzgebung, Regulierung oder durch internationale Abkommen an EU-Standards angepasste Regeln in ihren eigenen Rechtssystemen verankern (dies., S. 67-68). Dadurch wird die Einflussnahme der EU auf globale Regulierungen institutionalisiert und verstärkt. Insgesamt zeigt der Brüssel-Effekt, wie die EU ihre regulatorische Macht über nationale Grenzen hinweg ausübt und globale Standards maßgeblich beeinflusst.

Insbesondere die Datenschutz-Grundverordnung (DSGVO) hat Wirkungen ausgelöst, die weit über das Territorium der EU hinausreichen. Erstens gilt unter dem Markttortprinzip, das in der DSGVO (Art. 3 Abs. 2) verankert ist, dass Anbieter digitaler Produkte und Dienste in der EU die

Datenschutzregeln der EU einhalten müssen, ungeachtet dessen, wo sie ihren Firmensitz haben. Zweitens sind europäische Datenschutzprinzipien in internationalen Handelsabkommen der EU mit Drittländern verankert, was die Etablierung globaler Standards fördert. Für globale Technologieriesen wäre es ökonomisch unklug, den lukrativen europäischen Markt aufzugeben; die Organisation ihrer Geschäftstätigkeit auf der Grundlage vieler verschiedener rechtlicher Rahmenbedingungen wäre mühsam, und die Mobilität der Daten erfordert faktisch eine transnationale Harmonisierung (Bendiek/Römer 2019). Zudem kann die EU für den Transfer persönlicher Daten in Drittländer einen Angemessenheitsbeschluss fassen, womit diese dem Datenschutz innerhalb der EU gleichgestellt werden und keine weitere Genehmigung bedürfen (laut Art. 45 Abs. 3 DSGVO).

Bradford (2019) argumentiert, dass es für die Unternehmen effizienter sei, strenge europäische Vorschriften weltweit umzusetzen, als Architektur und Design ihrer Dienste zu fragmentieren. Infolgedessen tendierten diese Anbieter digitaler Dienstleistungen dazu, Verbraucher:innen in anderen Rechtsordnungen das gleiche Schutzniveau zu bieten wie den Europäer:innen. Diese Situation führe dazu, dass die EU ihre Datenschutzgesetze effektiv über ihre Grenzen hinaus ausdehne und ausländische Marktteilnehmer veranlasse, sich an die EU-Vorschriften zu halten, unabhängig davon, ob sie Kund:innen in der EU, den USA oder in anderen Ländern beliefern.

3.3 Der EU-Ansatz für rechtsbasierte und menschenzentrierte digitale Governance

Das digitale Governance-Regime der Europäischen Union bietet einen strukturierten Rahmen, um der dominierenden Einflussnahme großer Tech-Unternehmen entgegenzuwirken. Es versteht sich als Korrektiv gegenüber den wahrgenommenen regulatorischen Schwächen in den USA und den Übergriffen des autoritativen Modells Chinas. Der EU-Rahmen zeichnet sich dadurch aus, dass er den Schwerpunkt auf die Förderung des öffentlichen Interesses, die Abwägung der Macht von Unternehmen und die Wahrung demokratischer Werte legt. Wie in Tabelle 3 dargestellt, basiert die digitale Governance der EU auf Prinzipien, die mit Menschenrechten und demokratischen Grundwerten in Einklang stehen. Dies fußt auf einem Gesellschaftsvertrag, der Grundrechte, Demokratie, Solidarität, und Rechenschaftspflichten verankert sowie auf dem Ziel, einen digitalen Binnenmarkt zu schaffen (Bradford 2023b; European Commission 2021).

Tabelle 2: Das digitale Governance-Modell der Europäischen Union

	Europäische Union
Regulatorischer Ansatz	Starkes regulatorisches Rahmenwerk mit Schwerpunkt auf Transparenz, Fairness und Rechenschaftspflicht in der digitalen Wirtschaft.
Innovationsfokus	Will ethische und menschenzentrierte Innovation priorisieren, um sicherzustellen, dass KI und digitale Technologien sicher, nachhaltig und vertrauenswürdig sind.
Marktdynamik	Sucht eine Balance zwischen Regulierung und Wettbewerb, um Monopole zu verhindern und gleichzeitig einen wettbewerbsfähigen Markt zu fördern.
Wirtschaftsentwicklung	Fördert eine digitale Wirtschaft, die mit europäischen Werten im Einklang steht, mit Schwerpunkt auf Nachhaltigkeit und sozialer Verantwortung.
Soziale Kontrolle	Betont digitale Rechte und will sicherstellen, dass Nutzer:innen die Kontrolle über ihre Daten und digitalen Interaktionen behalten.
Daten-Governance	Umfassendes Rahmenwerk für Daten-Governance, einschließlich DSGVO, um Datenschutz, Sicherheit und Nutzerermächtigung zu stärken.
Globaler Einfluss	Exportiert regulatorische Standards weltweit durch den „Brüssel-Effekt“ und beeinflusst so Digitalpolitik über die eigenen Grenzen hinaus.

Die Vorteile des EU-Governance-Modells liegen in der Gemeinwohlorientierung und der Bewahrung demokratischer Strukturen. Doch es gibt Herausforderungen, vor allem bei der Innovationsfähigkeit: Kritiker warnen, dass strenge EU-Vorschriften die Innovation hemmen und verweisen auf die vergleichsweise geringe Zahl führender europäischer Tech-Unternehmen. Der Ende 2024 veröffentlichte Draghi-Bericht moniert viel zu geringe private und öffentliche Investitionen in digitale Technologien (European Commission 2024) und fordert regulative Vereinfachung. Bradford (2023b und 2024) weist jedoch darauf hin, dass Probleme wie ein fragmentierter digitaler Markt und unzureichende Risikokapitalressourcen sowie die Abhängigkeit von ausländischen Datenzentren eine größere Rolle bei der Innovationslücke spielen als die Regulierung selbst.

Für die EU ist es entscheidend, ihre Vorschriften kohärent in allen Mitgliedstaaten zu implementieren. Nur durch eine effektive Durchsetzung kann die EU ihre globale Glaubwürdigkeit sichern und die Wirksamkeit ihrer regulatorischen Maßnahmen unter Beweis stellen. Ein Beispiel für gewisse Vollzugsdefizite bildet die langwierige Durchsetzung der DSGVO. So hat die irische Datenschutzbehörde erst 2022/2023 begonnen, hohe Bußgelder gegen Digitalunternehmen zu verhängen, die ja überwiegend aus Steuergründen ihren europäischen Sitz in Irland haben. Das bislang höchste Bußgeld beträgt 1,2 Milliarden Euro gegenüber Meta Platforms

Ireland wegen unzureichender Rechtsbasis für deren Datenverarbeitung. Zudem verhängte die irische Aufsichtsbehörde eine Strafe in Höhe von 345 Millionen Euro gegen TikTok. Luxemburg sanktionierte Amazon Europe mit 746 Millionen Euro wegen unzureichender Rechtsbasis für die Datenverarbeitung (GDPR Enforcement Tracker 2025). Entscheidend für den Erfolg der europäischen Datenschutzaufsichtsbehörden wird sein, ob sie in der Lage sind, die Einhaltung der Vorschriften nicht nur durch hohe Bußgelder einzufordern, sondern andere, datenschutzkonforme Geschäftsmodelle durchzusetzen.

Der Erfolg neuer Regelwerke wie des Digital Services Act (DSA), des Digital Markets Act (DMA) und des AI-Acts hängt wesentlich davon ab, wie effektiv die EU diese Gesetze um- und durchsetzen kann. Dabei sind eine abgestimmte Policy-Koordination zwischen Europäischer Kommission und den nationalen Mitgliedstaaten sowie sektorübergreifende Strategien notwendig. Zudem muss die EU gegen Vorwürfe von Überregulierung antreten: Insbesondere aus den USA wird die Ansicht vertreten, die strengen Regeln der EU seien protektionistische Maßnahmen gegen US-Unternehmen (The White House 2025). Die EU betont jedoch, dass es um Verhaltensstandards gegen den Missbrauch marktbeherrschender Macht geht, unabhängig von der Nationalität der Unternehmen. Gleichwohl prägen die EU-Verordnungen weiterhin globale Standards und gelten vielfach als Vorbild für regulatorische Reformen, die von Gesetzgebern und zivilgesellschaftlichen Akteuren gleichermaßen begrüßt werden.

4. Die Wirkung des Brüssel-Effekts im Datenschutz

Der Datenschutz ist das prominenteste Beispiel für den Brüssel-Effekt. Die DSGVO hat zahlreiche Länder inspiriert, ihre eigenen Regelungen zu schaffen und gilt aufgrund des hohen Datenschutzniveaus weltweit als Goldstandard (UNCTAD 2021). Bislang haben 167 Staaten entsprechende – teilweise an die DSGVO angelehnte – Gesetze erlassen, über 94 Nationen Datenschutzbehörden eingerichtet, sodass etwa 83 % der Weltbevölkerung in Rechtsordnungen mit umfassendem Datenschutz leben (Banisar 2025). Dies klingt wie eine globale Erfolgsgeschichte der DSGVO. Es bleibt jedoch wichtig, nicht nur die formalen legislativen Errungenschaften zu betrachten, sondern auch die praktische Umsetzung des Datenschutzes in den jeweiligen Ländern zu untersuchen. In allen vier betrachteten Schwellenländern wird die Privatsphäre der Bürger:innen als ein fundamentales,

verfassungsrechtlich geschütztes Recht anerkannt. Die Umsetzung dieses Grundrechts mittels Datenschutzgesetzen und deren Implementierung ist jedoch mit erheblichen Herausforderungen verbunden, wie nun anhand der Datenschutzgesetze und ihrer Durchsetzung in Mexiko, Brasilien, Indien und Südafrika ausgeführt wird.

4.1 Datenschutz in Mexiko

Mexiko verfügt über zwei Datenschutzgesetze: eines für den privaten Sektor und ein zweites für den öffentlichen Sektor. Das 2010 verabschiedete Bundesgesetz zum Schutz persönlicher Daten in der Hand von Personen (*Ley Federal de Protección de Datos Personales en Posesión de Particulares*, kurz LFPDPPP) gilt für den Privatsektor. Für den öffentlichen Sektor wurde 2017 das Allgemeine Gesetz zum Schutz von Daten in der Hand von Verpflichteten (*Ley General de Protección de Datos en Posesión de Sujetos Obligados*) verabschiedet, das sich deutlich an der DSGVO orientiert. Diese Doppelstruktur schafft gewisse Inkonsistenzen, da der öffentliche Sektor nunmehr stärker reglementiert ist als der private. Zudem hat Mexiko 2018 die Konvention 108 des Europarats zum Datenschutz unterzeichnet, was einen bedeutenden Schritt in Richtung einer Harmonisierung des internationalen Datenverkehrs darstellt.

Das Nationale Institut für Transparenz, Zugang zu Informationen und Datenschutz (INAI – *Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales*) beschäftigte bis Ende 2024 etwa 100 Mitarbeitende, die sich dem Vollzug der Datenschutzvorschriften widmeten. Von 2014 bis Ende 2024 hat das INAI als unabhängige Behörde agiert.

Das INAI ist eine sehr aktive Aufsichtsbehörde, die im Jahr 2022 119 Verfahren eingeleitet und 78 davon abgeschlossen hat, was zu Bußgeldern in Höhe von umgerechnet insgesamt 2,8 Millionen Euro vor allem an Medienunternehmen, Finanzdienstleister und Versicherungen führte (Villanueva Plasencia 2023). Sanktionen durch das INAI werden jedoch häufig gerichtlich angefochten, was ihre Durchsetzung erschwert. Kritiker bemängeln, das INAI habe in der Vergangenheit zu wenig proaktiv agiert und Verstöße unzureichend verfolgt.

Herausforderungen in der Durchsetzung des Datenschutzes bestehen in einer schwachen Datenschutzkultur sowie in erheblichen Verstößen, die kaum geahndet werden. Das Freihandelsabkommen USMCA/T-MEC von

2020 enthält zwar eine Datenschutzklausel, verbietet jedoch Datenlokalisierung auf nationaler Ebene, was es Unternehmen erleichtert, ihre Server in die USA zu verlegen und damit die mexikanischen Vorgaben auszuhebeln. Dieses „Forum-Shopping“ von großen Unternehmen um die niedrigsten Datenschutzstandards bildet zum Verdruss des INAI ein hohes Hindernis für das effektive Implementieren der mexikanischen Datenschutzgesetze. Weitere Schwierigkeiten ergeben sich aus mangelnder Sensibilisierung für Datenschutzfragen, geringer Bewusstheit über die rechtlichen Implikationen der Datenverarbeitung sowie mangelnder Kenntnis der Bürger:innen über ihre Rechte (Schneider 2022). Allerdings hat das INAI durchaus erfolgreich niedrigschwellige Aufklärung über Datenschutzrechte geleistet und dabei mit Comics, Spielen und anderen Informationseinheiten innovative Wege eingeschlagen.

Das INAI wurde, initiiert durch Präsident Andrés Manuel López Obrador und vollendet durch seine Nachfolgerin Präsidentin Claudia Sheinbaum, durch eine Verfassungsreform im Dezember 2024 ebenso wie sechs weitere autonome Behörden aufgelöst; begründet wurde dies mit Effizienz und Verwaltungsvereinfachung. Die Aufgaben der INAI wurden auf das neu geschaffene Sekretariat für Korruptionsbekämpfung und gute Regierungsführung übertragen und damit dem Ministerium unterstellt (Huitron 2025). Beobachter sehen darin eine bedeutsame Schwächung des Datenschutzes und fürchten, dass die Regierung den Datenschutz politischen Motiven gefügig macht. Mexiko war zudem im Begriff, von der EU einen Angemessenheitsbeschluss für den personenbezogenen Datentransfer zu erhalten, die es Mexiko ermöglicht hätte, digitale Dienstleistungen mit starken Datenschutzgarantien anzubieten. Dies ist nach dem Verlust der Unabhängigkeit als Behörde nunmehr wohl nicht mehr möglich. Im Zuge der Unsicherheit über die Zukunft des INAI haben eine Reihe langjähriger Mitarbeiter:innen das INAI verlassen, was auch mit dem Verlust von Erfahrungswissen einhergeht.

4.2 Datenschutz in Brasilien

Brasilien zählt zu den Pionieren im Bereich der digitalen Rechte. 2014 wurde der *Marco Civil da Internet* verabschiedet, ein grundlegendes Gesetz, das zentrale digitale Rechte, einschließlich der Netzneutralität, kodifiziert hat (Belli/Doneda 2022). Das 2018 in Kraft getretene Allgemeine Datenschutzgesetz (LGPD – *Lei Geral de Proteção de Dados*) stimmt in recht

hohem Maße mit der DSGVO überein. LGPD war gleichwohl das Produkt ausführlicher, mehrjähriger Debatten im Parlament, in Anwaltskreisen, Unternehmen und der Zivilgesellschaft (Brioni 2020).

Die brasilianische Datenschutzbehörde (ANPD – *Autoridade Nacional de Proteção de Dados*) wurde im November 2020 eingerichtet und erhielt im Oktober 2022 formale Autonomie. In den Anfangsjahren unter der Regierung von Präsident Jair Bolsonaro arbeitete die ANPD in einer schwierigen Konstellation, drei der fünf Direktoren stammen vom Militär. Obwohl ANPD von 50 im Jahr 2021 auf 141 Mitarbeitende im Jahr 2024 gewachsen ist, besteht weiterhin Ressourcenknappheit.

Die ANPD hat wichtige Regelungen zum Datenschutz in Brasilien erlassen, darunter Meldepflichten bei Datenpannen und Kooperationspflichten. Die Verhängung von Sanktionen erfolgt bedächtig, obwohl tausende von Beschwerden wegen Datenschutzverletzungen eingegangen sind. Bis Herbst 2024 wurden lediglich sieben Verwarnungs- und Sanktionsentscheidungen getroffen, zumeist im Bereich der öffentlichen Verwaltung und unzureichender Meldung von Sicherheitsvorfällen (ANPD 2024c).

Das Einhalten der Datenschutzvorschriften gestaltet sich sowohl im öffentlichen als auch im privaten Sektor herausfordernd. Datenschutz wird jedoch für Unternehmen bedeutender, da er sich auf ihre Reputation auswirkt. Die bisher wenigen, aber strengen Maßnahmen der ANPD veranschaulichen, dass ANPD bestrebt ist, Compliance-Praxen zu verbessern und interne Prozesse zu stärken. Unter der Regierung von Präsident Lula da Silva seit 2022 entwickelt sich die ANPD zu einer resilienteren und glaubwürdigeren Institution, insbesondere im Hinblick darauf, die Standards der OECD, zu der Brasilien beitreten will, zu erfüllen.

Seit 2024 erhielt ANPD weitere Aufgaben, sie fungiert nun auch als Koordinationsbehörde für die Regulierung Künstlicher Intelligenz. Im Zuge dieser Aufgabenerweiterung hat ANPD eine öffentliche Konsultation zu automatisierten Entscheidungen durch KI ausgeschrieben, deren Ergebnisse sie in einer Technischen Mitteilung zusammenfasst (ANPD 2024a). Das Personal soll nunmehr um weitere 200 Personen aufwachsen, um die Aufsicht bei der Regulierung von KI zu übernehmen. Ein brasilianisches KI-Gesetz wurde im Dezember 2024 vom Senat verabschiedet und an den Kongress zur Befassung überwiesen.

Im Juli 2024 erließ ANPD (2024b) eine Präventivmaßnahme, mit der die sofortige Aussetzung der neuen Datenschutzrichtlinie von Meta in Brasilien angeordnet wurde, welche die Verwendung der auf seinen Plattformen veröffentlichten personenbezogenen Daten für das Training von KI-Syste-

men erlaubten. Für die Nichteinhaltung wurde eine tägliche Geldstrafe von 50.000 R\$ (rund 8000 Euro) festgesetzt. Im November 2024 begann die ANPD, TikTok hinsichtlich des Umgangs mit Daten von Kindern zu untersuchen. Die ANPD prüfte, ob die Plattform Daten von Minderjährigen unrechtmäßig sammelt und verarbeitet, und hat die Nutzung der App ohne Registrierung und Altersüberprüfung verboten. Im März 2025 versprach ByteDance, dieser Anordnung nachzukommen (Flach 2025).

Das 2025 in Brasilien gestartete Pilotprojekt „dWallet“, initiiert von der kalifornischen Firma DrumWave in Zusammenarbeit mit der staatlichen Firma Dataprev soll Bürger:innen ermöglichen, ihre persönlichen digitalen Daten zu verwalten, Eigentumsrechte daran geltend zu machen und durch deren Verkauf Geld zu verdienen. ANPD hat bereits 2022 ein Inspektionsverfahren gegen DrumWave eingeleitet, um seine Vereinbarkeit mit LGPD zu prüfen (ANPD 2022; Daros 2025).

TFH, einem Unternehmen, das von Sam Altman, CEO von OpenAI, und dem deutschen Informatiker Alex Blania gegründet wurde, gelang es, die Iris-Scan-Daten von 400.000 Brasilianer:innen zu registrieren, indem es ihnen einen Geldbetrag in Kryptowährung anbot. Im Januar 2025 ordnete ANPD jedoch an, dass Tools for Humanity (TFH) diese Praxis einstellen muss, unter Verweis auf eine Beeinträchtigung für die freie Zustimmung der Nutzer und Verstöße gegen das Datenschutzgesetz. TFH argumentiert, dass die Sammlung biometrischer Daten digitale Sicherheit erhöht und es Datenschutzstandards einhält, doch ANPD hält die Praxis aufgrund der Nicht-Rückholbarkeit der gesammelten Daten und der Vulnerabilität der Teilnehmenden für besonders bedenklich (ANPD 2025a, DW 2025).

Wie aus diesen Maßnahmen deutlich wird, hat ANPD inzwischen an Biss gewonnen und geht auch den Praktiken großer US-Unternehmen auf den Grund. Obwohl das LGPD eine wichtige Errungenschaft darstellt, ist seine Durchsetzung in Brasilien selbst bisher noch schwach. Dies liegt auch daran, dass eine Datenschutzkultur kaum ausgeprägt ist. In Brasilien ist es üblich geworden, die Steuernummer CPF (*Cadastro de Pessoas Físicas*) überall abzufragen; in Supermärkten erhält man damit einen Rabatt, auch Apotheken, Museen und Ämter erfragen sie. Sensible Daten können so leicht getrackt und unter der einheitlichen CPF zusammengeführt werden. Zudem trennen Brasilianer:innen in ihren sozialen Netzwerken und Messenger-Diensten nicht zwischen Beruf und Privatem, sondern teilen sogar recht intime Fotos bereitwillig mit Kollegen und Öffentlichkeit. Allfällige Datenlecks werden leichtfertig hingenommen.

Allerdings gibt es weitere Kräfte, die dazu führen, dass Privatsphäre ernster genommen wird. Dazu zählen das Verfassungsgericht, wo wichtige Verfahren anhängig sind und eine gut organisierte digitalrechtliche Zivilgesellschaft. Bundesrichter Alexandre de Moraes vom Obersten Bundesgericht Brasiliens ordnete beispielsweise am 30. August 2024 die Telekommunikationsbetreiber an, die App X (ehemals Twitter) aufgrund unzureichender Bekämpfung von Hassrede und Verletzung der Regelungen zur Anwesenheit eines rechtlichen Vertreters im Land zu sperren. Diese Anordnung wurde am 2. September 2024 vom Obersten Gerichtshof bestätigt. Moraes hatte Elon Musk ein Ultimatum gesetzt, bestimmte rechtsradikale Nutzerkonten und die Verbreitung gewisser Falschinformationen, insbesondere zum Sturm auf die Regierungsgebäude in Brasília im Januar 2023, zu löschen. Dem war Musk nicht nachgekommen, sondern zog stattdessen seinen rechtlichen Vertreter aus Brasilien ab. Nachdem X dann angeblich „versehentlich“ eine Umgehungsmöglichkeit zur weiteren Nutzung von X in Brasilien eröffnet hatte, wurde zudem ein hohes Strafmaß verhängt. Aus diesem Kräftemessen mit X ging Moraes als Sieger hervor. Nach etlichen Verunglimpfungen fügte sich Musk, zahlte die Geldstrafe von rund 5 Mio. US-Dollar und benannte auch wieder einen Repräsentanten für das Land, woraufhin am 9. Oktober 2024 die Sperrung aufgehoben wurde (AP 2024). Zu Musks Einlenken hat sicherlich auch beigetragen, dass binnen weniger Tage Bluesky in Brasilien zwei Millionen neue Nutzer:innen (insgesamt 4 Millionen) verzeichnete (X hat 21 Millionen Nutzer in Brasilien).

Der Oberste Gerichtshof Brasiliens STF (*Supremo Tribunal Federal*) traf am 26. Juni 2025 eine weitreichende Entscheidung über die Haftung von Online-Plattformen für Nutzerinhalte. Die Richter entschieden mit einer Mehrheit von 8 zu 3 Stimmen, dass Social-Media-Plattformen in Zukunft direkt für illegale Inhalte ihrer Nutzer haftbar gemacht werden können. Eine vorherige gerichtliche Anordnung zur Löschung solcher Beiträge ist daher nicht mehr erforderlich (Krempf 2025).

Abschließend bleibt festzuhalten, dass das Datenschutzgesetz LGPD ein bedeutender Fortschritt ist, aber bisher auch aufgrund begrenzter personeller und finanzieller Ressourcen noch nicht stark durchgesetzt wird. US-Technologieplattformen wie Meta und Alphabet ziehen weiterhin große Mengen an personenbezogenen Daten ab. Dies wird durch geringe Datenkompetenz und Zero-Rating-Angebote begünstigt, bei denen Mobilfunkanbieter den Kund:innen Tarife anbieten, welche die Nutzung von Meta-Diensten wie Facebook, Instagram und WhatsApp ermöglichen, ohne dass dies ihr Datenvolumen einschränkt. Viele ärmere Internetnutzer nut-

zen somit fast nur diese Dienste und können entsprechende Postings nicht durch Suchmaschinen und andere Quellen überprüfen. ANPD hat jedoch seit 2022 durchaus an Gewicht gewonnen. Brasilien orientiert sich nicht nur an der DSGVO, sondern neuerdings auch am AI-Act und dem DMA der EU (Carvalho/Iglesias 2025). Insofern ist der Brüssel-Effekt durchaus wirksam.

4.3 Datenschutz in Indien

Indiens Weg hin zu einer Datenschutzgesetzgebung begann am 24. August 2017, als sein Oberster Gerichtshof im spektakulären *Puttaswamy v. Union of India-Urteil* das Recht auf Privatsphäre als verfassungsmäßiges Grundrecht anerkannte. Nach vier Durchgängen von Gesetzentwürfen, in denen deren Inhalt immer mehr verwässerte, verabschiedete das Parlament 2023 schließlich die *Digital Personal Data Protection Bill (PDPB)*. Diese letztliche Gesetzesfassung ist jedoch bislang nicht in Kraft getreten; die hierfür notwendig zu erlassenden Ausführungsvorschriften (*Rules*) wurden erst im Januar 2025 als Entwurf veröffentlicht. Es sind zudem noch die Ernennung einer Datenschutzkommission sowie Mechanismen für Audits und grenzüberschreitende Datenübertragungen erforderlich.

Das PDPB-Gesetz integriert zentrale Prinzipien des Datenschutzes, tendiert jedoch eher zu einer prozeduralen Regulierung und stützt sich nicht explizit auf ein zu schützendes Grundrecht. Es enthält DSGVO-ähnliche Bestimmungen zum Zugang, zur Berichtigung und Löschung persönlicher Daten sowie Verpflichtungen bezüglich Datenminimierung, Zweckbindung und Eingrenzungen bei der Speicherung. Eine explizite Begrenzung der Datensammlung und eine spezifische Kategorie für sensible Daten fehlen jedoch, stattdessen wird ein schwammiges Konzept des „deemed consent“ (vermutetes Einverständnis) eingeführt.

Das finale PDPB-Gesetz verzichtet auf die Forderung nach Datenlokalisierung, die Indien lange international vorangetrieben hatte. Stattdessen sieht es die amtliche Benachrichtigung über eine Liste „vertrauenswürdiger Geografien“ für Datenübertragungen vor. Die aktuellen Entwürfe von Ausführungsbestimmungen enthalten Regelungen, die bedeutsame Datenverarbeiter verpflichten können, bestimmte Kategorien persönlicher Daten lokal in Indien zu speichern (Rajmohan 2025).

PDPB enthält Klauseln, die der Regierung recht umfassende Befugnisse zum Zugriff auf persönliche Daten gewähren, auf Grundlage weit ge-

fasster Interessen wie nationale Souveränität, Sicherheit, außenpolitische Beziehungen und öffentliche Ordnung (Chapter IV, 17, 2(a) PDPB). Kritiker bemängeln, dass das Gesetz eher die Machtbefugnisse der Regierung stärke als den Individuen größere informationelle Selbstbestimmung zu verschaffen (Jhalani 2022). Man vermutet, dass einige Bestimmungen des PDPB vor dem Verfassungsgericht landen werden und die Regierung Modi sich lediglich Zeit habe kaufen wollen (Interviews Indien). Angesichts der bislang verabschiedeten PDPB-Regelungen dürfte Indiens Datenschutzrahmen größte Schwierigkeiten haben, die Angemessenheits-Standards der EU hinsichtlich des grenzüberschreitenden Datenverkehrs zu erfüllen.

Die indische Regierung entwirft eine eigenständige, techno-nationalistische Digital-Agenda, unterstützt durch *NITI Aayog* (*National Institution for Transforming India*) und den privaten Thinktank *Observer Research Foundation* (ORF), gegründet von der schwerreichen Ambani Familie. Indien distanziert sich von China und hat beispielsweise den Betrieb der App Tiktok verboten. Neben dem Datenschutz verfolgt Indien eine strategische Neuausrichtung im Bereich der digitalen Governance und strebt die Etablierung eines „Vierten Weges“ in der Digitalpolitik an, der auf die Förderung digitaler öffentlicher Infrastrukturen (*digital public infrastructures*, *DPIs*) setzt und zielt damit auf eine globale Transformationsrolle im Rahmen von G20 und UN (Sharma et al. 2023).

4.4 Datenschutz in Südafrika

Die Entwicklung des Datenschutzes in Südafrika reflektiert einen breiteren Trend in Afrika. Seit 2001 haben 35 afrikanische Staaten Datenschutzgesetze verabschiedet. Regionale Abkommen wie die Konvention für Cybersicherheit und Datenschutz der Afrikanischen Union (Malabo-Übereinkommen) betonen die Bedeutung eines umfassenden Datenschutzes, jedoch haben noch nicht alle Mitgliedsstaaten das Übereinkommen ratifiziert (Access Now 2024). In der neuen Verfassung Südafrikas nach dem Ende der Apartheid wurde 1996 das Recht auf Privatsphäre (Artikel 2, Abs. 14) konstitutionell verankert.

Das Schutzgesetz für persönliche Daten (*POPIA- Protection of Personal Information Act*), verabschiedet 2013, wurde erst 2020 vollständig umgesetzt und die Durchsetzungsmaßnahmen im Jahr 2021 eingeleitet. Das Gesetz enthält zahlreiche Elemente, die an die DSGVO erinnern. Es hat allerdings die Besonderheit, dass auch personenbezogene Daten juristischer Personen

geschützt sind. Die Umsetzung wird durch den unabhängigen *Information Regulator*, so der Name der Datenschutzbehörde, überwacht. Im Haushaltsjahr 2022/2023 wurden 895 Beschwerden eingereicht; 68,8 % dieser Fälle wurden gelöst (Malinga 2023). Diese hohe Aufklärungsrate unterstreicht das Engagement dieser Behörde, insbesondere bei Verletzungsfällen in Regierungsstellen. Im Jahr 2023 verhängte die Datenschutzbehörde erstmals Bußgelder, vor allem gegen staatliche Organisationen wie Justizministerium, Bildungsministerium und Polizeibehörden, was auf erhebliche Mängel im Umgang mit persönlichen Daten hinweist (Information Regulator 2023). 2024 folgten weitere Ordnungsmaßnahmen, etwa gegenüber der Wahlkommission und dem Bildungsministerium (Mzekandaba 2024a).

Der Information Regulator befasst sich zunehmend auch mit US-Unternehmen, was seinen Willen zur Durchsetzung der Vorschriften gegen große Akteure im Datenökosystem verdeutlicht. So wurde WhatsApp wegen Doppelstandards bei der Datenverarbeitung zwischen Europa und Südafrika gerügt, wobei vor allem Metas Praxis, WhatsApp-Daten mit Facebook ohne Widerspruchsmöglichkeit seitens der Nutzer zu teilen, kritisiert wurde. Bereits im März 2021 hatte der Information Regulator einen Brief an Facebook Südafrika gesendet, im September 2024 folgte eine Vollstreckungsverfügung (Information Regulator 2021; Mzekandaba 2024b).

Der Information Regulator ist auf einem guten Weg, Datenschutz solide zu implementieren. Trotz positiver Entwicklung bestehen jedoch Herausforderungen wie etwa knappe Personalressourcen, mit nur 90 Mitarbeitenden bei einem Jahresbudget von rund 100 Millionen ZAR (4,8 Mio. EUR). Die Bewältigung von Verletzungen bei der Datensicherheit und die Steigerung der Compliance bleiben weiterhin zentrale Anliegen. Die geringe Datenschutz- und Privatsphäre-Kultur in der Bevölkerung erschwert die Kontrolleinsätze zusätzlich. Die Überwachung von Social-Media-Plattformen befindet sich noch im Anfangsstadium; die Bußgeldschwelle von maximal 10 Millionen ZAR (rund 482.000 EUR) erscheint unzureichend, um größere Tech-Firmen abzuschrecken. Zudem mangelt es am Austausch mit zivilgesellschaftlichen Organisationen, was Potenziale stärkeren aufklärerischen Engagements ungenutzt lässt.

4.5 Fazit zum Datenschutz

Datenschutzbehörden müssen sich mit zunehmenden technologischen Komplexitäten befassen, insbesondere im Bereich sozialer Netzwerke, KI

und automatisierter Entscheidungsprozesse. Relevante öffentliche Akteure, Wissenschaftler:innen sowie zivilgesellschaftliche Organisationen in den untersuchten Ländern bekunden ihre Wertschätzung gegenüber den digitalen regulatorischen Bemühungen der EU. Mehrere Länder des Globalen Südens orientieren sich an der EU im Bestreben, die Macht der Big Tech-Unternehmen (GAFAM) einzuschränken, Marktdiversität zu fördern und die demokratische Integrität zu schützen. Allerdings sind die Durchsetzungsfähigkeiten der lokalen Institutionen finanziell und organisatorisch begrenzt, und die politischen Prioritäten der jeweiligen Staaten liegen häufig auf anderen Feldern.

Zusammenfassend lässt sich festhalten, dass die DSGVO die Datenschutzgesetzgebung in den genannten Ländern maßgeblich beeinflusst hat, und somit ein de-jure-Brüssel-Effekt durchaus erkennbar ist. In der praktischen Um- und Durchsetzung der nationalen Datenschutzgesetze gibt es jedoch eine große Spannweite. Mexiko hat mit INAI eine aktive Datenschutzbehörde aufgebaut, die jedoch jüngst von der Regierung unter Kuratel gestellt und mit dem Verlust der behördlichen Unabhängigkeit deutlich geschwächt wurde. Brasilien und Südafrika haben durchaus ernsthafte Schritte in der Durchsetzung von Datenschutz unternommen. Brasiliens ANPD richtet sich derzeit stärker im Hinblick auf KI-Regulierung aus. Südafrikas Information Regulator hat bisher vor allem Datenschutzverletzungen im öffentlichen Sektor im Fokus und konzentriert sich auf das Durchsetzen bestehender Regularien zur Bekämpfung von Korruption und zur Stärkung der Rechenschaftspflichten der Regierung.

Im Hinblick auf eine stärkere Regulierung der großen Tech-Plattformen sind die untersuchten Länder bisher eher zaghaft. Dies liegt mit daran, dass die administrativen Kapazitäten als unzureichend angesehen werden, da Beamte teils nicht gut genug ausgebildet sind oder Personal häufig fluktuiert. Auch die Furcht, hohe Kosten bei Rechtsstreits aufzuwerfen und ggf. gerichtlich zu unterliegen, spielt eine Rolle. Nicht zuletzt ist die Lobbymacht und das Drohpotential der Plattformen nicht zu unterschätzen, da einige Plattformen bei Auseinandersetzungen durchaus gedroht haben, ihre Dienste aus dem Land abzuziehen. Dass sie dies in die Tat umsetzen, erscheint sehr unwahrscheinlich, sind doch die Länder des Globalen Südens nicht nur bevölkerungsreich, sondern es befinden sich dort bei gesättigten Märkten in den Industriestaaten auch die nächsten Milliarden Kund:innen. Gleichwohl zeitigen diese Drohungen eine gewisse Abschreckungswirkung. Das geschilderte Beispiel der temporären Suspendierung von X in Brasilien zeigt jedoch, dass demonstrative Stärke und Beharren auf dem Rechtsstaat

auch gegenüber einem Elon Musk obsiegen kann. Der eigenen Bevölkerung indes den kostenfreien Zugang zu Metas Diensten (im Sinne des Zero-Rating beim Handy-Datenvolumen) streitig zu machen, wird sich wohl weder Brasilien noch eine andere Regierung trauen, auch wenn man dieses Zero-Rating als Verstoß gegen die Netzneutralität werten könnte. Hier wäre der breite Ausbau öffentlicher WLAN-Netze eine Alternative, um auch ärmeren Bevölkerungsschichten den Zugang zum Internet zu gewähren.

Südafrika pocht gegenüber den großen US-Plattformen darauf, dass in Europa durchgesetzte Regelungen auch in Südafrika Geltung erlangen, etwa bei Metas Zusammenführung von Daten von WhatsApp mit Facebook, darüber hinaus auch bei kartellrechtlichen Untersuchungen (CCSA 2023). Insofern scheint Südafrika den Brüssel-Effekt sogar aktiv einzufordern, indem es sich darauf beruft, die Plattformen sollten nicht mit Doppelstandards agieren, sondern das hohe europäische Schutzniveau auch in Südafrika anwenden.

In Indien hingegen scheint Datenschutz - bisher jedenfalls - eher eine Fassade zu sein, denn ein ernsthaftes Unterfangen. Allerdings verfügt Indien über eine wache und agile Zivilgesellschaft, die Digitalrechte einfordert, jedoch zunehmend unter repressiven Druck seitens der Regierung von Präsident Narendra Modi gerät. Indiens „vierter Weg“ in der Digitalpolitik, vorgestellt im Rahmen seiner G20-Präsidentschaft im Jahr 2023, zielt darauf ab, digitale Infrastrukturen als öffentliches Gut (DPIs) weltweit zu fördern. Mittels der Zusammenarbeit mit dem Entwicklungsprogramm der Vereinten Nationen (UNDP 2024) und dem „Global Digital Compact“ durch die UN im Jahr 2024 strebt Indien eine führende Rolle in einer multipolaren globalen Ordnung an. Die Bedeutung der DPIs wächst international, wobei durchaus Synergien mit den EU-Initiativen im Bereich Daten Governance und Data Act entstehen können (Dang et al. 2024).

5. Schlussfolgerungen für die EU Digital-Governance

Während die Datenschutzbehörden die Relevanz der EU-Regulierungen anerkennen, bilden diese dennoch nur einen von mehreren Referenzpunkten. Indien, Brasilien und Südafrika sind auch Mitglied der BRICS-Staaten und sehen in der Ausweitung zu BRICSplus Optionen für ein stärkeres eigenständiges Gewicht des Globalen Südens. Insgesamt beharren alle vier Staaten darauf, Datenschutz an den eigenen sozio-politischen Kontext anzupassen, statt ein einheitliches Modell europäischer Vorschriften wie der

DSGVO zu implementieren. So wird etwa ein „Recht auf Vergessenwerden“ von der Zivilgesellschaft in vielen Ländern abgelehnt, da sie befürchten, dass korrupte Politiker dadurch sie belastende Informationen unzugänglich machen könnten.

Insgesamt sind unterschiedliche Prioritäten erkennbar: Während Indien eine innovative, globale digitale Rahmenordnung anstrebt, die gleichen Zugang zu Technologie fördert, konzentriert sich Südafrika auf die Durchsetzung datenschutzrechtlicher Vorgaben in einem Kontext von historisch bedingtem Misstrauen (sowohl innerstaatlich wie international), wie auch angesichts enormer sozioökonomischer Herausforderungen. Indien navigiert derzeit durch innenpolitische Spannungen hinsichtlich Überwachung, nationaler Sicherheit und technikbasierter Kontrolle. Das biometrische Aadhaar-Authentifizierungs-System, bei dem über 1,2 Milliarden Inder:innen registriert sind, bildet die Grundlage für weitere „Schichten“ des *India Stack*, das digitale Zahlungssysteme und weitere digitale Anwendungen großflächig ausrollen will. Indien verfolgt damit das Ziel, internationale Anerkennung und Wertschätzung für seinen Ansatz der digitalen öffentlichen Infrastrukturen (DPIs) zu gewinnen (Sieker 2024; Sharma 2023).

Der geopolitische Kontext, geprägt durch Russlands Invasion in der Ukraine und Konflikte im Nahen Osten, hat die Staaten des Globalen Südens vom Westen distanziert und sie im BRICSplus-Verbund enger an China und Russland herangeführt. Diese Verschiebung könnte sich auf den digitalen Raum auswirken. Zudem gibt es durchaus auch einen „Beijing-Effekt“, mittels dessen China versucht, über technische Infrastrukturen, Standards und internationale Foren seine Einflussphäre auszudehnen (Erie/Streinz 2021; Recorded Future 2021). Und man könnte möglicherweise von einem „Washington-Effekt“ sprechen, bei dem die aktuelle US-Regierung durch Ausweitung der Exekutivbefugnisse und Vergeltungsdrohungen die Durchsetzung von Regulierungen in der EU und anderen Ländern zu behindern sucht (The White House 2025; Chen 2025). Das im April 2025 begonnene Verhängen unilateraler Zölle seitens der US-Regierung gegen ihre Handelspartner weltweit, legitimiert als (protektionistischer) Schutz der US-Industrie, dient demnach vor allem als Druckmittel, um Länder zu Zugeständnissen zu zwingen. Mitte des Jahres 2025 verhandeln die USA mit über 70 Ländern über Handelsbelange. Die US-Forderungen betreffen sowohl die Rücknahme von Digitalsteuern als auch die Abschwächung von Digital-Regulierungen wie DMA, DSA und AI-Act. Sie dienen zudem als Faustpfand für den US-Handelsbeauftragten (USTR), um den globalen digitalen Handel zu liberalisieren, privatisieren und deregulieren. Big-Tech-

Unternehmen stellen die US-Zölle als marktkorrigierende Mechanismen dar, die wettbewerbsverzerrende Praktiken bestrafen sollten. Digitale Regulierungen werden somit als „nichttarifäre Handelshemmnisse“ reframed, und Handelspolitik als ein strategisches Instrument ergriffen, um strategische Prioritäten von großen US-Digitalunternehmen weltweit voranzutreiben. Beim Begünstigen der US-Digitalplattformen geht es darum, Services ohne Betriebsstätte im Land anzubieten, grenzüberschreitende Datentransfers unreguliert zu erlauben, Datenzentren aufzubauen sowie Daten zu extrahieren und zu speichern, ohne Steuern im jeweiligen Land zu errichten (Nayyar 2025; Kilic 2025; Hingle 2025; Banga et al. 2025).

Der Brüssel-Effekt wird häufig nur aus europäischer Perspektive betrachtet, was Reminiszenzen an koloniale Attitüden wecken kann. Die Länder verlangen kooperative Partnerschaften und Dialog auf Augenhöhe. Während die Staaten des Globalen Südens zunehmend eigene digitale Governance-Modelle entwickeln, stehen sie vor spezifischen Herausforderungen und suchen an ihre jeweiligen Kontexte angepasste Lösungen. Der Einfluss der EU ist spürbar, aber keineswegs ein Selbstläufer. Mexiko ist ökonomisch eng mit den USA verbunden und hat es schwer, eigene regulative Ansprüche durchzusetzen. Staaten mit stärkeren wirtschaftlichen Verflechtungen zur EU tendieren eher dazu, deren Regelwerke zu übernehmen, wobei gemeinsame Werte bezüglich Demokratie und Menschenrechten eine wichtige Rolle spielen – insbesondere bei jüngeren Demokratien wie Brasilien und Südafrika. Die Unterstützung der EU beim Kapazitätsaufbau und Wissenstransfer zur Regulierungspraxis könnte diesen Ländern helfen, wirksame digitale Governance-Strukturen zu etablieren (Schneider 2025).

Abschließend besteht Forschungsbedarf, um Anu Bradfords These zu prüfen, wonach Big Tech-Plattformen ihre Plattform-Designs global an den hohen EU-Standards ausrichten („de facto Brüssel-Effekt“). Zum einen gibt es – jedenfalls anekdotische – Hinweise dafür, dass die Digitalunternehmen ihre Dienste durchaus im Hinblick auf den Datenschutz differenzieren und die hohen EU-Vorschriften nicht gleichermaßen überall anwenden. Zum anderen könnten sich paradoxerweise gerade *durch* die zunehmenden *nationalen* gesetzlichen Regelungen des Datenschutzes graduelle oder gar stark divergierende Abweichungen vom DSGVO-Standard ergeben, so dass Unternehmen dies ausnutzen, etwa geringere Datenverarbeitungsstandards anwenden oder mehr Daten erheben und an Dritte weitergeben. Hier bedarf es weiterer empirischer Forschungen, um die tatsächlichen Effekte und Wechselwirkungen zu verstehen.

Auf einer übergeordneten Ebene stehen Europa und der Globalen Süden vor ähnlichen Herausforderungen, wie zunehmende geopolitische Spannungen und Abhängigkeiten von global agierenden Tech-Unternehmen. Diese Entwicklungen betonen die Notwendigkeit, die digitale Souveränität zu stärken und eigene technologische Kapazitäten aufzubauen. Beispielsweise kann die öffentliche Beschaffung als ein Instrument genutzt werden, um unterschiedliche Anbieter und technologische Lösungen zu fördern. Im Rahmen öffentlicher Aufträge trägt dies dazu bei, Abhängigkeiten zu verringern, Innovationen zu fördern und den Wettbewerb zu stärken (FES 2024). Europa sollte den Dialog mit den Ländern des Globalen Südens intensivieren, die meist technikoptimistischer sind und danach streben, digitale Entwicklungssprünge zu machen sowie als wichtige Akteure auf der Weltbühne anerkannt zu werden. Im Austausch zu europäischen historischen Erfahrungen, etwa gezogene Lehren aus staatlicher Überwachung, kann dies dazu beitragen, Sensibilisierung und gegenseitiges Verständnis zu fördern. Europa muss anerkennen, dass die Prioritäten des Globalen Südens neben Sicherheitsfragen etwa die Verbesserung der Konnektivität, die Überbrückung der digitalen Kluft und die Förderung digitaler Inklusion umfassen, stets im Einklang mit den UN-Zielen für nachhaltige Entwicklung (SDGs) (G20 South Africa 2025; UNCTAD 2024). Der stärkere Impetus auf kollektive Rechte, Entwicklung und globale öffentliche Güter in diesen Regionen erfordert es, unterschiedliche Narrative, kulturelle Kontexte und drängende Anliegen zu berücksichtigen, um einen gemeinsamen Verständigungsraum zu schaffen.

Insofern reicht es nicht, auf den Brüssel-Effekt zu vertrauen, sondern die EU muss sich stärker nach außen orientieren, um ihre Position in der globalen Digital-Governance zu behaupten. Die EU sollte strategische Allianzen mit gleichgesinnten Ländern wie Brasilien, Indien, Südafrika, Mexiko, Kanada, Großbritannien, Japan und Australien schmieden, um ihre digitale Resilienz, Souveränität und globale Stellung zu stärken. Solche Allianzen sind von entscheidender Bedeutung für die Förderung einer wettbewerbsfähigen und nachhaltigen digitalen Wirtschaft, in der die Grundwerte, die Menschenrechte und die Rechtsstaatlichkeit geachtet werden. Im „Digitalen Kompass“, der EU-Strategie bis 2030, wird anerkannt, dass die EU einen umfassenden und koordinierten Ansatz für den Aufbau digitaler Koalitionen und diplomatische Initiativen benötigt, um geopolitische Rivalitäten zu bewältigen (European Commission 2021, Kap.6; European Council 2022 und 2024). Dabei ist es wichtig, Grundrechte, offene und menschenzentrierte Technologien in Partnerschaften zu integrieren und gemeinsam

geteilte technologische Souveränität anzustreben, um machtarke Einflussnahmen, Cyberangriffe und technologische Dominanz zu verhindern. Die EU hat mit den digitalen Regulierungsakten bereits bedeutende Vorbilder geschaffen, doch um ihre Glaubwürdigkeit als globales Referenzmodell zu wahren, muss sie diese Verordnungen konsequent umsetzen und ihre Position gegen Tech-Monopole stärken (Csernatori 2025; von Thun et al. 2025; Schneider 2018; 2020; 2025). In der internationalen Zusammenarbeit ist eine feste Allianz zur Einhegung von Tech-Giganten notwendig, um den Einfluss aus den USA, China und Russland einzudämmen. Die EU sollte sich zudem aktiv gegen das Ausnutzen der Marktmacht der Tech-Konzerne stellen, um ihre demokratischen Werte und wirtschaftlichen Interessen zu sichern, statt zögerlich auf Konfrontation zu verzichten. Nur durch mutige Regulierung und Kooperation kann die EU ihre technologische Souveränität und ihren globalen Einfluss langfristig sichern.

Danksagung

Diese Forschung wurde vom Rahmenprogramm für Forschung und Innovation „Horizont 2020“ der Europäischen Union im Rahmen der Marie-Sklodowska-Curie-Fördervereinbarung Nr. 873119, PRODIGEES (Promoting Research on Digitalisation in Emerging Powers and Europe towards Sustainable Development) mitfinanziert. Die Autorin dankt allen Interviewpartner:innen sehr herzlich für ihre wertvollen Einblicke und Perspektiven. Teile dieses Artikels basieren in überarbeiteter Fassung auf Auszügen aus meinem englischsprachigen Policy Report für die spanische IE University (Schneider 2025).



Co-funded by
the European Union

Literatur

Alle angegebenen Webseiten wurden zuletzt am 29. Juni 2025 besucht.

- Access Now (2024): *Strengthening data protection in Africa. Key issues for implementation*. URL: <https://www.accessnow.org/wp-content/uploads/2024/01/Strengthening-data-protection-in-Africa-key-issues-for-implementation-updated.pdf>
- ANPD (Autoridade Nacional de Proteção de Dados) (15. Juli 2022): *Instauração de procedimento de fiscalização*, https://www.gov.br/anpd/pt-br/assuntos/fiscalizacao-2/saiba-como_fisalizamos/arquivos-processos-de-fiscalizacao-concluidos/serpro-x-drumwave-00261-001457_2022_84_documentos_publicos.pdf
- (20. Juni 2024a): *ANPD é formalizada como coordenadora do Sistema Nacional de Inteligência Artificial*. URL: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-e-formalizada-como-coordenadora-do-sistema-nacional-de-inteligencia-artificial>
- (2. Juli 2024b): *ANPD determina que Meta suspenda uso de dados pessoais para treinamento da IA*. URL: <https://agenciagov.ebc.com.br/noticias/202407/anpd-determina-suspensao-cautelar-do-tratamento-de-dados-pessoais-para-treinamento-da-ia-da-meta>
- (2024c): *Balanco de 4 Anos, 11/2024*. URL: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/anpd-balanco-4-anos.pdf>
- (23. Mai 2025): *Inteligência Artificial: ANPD publica nota técnica sobre decisões automatizadas*. URL: <https://lefosse.com/noticias/inteligencia-artificial-anpd-publica-nota-tecnica-sobre-decisoes-automatizadas/>
- (24. Januar 2025b): *ANPD determina suspensão de incentivos financeiros por coleta de íris*, URL: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-determina-suspensao-de-incentivos-financeiros-por-coleta-de-iris>
- AP (Associated Press) (2024): *Musk's X to be reinstated in Brazil after complying with Supreme Court demands*. 09.10.2024. URL: <https://apnews.com/article/brazil-x-elon-musk-supreme-court-de-moraes-e32c4b417e78cbe8994f53713a922f7>
- (2025): *JD Vance rails against 'excessive' AI regulation in a rebuke to Europe at the Paris AI summit*. 11.02.2025. URL: <https://apnews.com/article/paris-ai-summit-vance-1d7826affdcdb76c580c0558af8d68d2>
- Banga, Karishma; Beyleveld, Alexander und Munu, Martin Luther (2025): *Trading away tax sovereignty? How trade rules shape taxation of the digital economy in Africa*, *Journal of International Economic Law*, 28(1), S. 43–62, <https://doi.org/10.1093/jiel/jgaf004>
- Banisar, David (28. Januar 2025): *National Comprehensive Data Protection/Privacy Laws and Bills 2025*. URL: <https://ssrn.com/abstract=1951416>
- Belli, Luca und Zingales, Nicolo (2017): *Platform regulations: how platforms are regulated and how they regulate us*. FGV Brasil, URL: <https://repositorio.fgv.br/items/d35abb4b-ed3c-467c-97c8-5c59710cc9c7>
- Belli, Luca und Doneda, Danilo (2022): *Data protection in the BRICS countries: legal interoperability through innovative practices and convergence*, *International Data Privacy Law* 13(1): ipac019, <https://doi.org/10.1093/idpl/ipac019>

- Bendiek, Annegret und Römer, Magnus (2019): Externalizing Europe: the global effects of European data protection. *Digital Policy, Regulation and Governance* 21(1), S. 32-43.
- Biden, Joseph (2023): Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, 30.10.2023, URL: <https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/>
- Bioni, Bruno (2020): Memory of the LGPD, URL: <https://www.observatorioprivacidad.com.br/en/memory/>
- Bradford, Anu (2019): *The Brussels Effect: How the European Union Rules the World*. Oxford University Press.
- (2023a): *Digital Empires*. Oxford University Press.
- (2023b): Europe's Digital Constitution, 6.9.2023, Verfassungsblog, <https://verfassungsblog.de/europes-digital-constitution/>
- (2024): The False Choice Between Digital Regulation and Innovation, *Northwestern University Law Review*, 118(2).
- Bruegel (2024): Digital factsheet #4: A dataset on EU legislation for the digital world, Q3, 20.07.2024, URL: <https://www.bruegel.org/dataset/dataset-eu-legislation-digital-world>
- CAIDP (2025): Artificial Intelligence and Democratic Values Report, <https://www.caidp.org/reports/aidv-2025/>
- Carvalho, Daniel und Iglesias, Simone (2025): Brazil Took on Musk and Won. Now Lula Is Sharing Notes With Europe, Bloomberg, 03.02.2025, URL: <https://www.yahoo.com/news/brazil-took-musk-won-now-100000060.html>
- CCSA (Competition Commission South Africa) (2023): Online Intermediation Platforms Market Inquiry, Final Report and Decision, July 2023, URL: <https://www.compcos.co.za/online-intermediation-platforms-market-inquiry/>
- CERRE (Centre on Regulation in Europe) (2024): Global Governance for the Digital Ecosystems Project, URL: <https://cerre.eu/global-governance-for-the-digital-ecosystems/>
- Chen, Brian J. (2025): The 'Washington effect' could decide the AI race, 23.06.2025, URL: <https://www.koreatimes.co.kr/opinion/20250623/the-washington-effect-could-decide-the-ai-race>
- Cohen, Julie E. (2019): *Between Truth and Power: The Legal Constructions of Informational Capitalism*. New York, NY: Oxford University Press.
- Csernaton, Raluca (2025): The EU's AI Power Play: Between Deregulation and Innovation, 20.05.2025, URL: <https://carnegieendowment.org/research/2025/05/the-eus-ai-power-play-between-deregulation-and-innovation>
- Dachwitz, Ingo und Hilbig, Sven (2025): *Digitaler Kolonialismus. Wie Tech-Konzerne und Großmächte die Welt unter sich aufteilen*. München: C.H. Beck
- Dang, Vy; Bootwalla, Aliasger; Lynders, Eva Maria; Reiners, Wulf (2024): Synergising digital public infrastructure and digital commons for sustainable development: the governance of digital resources in India and the EU, URL: <https://www.gatewayhouse.in/synergising-dpi-digital-commons/>

- Daros, Gabriel (30. Mai 2025): In a world first, Brazilians will soon be able to sell their digital data, URL: <https://restofworld.org/2025/brazil-dwallet-user-data-pilot/>
- DW (25. Januar 2025): ANPD prüft pagamento por coleta de íris no Brasil, Deutsche Welle, <https://www.dw.com/pt-br/anpd-pro%C3%ADbe-pagamento-de-criptomoed-as-por-coleta-de-%C3%ADris-no-brasil/a-71404849>
- Erie, Matthew Steven und Streinz, Thomas (2021): The Beijing Effect: China's 'Digital Silk Road' as Transnational Data Governance. *N.Y.U. J. Int'l L. & Pol* 54 (1).
- European Commission (2020): Digital Compass: The European way for the Digital Decade, COM/2021/118 final, URL: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52021DC0118>
- (2024): The future of European competitiveness – A competitiveness strategy for Europe, Draghi Report, 09.09.2024, URL: https://commission.europa.eu/topics/strengthening-european-competitiveness/eu-competitiveness-looking-ahead_en
 - (2021): Digital Compass: the European way for the Digital Decade, COM/2021/118 final, URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52021DC0118>
- European Council (2022a): 'Path to the Digital Decade': the EU's plan to achieve a digital Europe by 2030, URL: <https://www.consilium.europa.eu/en/infographics/digital-decade/>
- (2022b): EU Digital Diplomacy: Council Conclusions, Foreign Affairs Council, 18 July 2022, 11406/22.
 - (2024): A digital future for Europe, URL: <https://www.consilium.europa.eu/en/policies/a-digital-future-for-europe/>
- FES (Friedrich Ebert Stiftung) (2024): Policy Study: Time to build a European digital ecosystem, 09.12.2024, <https://library.fes.de/pdf-files/bueros/bruessel/21688.pdf>
- Fischer, David (2022): The digital sovereignty trick: why the sovereignty discourse fails to address the structural dependencies of digital capitalism in the global south. *Z Politikwiss* 32, S. 383–402 (2022). URL: <https://doi.org/10.1007/s41358-022-00316-4>
- Flach, Natália (14. März 2025): TikTok complies with Brazilian data authority ruling on minors, O Globo, URL: <https://valor.globo.com/empresas/noticia/2025/03/14/tiktok-cumpre-decisoes-da-anpd-sobre-acesso-de-jovens.ghtml>
- G20 South Africa (2025): Speech by Minister Solly Malatsi During the Opening Ceremony of the Second G20 Meeting of the Digital Economy Working Group, 07.04.2025, URL: <https://g20.org/g20-media/minister-solly-malatsi-during-the-opening-ceremony-of-the-second-g20-meeting-of-the-digital-economy-working-group/>
- GDPR Enforcement Tracker (2025), URL: <https://www.enforcementtracker.com/>
- Glenny, Misha und Muggah, Robert (2025), Big Tech Is Part of Trump's Threat to the Global Order, Foreign Policy, 03.06.2025, URL: <https://foreignpolicy.com/2025/06/03/trump-big-tech-companies-silicon-valley-threat-geopolitics-digital-sovereignty/>
- Golumbia, David (2024): *Cyberlibertarianism: The Right-Wing Politics of Digital Technology*. University of Minnesota Press.
- Hingle, Audrey (15. Mai 2025): The Winners of Tariff Diplomacy: U.S. Tech Companies, URL: <https://internet.exchangepoint.tech/the-winners-of-tariff-diplomacy-u-s-tech-companies/>

- Hobbs, Carla (2020): The EU as a digital regulatory superpower: Implications for the United States, URL: https://ecfr.eu/article/commentary_the_eu_as_a_digital_regulatory_superpower_implications_for_the_u/
- Holzmann, Anna und Zenglein, Max (2019): Made in China 2025 - Wie weit China auf dem Weg zu globaler Technologieführerschaft bereits gekommen ist. Merics. URL: <https://merics.org/de/studie/made-china-2025>
- Huitron, Ale (9. Mai 2025): INAI desaparece; Secretaría Anticorrupción y Buen Gobierno asume funciones, URL: <https://www.infobae.com/mexico/2025/05/10/inai-desaparece-secretaria-anticorrupcion-y-buen-gobierno-asume-funciones/>
- Information Regulator (2021): Information Regulator to take further action regarding the WhatsApp privacy policy, 13.05.2021, URL: <https://inforegulator.org.za/wp-content/uploads/2020/07/ms-20210513-WhatsAppPrivacyPolicy.pdf>
- Information Regulator (2023): Annual Report 2022 – 2023, URL: <https://inforegulator.org.za/wp-content/uploads/2020/07/Information-Regulator-Annual-Report-2023-Compressed.pdf>
- Jhalani, Radhika (2022): India's Data Protection Bill: the hits and misses, 07.12.2022, URL: <https://www.context.news/surveillance/opinion/indias-data-protection-bill-the-hits-and-misses>
- Jia, K., Chen, S. (2022): Global digital governance: paradigm shift and an analytical framework. *GPPG* 2, 283–305). URL: <https://doi.org/10.1007/s43508-022-00047-w>
- Kilic, Burcu (27 Juni 2025): Between Tariffs and Tech: What Will Europe Choose? Bot Populi, URL: <https://botpopuli.net/between-tariffs-and-tech-what-will-europe-choose/>
- Krempel, Stefan (29. Juni 2025): Brazil's Supreme Court: Digital platforms are liable for user contributions, URL: <https://www.heise.de/en/news/Brazil-s-Supreme-Court-Digital-platforms-are-liable-for-user-contributions-10463575.html>
- Lilkov, Dimitar (2020): Made in China. Tackling Digital Authoritarianism. Martens Center for European Studies, URL: https://www.martenscentre.eu/wp-content/uploads/2020/06/paper_made-in-china-webversion.pdf
- Malinga, Sibahle (2023): InfoReg resolves 70% of POPIA complaints, Johannesburg, 05 April 2023, URL: <https://www.itweb.co.za/article/inforeg-resolves-70-of-popia-complaints/LPp6VMrByz4MDKQz>
- Mayring, Philipp (2022): *Qualitative Inhaltsanalyse*. 13. Auflage. Weinheim; Basel: Beltz.
- Mazzucato, Mariana (2013). *The Entrepreneurial State: Debunking Public vs. Private Myths in Risk and Innovation*. London: Anthem Press.
- Mzekandaba, Simnikiwe (2024a): POPIA violation lands education dept in hot water, 14.11.2024, URL: <https://www.itweb.co.za/article/popia-violation-lands-education-dept-in-hot-water/KzQenvjynNyqZd2r>
- Mzekandaba, Simnikiwe (2024b): WhatsApp privacy policy fails POPIA compliance, says watchdog, 11.09.2024, URL: <https://www.itweb.co.za/article/whatsapp-privacy-policy-fails-popia-compliance-says-watchdog/Gb3BwMWaV1ov2k6V>
- Nayyar, Abhineet (26 Juni 2025): Trump's Tariffs and the Big Tech Takeover, Bot Populi, URL: <https://botpopuli.net/trumps-tariffs-and-the-big-tech-takeover/>

- Open.AI (2025): Ankündigung: The Stargate Project, URL: <https://openai.com/de-DE/index/announcing-the-stargate-project/>
- Rajmohan, Karthika (23. Januar 2025): Data Localization: India's Tryst with Data Sovereignty, URL: <https://www.techpolicy.press/data-localization-indias-tryst-with-data-sovereignty/>
- Recorded Future (2021): China's Digital Colonialism: Espionage and Repression Along the Digital Silk Road, 27.07.2021, URL: <https://go.recordedfuture.com/hubfs/reports/cta-2021-0727.pdf>
- Reid, Jenni (2025): The EU could hit Wall Street where it hurts with its tariff response – the tech giants, CNBC, 4.2.2025, URL: <https://www.cnbc.com/2025/04/04/how-the-eu-could-target-us-big-tech-with-its-tariff-response.html>
- Rudl, Thomas (21. Mai 2025): US-Regierung drängt Staaten zur Zulassung von Starlink, netzpolitik.org, URL: <https://netzpolitik.org/2025/globaler-sueden-us-regierung-draengt-staaten-zur-zulassung-von-starlink/>
- Schneider, Ingrid (2018): Bringing the state back in: Big Data-based capitalism, disruption, and novel regulatory approaches in Europe, in: Schneider, Ingrid; Rudinow Saetnan, Ann; Green, Nicola (Hrsg.): *The Politics of Big Data: Big Data, Big Brother?* New York: Routledge, S. 129-175.
- (2020). Democratic Governance of Digital Platforms and Artificial Intelligence? Exploring Governance Models of China, the US, the EU and Mexico. *JeDEM - EJournal of EDemocracy and Open Government*, 12(1), 1-24. URL: <https://doi.org/10.29379/jedem.v12i1.604>
- (2022): Das ferne Echo Europas: Plattformregulierung, Datenschutz und Digitalkultur in Mexiko, in: Bogner, Alexander; Decker, Michael; Nentwich, Michael; Scherz, Constanze (Hrsg.): *Digitalisierung und die Zukunft der Demokratie. Beiträge aus der Technikfolgenabschätzung*. Baden-Baden: Nomos.
- (2025): Policy Report "Reclaiming Digital Sovereignty: The EU's Role in the Geopolitics of Digital Governance", IE University, Center for the Governance of Change, 02/2025, URL: https://static.ie.edu/CGC/CGC_ReclaimingDigitalSovereignty_PolicyPaper.pdf
- Sharma, Sharad; Ramanathan, Madhumitha; Iyer, Arun; Abraham, Vivek (2023): Digital Public Infrastructures: Lessons from India for a Thriving Data Economy, IE CGC, 11/2023, URL: [https://static.ie.edu/CGC/12.%20ISPIRT%20-%20Digital%20Public%20Infrastructures%20\(November%202023\).pdf](https://static.ie.edu/CGC/12.%20ISPIRT%20-%20Digital%20Public%20Infrastructures%20(November%202023).pdf)
- Sieker, Felix (2024): Aadhaar and the rise of Digital Public Infrastructure in India, 13.11.2024, URL: <https://www.reframetech.de/en/2024/11/13/aadhaar-and-the-rise-of-digital-public-infrastructure-in-india/>
- Staab, Philipp (2024): *Markets and Power in Digital Capitalism*. Manchester: Manchester University Press.
- The White House (21. Februar 2025): Memorandum: Defending American Companies and Innovators From Overseas Extortion and Unfair Fines and Penalties, URL: <https://www.whitehouse.gov/presidential-actions/2025/02/defending-american-companies-and-innovators-from-overseas-extortion-and-unfair-fines-and-penalties/>

- UNCTAD (United Nations Conference on Trade and Development) (2021): *Digital Economy Report 2021*. New York.
- (2024): *Digital Economy Report 2024*, Shaping an environmentally sustainable and inclusive digital future, UNCTAD/DER/2024.
- UNDP (2024): UN Releases Universal DPI Safeguards Framework to Promote Safe and Inclusive Digital Public Infrastructure, 24.09.2024, URL: <https://www.undp.org/press-releases/un-releases-universal-dpi-safeguards-framework-promote-safe-and-inclusive-digital-public-infrastructure>
- Villanueva Plasencia, Daniel (11. Januar 2023): \$60 Million in fines from the INAI, URL: <https://www.linkedin.com/pulse/60-million-fines-from-inai-daniel-villanueva-plasencia/>
- von Thun, Max, Riekeles, Georg und Kuzev, Pencho 2025: Doubling Down, not Backing Down. Defending the EU's Digital Sovereignty in the Trump Era, 28.02.2025, KAS, URL: <https://www.kas.de/documents/d/guest/doubling-down-not-backing-down>