Germany's Role in Europe's Digital Regulatory Power: Shaping the Global Technology Rule Book in the Service of Europe

Barker, Tyson; Hagebölling, David

German Council on Foreign Relations

October 2022

DGAP REPORT

Germany’s Role in Europe’s Digital Regulatory Power

Shaping The Global Technology Rule Book in the Service of Europe

Tyson Barker
Head, Technology and
Global Affairs Program

Dr. David Hagebölling
Associate Fellow,
Technology and
Global Affairs Program

CHAPTER OVERVIEW

Key Takeaways

1 Four elements help to map the strengths and, at times, the limits of German power in digital rule-making. First, Germany anticipates EU digital regulation and attempts to establish facts on the ground. Second, Germany has outsized influence in the formal stages of EU digital regulatory policymaking. Third, the EU, in turn, provides Germany with a launch pad for influencing worldwide regulatory norms. Fourth, a belated reawakening of the capacity of the German private sector and affiliated technical standard bodies to influence global technical standards is occurring.

2 Germany, as an EU member state, is engaging in three significant areas of data governance and cybersecurity: digital identities and open data, lawful access to electronic messaging systems, and rules for sovereign cloud usage.

3 Germany's largely successful role as a key incubator for the EU's regulatory approach to digital technology and, therefore, as a proponent of the "Brussels Effect" of influencing global markets is not widely appreciated or understood at home. The lag among regulations, technology, and international context is evident in areas such as data protection, content moderation, and market power of online platforms. Even meaningful regulatory debates on quantum, the metaverse (AR/VR), and 6G have yet to arise in Germany.

4 Germany must change its approach to digital regulation to more accurately reflect the dynamic, general-purpose nature of emerging digital technologies against an increasingly fraught international landscape in which technological rules are a dimension of geopolitical power. This includes more fully addressing political trade-offs associated with digital regulation choices, expanding reviews and sunset clauses in digital regulation to encourage flexibility, and making greater use of multi-stakeholder regulatory approaches that incorporate civil society, companies, and other non-state actors. Germany must also increase the engagement of its foreign policy and national security communities in EU technology diplomacy and in global regulation enforcement.

Introduction

Germany is an important – perhaps the most important – force for setting the EU's digital regulatory approach, which forms a basis for European power in the geopolitics of technology. Germany has been at the heart of the EU's ambitious effort to root digital regulation in human rights, rule of law, and democracy. This regulation of platforms, algorithms, and data governance is set out in the EU's Digital Services Act (DSA), the Digital Markets Act (DMA), the Data Governance Act (DGA), the Artificial Intelligence Act (AI Act), the Data Act and the Cloud Rulebook.[1] Germany's central role in shaping these rules means that the EU will succeed in updating its rule book only if Germany likewise updates its own thinking. That includes acknowledging just how geopolitical regulation has become, and how other powers balance regulation and innovation and, at times, profit with the costs of the EU being a regulatory first mover. As the bloc tackles the next wave in data governance on cloud, edge computing and the Internet of Things (IoT), Germany and, therefore, the EU have the chance to shape a regulatory framework that fosters European values and global competitiveness.

The State of Play

Germany is a confident, assiduous, and skilled actor in shaping digital regulation at the national and, particularly, the EU level. It understands the levers of regulatory power on digital technology in Brussels, and through various channels – federal and state governments, the private sector, and German civil society – Germany has the tools to shape the European rule book in a way that is consistent with an ordoliberal, rule-centric approach to digital sovereignty. But to the extent that the rule book becomes the basis for global digital regulation, German awareness breaks down. Four elements help to map the strengths and, at times, the limits of German power in digital rule-making.

[1] Tyson Barker, "2021 Is the Year the Internet Gets Rewritten," Foreign Policy, January 19, 2021: https://foreignpolicy.com/2021/01/19/2021-is-the-year-the-internet-gets-rewritten (accessed June 1, 2022).

First, Germany routinely attempts to anticipate EU digital regulation trajectories and to frame digital regulation debates in Brussels around its own concerns, more so than probably any other member state. The EU, in turn, tends to monitor the German debate to pave the way for smooth legal passage of its own priorities. Consequently, German legal traditions (e.g., in the evolution of privacy as the basis for the General Data Protection Regulation (GDPR))[2] and normative ordoliberal thinking (e.g., skepticism of cartels and digital market concentration) enjoy strong influence at the EU level. At the same time, Germany finds itself in something of an echo chamber, believing that its priorities – and not cross-border liberalization of digital services with non-EU like-minded states or regulatory scrutiny of the cyber risks of ICT infrastructure manufactured by China's state-controlled enterprises, for example – are shared European priorities.

Of course, the EU rule book does not always reflect German priorities in the end, and other actors – the Commission, the European Parliament, the private sector including US technology companies, and other member states such as France and tech-savvy Nordic-Baltic states and Ireland – have typically influenced the transition from EU debate to legislation. Tension between the DMA and the 10th amendment to the German Competition Act is one example of this. So, too, is the friction between the DSA's illegal-content regulation and that of Germany's Network Enforcement Act (NetzDG). Still, German anticipation of EU legal debates is marked in almost every way by Berlin's own domestic digital technology policymaking, from the screening of digital foreign direct investment (FDI) to due diligence of technology supply chains.[3] The country's Data Ethics Commission, for example, sketched in 2017 a framework for AI risk categories and assessment that was reflected in the EU's 2020 AI White Paper and its 2021 draft AI Act.[4] Germany's IT Security Law 2.0 and Gaia-X, respectively, primed EU discourse on the Network and Information Security 2 (NIS 2) Directive and the European Cybersecurity Certification Scheme for Cloud Services (EUCS).

Second, Germany, the EU's largest member state, is, in fact, overrepresented in the bloc's digital regulatory policymaking. Germans occupy positions as key European Commission civil servants; well-positioned European Council staff; and members of the European Parliament (MEPs) serving as rapporteurs on key digital legislative packages[5] and influential committee chairs;[6] and key parliamentary secretariat staff. And, although many of these officials represent a broad ideological spectrum, they retain a German political sensibility. Only France rivals Germany in its use of key personnel to shape EU digital policymaking, particularly at the Commission (e.g., DG CONNECT) and in key regulatory agencies such as the Body of European Regulators for Electronic Communications (BEREC).

At times, these officials and representatives reflect the unadulterated interests of German institutions, including important German corporate players.[7] This bias is not problematic in itself but rather a natural byproduct rooted in the connective tissue that binds Germany's European policymakers in Brussels and the political discourse of the German business community. Companies can be good motors for German digital power, but they can also, if left unchecked, redirect German national leverage toward narrow corporate aims. And, more problematic still, they can perpetuate shared corporate blind spots. That includes their heightened sensitivity to potential Chinese retaliation against regulatory scrutiny of data processing and cybersecurity practices of Chinese companies operating in the EU. Businesses in Germany's non-EU allies – Australia, Canada and the United Kingdom – are less worried about this because they are less dependent on Chinese markets. Market codependence with China has forced Germany to strike a balance between its need for Chinese consumers and its commitment to its own values in digital technology.

International and geopolitical concerns do, of course, frame German – and European – digital regulation, but these still bear the scars of past experiences dealing with the United States and suspicions regarding data protection and espionage. Following the 2013 Snowden revelations, Germany's data privacy concern has been primarily aimed at the United States. Recent EU initiatives, particularly the DSA,

[2] Informational self-determination.

[3] Federal Ministry of Labour and Social Affairs, "CSR-Supply Chain Act," (July 22, 2021): https://www.csr-in-deutschland.de/EN/Business-Human-Rights/Supply-Chain-Act/supply-chain-act.html (accessed June 1, 2022).

[4] Tyson Barker, "The Digital Technology Environment and Europe's Capacity to Act," DGAP Report No. 7, German Council on Foreign Relations (November 2021), p. 23: https://dgap.org/sites/default/files/article_pdfs/Mercator%20Study%20Tech_Highres.pdf (accessed June 1, 2022).

[5] The GDPR, DMA, and the NIS Directive, for example.

[6] The Committee on Internal Market and Consumer Protection and the Committee on International Trade, for example.

[7] These include Deutsche Telekom, SAP, Infineon, Bosch, Axel Springer, and Bertelsmann.

the DMA, and European cloud proposals, also mainly affect American technology firms given their market dominance. But the extent to which this is perceived as a means of curtailing US tech influence can raise questions, and the overweening focus on the US simply does not reflect today's geopolitical threats (Box 1). The co-regulatory design – and broad implementing authority for the Commission – in the DSA and DMA provide both with flexibility to evolve in ways that reflect new risks in ever-changing information ecosystems online and the dynamism of platform market power. As the two laws enter into force, an early test for EU platform regulation will be to what extent the DSA and DMA are fit for purpose to respond to the platform landscape of 2023, not 2015.

Third, the EU provides Germany, like other member states, with a launch pad for influencing worldwide regulatory norms. Global technology companies have famously made the EU's GDPR the basis for data protection, including in jurisdictions outside the EU. Four years after the GDPR entered into force, countries such as Argentina, South Korea, Japan, and Kenya, and subnational powers such as California, with its California Privacy Rights Act (CPRA), use the GDPR as the basis for their own data protection regulation. Even the growing pressure on Washington to establish a federal US data protection law is driven, in part, by Europe. And the 2020 Schrems II decision, which struck down the 2016 Privacy Shield Framework for transatlantic transfers of personal data, forced the United States to make substantial changes to managing European grievances and to expanding checks on intelligence services' data collection. The EU, as a regulatory first mover, has bent the global regulatory environment toward itself. This is a success for German concerns, but there are drawbacks. Many non-EU states, and most EU member states for that matter, struggle to meet GDPR standards, and this disrupts free data flows. Furthermore, other potentially more fruitful channels are open for the EU to build an international rule book.

On this front, the EU and like-minded states such as Australia, Canada, and the United Kingdom have begun (intergovernmental) regulatory discourse in fields reaching beyond data protection. These fields include content moderation, platform governance, the market power of individual firms, data protection, and risk-based approaches to AI. But this is a laborious effort as differences in internal legislative processes, regulatory competencies, federal structures, and constitutional limits lead to different outcomes.

At the same time, China has learned to parrot EU regulatory principles in pursuit of a far less high-minded set of goals. Its discourse on technology giants' market power and data protection mirrors the debate in Germany and Europe, but its goal is to mollify international criticism while consolidating the Communist Party's absolutist power. China's 2021 Blocking Statute, which invalidates extraterritorial sanctions within the country, was modeled on EU law.[8] Chinese regulation on personal data protection (including the 2020 Global Initiative on Data Security),[9] competition, algorithms, and, most recently, on "positive energy" content governance[10] borrow from European deliberations and, at times, even take the letter of European law. Still, these efforts are designed to conscript the Chinese technology sector and other actors into the service of party-state interests.

Fourth, Europe's rule-setting power would be much smaller without Germany and its private sector's influence in global technical standard-setting bodies. The German Institute for Standardization (DIN), the German Commission for Electrical, Electronic & Information Technologies (DKE), and the Association for Electrical, Electronic & Information Technologies (VDE) comprise a core of national bodies that feed into their European and international counterparts. Germany is one of six permanent members of the International Organization for Standardization (ISO) Council and holds 18% of ISO secretariats, 19% of International Electrotechnical Commission (IEC) secretariats, and 29% of IEC working group chairs.[11] It also fields candidates for key positions, such as its 2022 bid for the director of the International Telecommunications Union's (ITU) Telecommunication Standardization Bureau.[12]

[8] Kelly Austin et al., "China's 'Blocking Statute' – New Chinese Rules to Counter the Application of Extraterritorial Foreign Laws," Gibson Dunn, January 13, 2021: https://www.gibsondunn.com/chinas-blocking-statute-new-chinese-rules-to-counter-the-application-of-extraterritorial-foreign-laws (accessed June 1, 2022).

[9] Embassy of the People's Republic of China in the United States of America, "Global Initiative on Data Security," September 8, 2020: https://www.mfa.gov.cn/ce/ceus//eng/zgyw/t1812951.htm (accessed June 1, 2022).

[10] Maria Siow, "Positive energy: the darker side of China's social media catchphrase," South China Morning Post, June 21, 2020: https://www.scmp.com/week-asia/people/article/3089846/positive-energy-darker-side-chinas-social-media-catchphrase (accessed June 1, 2022).

[11] International Organization for Standardization, "DIN," August 4, 2022: https://www.iso.org/member/1511.html (accessed August 10, 2022).

[12] International Telecommunication Union, "Elections," (2022): https://www.itu.int/pp22/en/elections/candidates (accessed June 1, 2022).

GERMANY'S HEAVY US FOCUS

The transatlantic technological relationship remains the world's primary artery of digital activity. Undersea information and communications technology (ICT) cables crossing the North Atlantic carry 55 percent more data flows than transpacific routes. But global digital activity, like all economic activity, is shifting away from the United States and toward the Indo-Pacific and Global South, even as Germany's regulatory enforcement posture remains intently Atlantic-centric.

Germany's January 2021 Data Strategy focused heavily on Gaia-X as a means of emancipating Europe from US cloud services (and the provisions of the Clarifying Lawful Overseas Use of Data (CLOUD) Act, which provides conditions for US authorities to access certain data in other countries), in part through the use of open source software such as OpenStack. The current German discussion about data localization, platform dependence, and encryption continues to be overshadowed by the National Security Agency revelations in 2013, former US President Donald Trump's election in 2016, and the Cambridge Analytica scandal in 2017.

The EU's regulatory enforcement effort is likewise primarily focused on the Euro-Atlantic. GDPR enforcement among Germany's 17 Data Protection Authorities (DPAs) remains directed at US service providers and platforms. This has been justified given the dominant role of US digital services in the European market over the past decade. But the preponderance of DPA scrutiny of US technology firms contrasts with the lack of scrutiny of systemic violations by firms from adequacy states such as the United Kingdom, Canada, and Japan, and even by European firms themselves. Perhaps most interesting has been the proportionate lack of scrutiny of systemic violations, particularly in legal access requirements, by authoritarian states such as China and Russia.

There are, however, some indications that the spotlight is slowly shifting away from the United States. The EU's draft AI regulation, informed by Germany's 2020 EU presidency and the Federal Government's Data Ethics Commission, pays greater attention to Chinese practices than similar EU regulation has in the past. The Commission draft's most stringent provisions address social scoring, which it bans, and remote real-time biometric identification, which only law enforcement agencies in narrowly defined situations may use. These measures are implicitly based on China's actions. The promotion of good moral behavior has long been characteristic of Chinese society, but AI-powered biometric identification combined with extensive video surveillance and a social scoring system forms a powerful and dangerous tool for social control.

But in the same way that Germany is sometimes blind to the abundant influence of its private sector in shaping European regulation, it has been slow to recognize the relative decline in influence of Team Germany – and, consequently, Team Europe – in international standard-setting. The role of Germany's private sector has been shrinking as especially Chinese state-owned and state-adjacent enterprises have gained control of key technical working groups and fielded model standards.[13] China's push for regional standard-setting arrangements through its Belt and Road Initiative could also create lock-in effects for third-party countries that tilt toward a mercantilist digital international system that favors China and techno-authoritarianism. This is part of a broader design that Henry Kissinger has called China's "patient accumulation of relative advantage."[14] Germany, like the rest of Europe, has only belatedly realized that technical standard-setting is freighted with geopolitical danger, and this realization has come at a time when German private sector participation in international standard-setting bodies has atrophied.

[13] Tim Rühlig, "Technical standardisation, China and the future international order. A European perspective," E-Paper, Heinrich Böll Stiftung Brussels (February 2020): https://eu.boell.org/sites/default/files/2020-03/HBS-Techn%20Stand-A4%20web-030320.pdf (accessed June 1, 2022).

[14] Tom McTague, "Joe Biden Has a Europe Problem," The Atlantic, January 21, 2021: https://www.theatlantic.com/international/archive/2021/01/joe-biden-europe/617753 (accessed June 1, 2022)

The Current Policy Approach

The present German government's digital regulation debate is focused on a number of data governance and cybersecurity questions related to seamless digital interaction with public administration, lawful access to electronic messaging systems, and rules for sovereign cloud usage. This marks a change in focus from recent waves of EU regulation, in the sense that it recontextualizes data protection much more in terms of cybersecurity and away from state, and state-adjacent private, actors. This could provide opportunities for a recalibration of Germany's European role to clearly define democratic principles of data governance in ways that are flexible and consistent with Germany's understanding of digital sovereignty. So, what, precisely, is Germany doing?

A DIGITALLY ENABLED STATE

First, on the demand side, German efforts are focused on establishing cross-sectoral and secure electronic digital identities (eIDs) that draw on the experience of the Nordic and Baltic EU member states, and Ukraine, which have adopted eIDs.[15] Germany's eID Act came into force in September 2021 and laid the legal foundation for digital identification via smartphones with secure authentication technology supported by the Federal Printing Office (*Bundesdruckerei*). The government promised limited digital ID services by the end of 2021, but they remain offline. Problems with digital driver's licenses, an ID wallet, and a Smart eID persist.[16] On the supply side, Germany's 2017 law on improving online access to public administration services (OZG) obliged federal, state, and local governments to offer administrative services digitally by the end of 2022, a deadline that governments at all levels are likely to miss.[17] The OZG aims to connect government portals so that businesses and citizens can use a single user account to access online services.[18] There is a risk here that bureaucratic foot-dragging in its implementation, lack of coordination among government agencies and, ultimately, non-uniform and uneven data availability could also lead to suboptimal use by researchers and the private sector.

LAWFUL ACCESS TO ONLINE COMMUNICATION

Another measure worth noting is the attempt by the German federal government to define conditions under which law enforcement agencies may compel messaging services to provide access to encrypted communications, a lingering point of tension between the law and end-to-end encryption. This has also been a topic of conversation for the EU since the disclosure of the FBI's "Lawful Access" document of January 2021 that revealed which data law enforcement authorities may obtain from various messenger services.[19] Services such as Apple, Signal, and Telegram continue to demur.[20]

Last year, the European Commission itself announced a draft law on "chat control," which then quickly disappeared from the agenda, possibly due to the massive protests of more than 30 civil society

[15] The Federal Ministry of Economic Affairs and Climate Action estimates that developed economies with a well-functioning digital identity infrastructure can increase their gross domestic product by 3 to 4 percent. Federal Ministry for Economic Affairs and Climate Action, "Im Fokus: Sichere digitale Identitäten" [In Focus: Secure digital identities], (October 2021): https://www.bmwk.de/Redaktion/DE/Schlaglichter-der-Wirtschaftspolitik/2021/11/05-im-fokus-digitale-identitäten.html (accessed June 1, 2022).

[16] Viola Heeger, "Digitale Identitäten: Deutschland im Verzug" [Digital identities: Germany behind schedule], Tagesspiegel Background Digitalisierung & KI, December 20, 2021: https://background.tagesspiegel.de/digitalisierung/digitale-identitaeten-deutschland-im-verzug (accessed June 1, 2022).

[17] Federal Ministry of the Interior and Community, "Onlinezugangsgesetz (OZG)" [Online Access Act (OZG)], (2022): https://www.bmi.bund.de/DE/themen/moderne-verwaltung/verwaltungsmodernisierung/onlinezugangsgesetz/onlinezugangsgesetz-node.html (accessed June 1, 2022).

[18] At the European level, the eIDAS regulation (Regulation (EU) No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market, which repealed Directive 1999/93/EC) contains binding Europe-wide regulations in the areas of "electronic identification" and "electronic trust services." The regulation created a uniform framework for the cross-border use of national electronic identification measures and, therefore, for the use of the German online ID card and trust services.

[19] Martin Holland, "FBI über Messenger: An welche Daten von WhatsApp & Co. US-Strafverfolger kommen" [FBI via Messenger: What data from WhatsApp & Co. US law enforcement officers obtain], Heise Online, December 2, 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 (accessed June 1, 2022).

[20] Apple's iMessage service offers end-to-end encryption and provides user data only under subpoenas, and chat info is available only if backed up in iCloud. Telegram can provide possible IP addresses and phone numbers. Signal releases only dates and times of the most recent message. With WhatsApp, the world's most popular messenger service, however, investigators can access user data, blocked accounts, contacts, and message destinations.

organizations.[21] But the Commission tabled in May 2022 a proposal to "[lay] down rules to prevent and combat child sexual abuse."[22] The intent is to hold providers of interpersonal communication, in particular, accountable "to detect, report and remove online child sexual abuse on their services."[23] This may subsequently compel messaging and hosting services such as WhatsApp and Signal to soften their encryption procedures or to introduce other controversial solutions, such as hash matching or scans of end-users' devices ("client-side scanning," or CSS).[24] Critics claim the proposal will undermine democratic principles by placing all European citizens under suspicion and undermining internet confidentiality and security.

SOVEREIGN CLOUD AND INDUSTRIAL DATA

Policy efforts in Germany and the EU have been circling each other in an effort to create a cloud infrastructure based on European rules and complemented by a federated European data infrastructure that may limit the market dominance of hyperscalers, with their vast capacity for processing data, through interoperability and portability requirements. The ultimate goal is a competitive cloud landscape under European rules that forms a foundation for infrastructure for the industrial internet and IoT.

Whether this German-led cloud approach will end up giving heft to the country's own ordoliberal, rules-centric notion of digital sovereignty remains unclear. Gaia-X, which is an industry-driven spin-off of a Franco-German government initiative, is one option for an interoperable cloud standards architecture for Europe and, perhaps, beyond. But Gaia-X's tack toward rules-centric digital sovereignty, in part by including US and Chinese players in its governance, has not lived up to the expectations of some European actors, including those in France. It has led some European actors to form rival initiatives, such as the European Cloud Industrial Alliance (EUCLIDIA) and EUCS. These are based on the French cloud certification regime, SecNumCloud, which is meant to isolate public administration from non-European cloud service providers. Moreover, despite announcements of related services such as a federated cloud infrastructure architecture (Structura-X) and sector-specific collaborations in mobility (Catena-X), agriculture (AgriGaia), and finance (EuroDat), Gaia-X seems beset by the deficiencies of similar, previous efforts: low adoption, uncertain private demand, and waning German political support.

Meanwhile, the German debate on data localization is growing. International data flows remain controversial, reflecting Germany's deep ambivalence about the value and benefits of data access. Some in the German government, and politicians, legal experts and NGOs in Germany, are joined by more vociferous voices in France who question whether US cloud providers should store sensitive data at all. Their concerns lie in post-Schrems uncertainty on the protection and privacy of transatlantic data flows and the US CLOUD Act's authorization for US law enforcement to access data stored on servers of US cloud service providers in Europe.[25]

Germany is consequently considering rules for cloud usage in its public administration and sensitive sectors, as the EU looks to create a cloud certification process that considers questions about data localization. Germany joined France, Italy, and Spain – against the Netherlands, Sweden, and Ireland – to back "sovereignty requirements" in EUCS and Gaia-X's Labelling Framework, which would essentially back data localization requirements. The strongest certification, EUCS's "High" and Gaia-X's "Level 3," would limit choice and potentially cut the EU off from hyperscalers – since Amazon, Microsoft and Google are based in the United States – and from European companies with an American footprint, including Deutsche Telekom, SAP, and Bertelsmann. While these certification schemes are currently voluntary, the expectation is that they will, in some form, be required for the provision of public services in the EU in future, with serious implications for data usage across digital

[21] Thomas Rudl and Markus Reuter, "Warum die Chatkontrolle so gefährlich ist" [Why chat control is so dangerous], Netzpolitik, November 4, 2021: https://netzpolitik.org/2021/eu-kommission-warum-die-chatkontrolle-so-gefaehrlich-ist (accessed June 1, 2022).

[22] European Commission, 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, (May 2022): https://eur-lex.europa.eu/resource.html?uri=cellar:13e33abf-d209-11ec-a95f-01aa75ed71a1.0001.02/DOC_1&format=PDF (accessed June 1, 2022).

[23] Ibid., p. 2.

[24] Stefan Krempl, "Chatkontrolle: Informatiker und IT-Verbände gegen EU-weite Massenüberwachung" [Chat control: Computer scientists and IT associations against EU-wide mass surveillance], Heise Online, March 29, 2022: https://www.heise.de/news/Chatkontrolle-Informatiker-und-IT-Verbaende-gegen-EU-weite-Massenueberwachung-6656545.html (accessed June 1, 2022).

[25] Some have even cited the Chinese firewall's level of control as a positive model for a European internet. Nick Sohnemann et al., New Developments in Digital Services, European Parliament, Policy Department for Economic, Scientific and Quality of Life Policies, Directorate-General for Internal Policies (May 2020): https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648784/IPOL_STU(2020)648784_EN.pdf (accessed March 11, 2021).

supply chains. Digital smart-city, health, and education services are among those that will be affected.

GERMANY'S GEOPOLITICAL BLIND SPOTS IN RULE-MAKING

As German policymaking moves forward on digital identities, cybersecurity, law enforcement and cloud governance, three blind spots are evident. These blind spots can impact Germany and the EU's ability to balance governance with innovation and maximize their shaping power.

First, Germany's largely successful role as a key incubator for the EU's regulatory approach to digital technology and, therefore, as a proponent of the "Brussels Effect" of influencing global markets, is not widely appreciated or understood in Germany itself. To the contrary, German debate on technology tends to be inward-looking and gives little thought to how Germany influences the EU and the world. Policy deliberations often leave it to technocrats to reactively elevate national preferences to the European level. The discourse also tends to exclude the potential global implications of German rules, and it fails to assuage German fears about digitalization and data flows, which continue to find expression in EU law.

Second, there are lingering geopolitical issues surrounding the implementation and enforcement of existing rules, particularly of the GDPR, the DSA, and the DMA, which reflect a mismatch between the rules set and the context in which they were set. The preponderant Euro-Atlantic nature of German and EU enforcement aligns with the international digital state of affairs between 2012 and 2015. Since then, Chinese and Russian state-adjacent players have become significant players in cloud services, platform services, closed messaging systems, and smart infrastructure technology. IoT has also assumed more global importance. Regulatory enforcement has not kept up, creating German and European vulnerability in digital governance.

Third, shaping emerging technology rules can be slow to arise in Germany in a meaningful way, even if the country is adept at anticipating the EU debate. The Federal Agency for Information Security (BSI) issued first-of-its-kind model standards for cyber security protection of low earth orbit satellites that are meant to inform European model standards with the European Space Agency.[26] And publicly funded R&D in quantum encryption will help drive standards on post-quantum cryptography, including with partners such as the US National Institute of Standards and Technology (NIST).[27] Nevertheless, the lag between technological development and governance generally remains pronounced in Germany, Europe, and like-minded states. This is hardly supportive of the strategic regulatory environment that Germany and Europe want. Given that Germany's and the EU's market size is in decline relative to the rest of the world, so, too, is their regulatory power. In the midterm, the growing role of demand in India and the Global South will recast their roles in setting global regulations, norms, and market power.

Recommendations

Three factors determine Germany's potential for global rule-making reach: the coherence of its vision, enforcement consistency in Germany and the EU, and the ability to make rules that preserve and strengthen European innovation, including for emerging critical technologies, without abetting protectionism. To embed its regulation and standards in a more hard-nosed geostrategic approach, Germany should:

Address the political trade-offs associated with digital regulation choices. The most difficult aspects of digital regulation often pit key German priorities, such as privacy and security, against each other. This forces policymakers to rank objectives. Debate on issues such as privacy, law enforcement, and national security should consider context, permit transparent oversight, and build on the principle that illegal activity offline is also illegal online.

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

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

Draft model clauses and modules that can be integrated into partner countries' regulation. This could involve creating an open source regulation repository that expedites the process for non-European partners when it comes to achieving adequacy with the EU on personal and industrial data flows, IoT security, and content moderation, and to addressing aforementioned challenges with the GDPR. Model regulatory clauses and modules should be crafted to prohibit their misuse by authoritarians to justify mass surveillance, censorship, and data theft. Germany should also support the ability of other European states to regulate in their own sovereign ways, and the EU could help partner countries assess the impact of their own regulation.

Conduct geopolitical impact assessments of draft German and European digital regulation. As we have argued, German and EU measures could inadvertently strengthen digital authoritarianism or enable unintended and unwanted global trends such as data localization, censorship, weakened cybersecurity, or internet fragmentation. Authoritarian states such as China and Russia have already shown that they are ready to exploit such unintended consequences, picking and mixing rules to justify mass surveillance, censorship, and digital control over their citizens. Candid assessments of the impact of German and EU technology policy outside Europe could combat such misuse.

Fight creeping state-centrism of European technical standard-setting. The international power of European bodies such as the European Committee for Standardization (CEN), the European Committee for Electrotechnical Standardization (CENELEC), and the European Telecommunications Standards Institute (ETSI) stems largely from their openness to private sector actors, including non-European firms. It is not simply that technical standard-setting should be left solely to the private sector. But Germany has an acute interest in balancing private sector leadership with state and European interest. It must lead the effort to preserve the pluralistic nature of European standard-setting. Tipping the balance too much toward the state risks greater inefficiencies and, consequently, diminished German and European power in this area. It could also set an unhelpful precedent for authoritarian regimes.

Bolster private sector technical standard-setting capacity. Germany should introduce tax incentives and public funding mechanisms for domestic companies, startups, and associations to participate in standard-setting bodies, seek chairmanships, field draft standards, and work with like-minded states. Financial support could include grants from the Federal Ministry of Economic Affairs and Climate Action (BMWK) and the Federal Ministry for Digital and Transport (BMDV).

Embed high European Cloud Certification and Gaia-X Architecture of Standards into global cloud governance efforts. As industrial data could become a new frontline in global technology regulation, Germany should look at ways to internationalize its data space model, Gaia-X, to include non-European powers, especially the United States. The EU-US Trade and Technology Council (TTC) could develop democratic data spaces for industrial data based on Gaia-X architecture in national hubs in like-minded non-European powers. And Germany's G7 presidency, in its final phase, could launch work on the free flow of data via trustworthy European regulation of, and architecture for, data storage, processing, and transfer. Japan could continue this work during its 2023 G7 presidency. Finally, Germany could support building the capacities of Global Gateway partner countries to use European cloud computing architectures to increase interoperability and preserve human rights. This aim aligns with the government's promise to strengthen digital sovereignty in the Global South.

Integrate digital regulation and technological standard-setting into the Zeitenwende and the National Security Strategy. Germany must consider more intently the effects of digital regulation on its national security posture and defense industry. The country must ensure it can adopt and deploy dual-use technology on par with peer nations such as France, Canada, Japan, and the United Kingdom. This will require more flexibility in addressing national security interests. Provisions of the AI Act, for example, may prohibit the adoption of deep learning that other states' militaries may exploit. And the unbundled digital services that German competition law and the DMA mandate will have unintended consequences for companies' ability to reinforce their cybersecurity. Germany must better balance its technology regulation with national, EU, and NATO security interests. Germany did this successfully when creating criteria for trustworthy telecommunications equipment in its 2021 IT Security Law 2.0.

Increase the engagement of Germany's foreign policy and national security communities in shaping and enforcing regulatory agreements. The German intelligence, foreign policy, law enforcement, and defense agencies have roles in enforcing technology regulations drawn up in Germany. Just as the United States should promote greater involvement of privacy rights groups in framework discussions, the German government should realize that it is time for those authorities to assume more prominence, and the post-Privacy Shield Transatlantic Data Privacy Framework (TDPF) era will offer a first chance. The German foreign and national security communities have a direct stake in maintaining an open EU-US data bridge that provides private actors with judicial access to US courts, enforceable rights, and limitations on indiscriminate personal data collection. They must take a leadership role in ensuring that the TDPF is a durable solution given the opportunity it presents to create clear regulations for free Euro-Atlantic data flows.

Establish a multistakeholder approach that incorporates civil society, companies, and other non-state actors. Germany and Europe have begun pioneering new models of managing technology regulation. Industrial regulation was highly regimented, appropriate for the engineering-oriented, stable technologies of the factory floor. Digital regulation, however, must be agile, ecosystem-based, and incentive-oriented. Following the DSA/DMA model, it must involve a thicket of relationships, responsibilities, and oversight that can more quickly raise alarms as blind spots in regulation arise. These flexible structures allow for constant oversight that is subject to compromise.

Expand reviews and sunset clauses in digital regulation to encourage flexibility. Given the rate of change in digital technology, regulatory and legal flexibility is key. Review and sunset clauses would compel regulators to consider the effectiveness and relevance of rules. Such clauses would also support consistency with regulation in other democracies. The aforementioned example of the GDPR shows the need for this effort, which also aligns with the imperative of ensuring regulatory certainty and with the importance of reform for future-proofing regulation.

7 – GERMAN AND EU DIGITAL TECHNOLOGY REGULATION (2015 – TODAY)

German Initiative	Stated Aims	EU Initiative	Stated Aims
2015 **IT-Security Law** (IT-Sicherheitsgesetz)	• Set leading standards on IT system security • Protect digital infrastructures, especially in critical technology areas (critical infrastructures/KRITIS) • Establish new warning obligations for telecoms	2016 **NIS Directive**	• Mandate national supervision of critical infrastructure sectors and critical digital service providers • Set requirements for member-state cybersecurity capabilities, including cybersecurity strategies and Computer Security Incident Response Teams (CSIRTS) • Cross-border collaboration
2017 **Network Enforcement Act** (Netzwerkdurchsetzungsgesetz, NetzDG)	• Set up content moderation frameworks for criminally punishable expression such as hate speech and fake news • Establish reporting obligations and penalties for online platforms	2020 **Digital Services Act (DSA) proposal**	• Reform EU-wide digital platform legislation • Set standards on content moderation, advertising, and algorithms • Define obligations including notice-and-action procedures for illegal content
2017 **Data Ethics Commission** (Datenethikkommission)	• Develop ethical guidelines for data policy • Provide a framework to deal with algorithms, AI, and digital innovation • Resolve data ethics questions • Define an approach for overcoming social conflicts within data policy	2021 **Draft AI Act** (derived from the Commission’s 2020 AI White Paper)	• Propose a “human-centric” legal framework for trustworthy AI • Address the risks associated with certain uses of AI • Give users confidence to embrace AI-based solutions while encouraging businesses to develop them
2018 **National Research Data Infrastructure** (Nationale Forschungsdateninfrastruktur, NFDI)	• Network data holdings domestically and internationally • Systematically develop, sustainably store, and make accessible scientific and research data	2018 **European Open Science Cloud (EOSC)**	• Provide European researchers, innovators, companies, and citizens with an open, multidisciplinary environment • Provide European science, industry, and public authorities with world-class data infrastructure, high-speed connectivity, and powerful high-performance computers
2019 **Gaia-X initiative**	• Develop a common software governance framework with the objec tive of ensuring European digital sovereignty • Implement a common set of rules that can be applied to existing technology stacks • Obtain transparency, controllability, portability, and interoperability across data and services.	2021 **Alliance for Industrial Data, Edge and Cloud**	• Strengthen the position of EU industry on cloud and edge technologies • Meet the needs of EU businesses and public administrations processing sensitive data • Foster the development and deployment of next-generation cloud and edge capacities for public and private sectors • Important Project of Common European Interest for Next Generation Cloud Infrastructure and Services (IPCEI-CIS) contributes to the review of the EU Industrial Strategy
2019 **Federal Blockchain Strategy**	• Aim to use the opportunities offered by blockchain and mobilize its potential for digital transformation • Five fields of action: blockchain in the financial sector; funding of projects and real labs; clear reliable framework conditions; digital administrative services; knowledge, networking, and collaboration		
2021 **Federal Data Strategy** (Datenstrategie der Bundesregierung)	• Enhance the innovative and responsible use of data • Develop data competency and establish a data culture • Make data infrastructure effective and sustainable • Put state data infrastructure on a sustainable footing and enhance the data competency of civil servants	2022 **Data Act**	• Ensure fairness through rules for the use of data generated by IoT devices • Develop a framework to promote business-to-government data sharing • Support business-to-business data sharing • Evaluate the Integrated Planning and Reporting (IPR) framework with a view to further enhancing data access and use
		2020 **Data Governance Act proposal**	• Increase trust in data sharing • Strengthen data-sharing mechanisms across sectors and the EU, increasing data availability and overcoming technical obstacles to reuse data
		2021 **EU Cloud Code of Conduct**	• Contribute to an environment of trust and transparency in the European cloud computing market • Simplify the risk-assessment process of Cloud Service Providers (CSPs) for cloud customers.
2021 **IT-Security Law 2.0** (IT-Sicherheitsgesetz 2.0)	• Patch gaps to protect critical infrastructures (KRITIS) • Expand competencies of the Federal Office for Information Security (BSI), allowing for stronger cooperation with law enforcement	2021 **NIS Directive reform**	• Broaden NIS mandate to address fragmentation and implementation snags • Coordinate information sharing, reporting obligations, and sanction regimes across the EU • Set more rigorous requirements for critical infrastructure, such as supply chain security

Source: Authors own illustration

German Initiative	Stated Aims	EU Initiative	Stated Aims
2021 **Telecommunications-Telemedia Data Protection Act** (Telekommunikation-Telemedien-Datenschutz-Gesetz, TTDSG)	• Merge provisions on the protection of telecommunications secrecy and data privacy previously contained in the Telecommunications Act (TKG) and in the Telemedia Act into a new parent law • Adapt existing provisions to the European General Data Protection Regulation and to new definitions in the Telecommunications Act	2017 **e-Privacy Regulation proposal**	• Enforce privacy rules on new players, such as WhatsApp, Facebook Messenger, and Skype • Standardize EU privacy protection • Guarantee protection of communications content and metadata • Streamline cookie consent regulation • Protect users more effectively against spam
		2020 **Data Governance Act proposal**	• Safely enable the sharing of sensitive data held by public bodies, and regulate data sharing by public actors • Increase trust in data intermediaries • Strengthen data-sharing mechanisms across the EU
2021 **10th Amendment to the Restriction of Competition Act** (Gesetz gegen Wettbewerbsbeschränkungen, GWB)	• Give the Federal Cartel Office (*Bundeskartellamt*, BKartA) the ability to take preventive measures to curb the market power of large digital platforms • Introduce changes concerning antitrust investigations procedures, leniency, and cartel damage claims.	2020 **Digital Markets Act (DMA)**	• Curb digital gatekeepers’ unfair business practices • Create a fairer business environment for businesses dependent on gatekeepers • Allow for freer innovation by technology startups • Eliminate unfair terms and conditions limiting technology development • Expand range of customer choices of service providers
2021 **Amendment to the Telecommunications Act** (TKG)	• Create a tailored and forward-looking legal framework for the German telecommunications market • Strengthen the rights of end users • Accelerate the rollout of fiber-optic and mobile networks	2018 **EU Directive 2018/1972:** Establishing the European Electronic Communications Code	• Consolidate and reform the framework for regulating electronic communication networks and services
2020 **Draft Law implementing EU Directive 2018/1972**	• Expand very-high-capacity networks and their use • Ensure sustainable and effective competition and the interoperability of telecommunications services • Ensure accessibility and security of networks and services • Promote the interests of end users		
2021 **17th Amendment to the Foreign Trade and Payments Act** (Außenwirtschafts-verordnung, AWG)	• Comprehensively protect critical infrastructure and key technologies from foreign investment • Extend notifiable acquisitions to new industries in the cross-sectoral screening • Reduce relevant thresholds for notification obligations • Extend sector-specific screening • Standardize deadlines for cross-sectoral and sector-specific screening	2019 **FDI Screening Regulation**	• Preserve Europe’s strategic interests while keeping the EU market open to investment • Address European concerns about the impact of foreign acquisitions • Regulate the notification of existing national investment screening mechanisms to the European Commission (EC) • Establish formal contact points and secure channels in each member state and within the EC for the exchange of information • Develop procedures for member states and the EC to quickly react to FDI concerns
		2021 **Regulation (EU) 2021/821** Control of exports, brokering, technical assistance, transit, and transfer of dual-use items	• Update previous regulatory framework to modernize the EU export controls regime for dual-use items • Set up a regime for the control of exports, brokering, technical assistance, transit, and transfer of dual-use items • Subject dual-use items to effective control when they are exported from or in transit through the EU • Implement new catch-all controls • Set up national control lists and place new controls on technical assistance including on military end-use • Ensure more information exchange and transparency
2017 **Open Data Act**	• Oblige federal authorities to publish on publicly accessible networks unprocessed data that was obtained when fulfilling public-law duties or through third parties • Establish judicial foundation for obtaining data from all public authorities subject to federal government oversight	2019 **Open Data Directive**	• Strengthen the EU’s data economy by increasing the amount of publicly held and publicly funded data available for reuse • Require public bodies to make data available for reuse where possible • Provide real-time access to dynamic data via adequate technical means • Increase the supply of valuable public data for reuse, including from public undertakings • Tackle the emergence of new forms of exclusive arrangements

DGAP

Advancing foreign policy. Since 1955.

Rauchstraße 17/18
10787 Berlin
Tel. +49 30 25 42 31 -0
info@dgap.org
www.dgap.org
@dgapev

The German Council on Foreign Relations (DGAP) is committed to fostering impactful foreign and security policy on a German and European level that promotes democracy, peace, and the rule of law. It is nonpartisan and nonprofit. The opinions expressed in this publication are those of the author(s) and do not necessarily reflect the views of the German Council on Foreign Relations (DGAP).

DGAP receives funding from the German Federal Foreign Office based on a resolution of the German Bundestag.

Publisher
Deutsche Gesellschaft für
Auswärtige Politik e.V.

ISSN 2198-5936

Editing Andrew Cohen

Layout Lara Bührer

Design Concept WeDo

Author picture(s) © DGAP

Cover Photo © IMAGO / aal.photo