ie UNIVERSITY

CENTER FOR THE GOVERNANCE OF CHANGE

cgc.ie.edu

RECLAIMING DIGITAL SOVEREIGNTY

THE EU'S ROLE IN THE GEOPOLITICS OF DIGITAL GOVERNANCE

POLICY PAPER #1
FEBRUARY 2025

TABLE OF CONTENTS

AUTHOR:
Ingrid Schneider

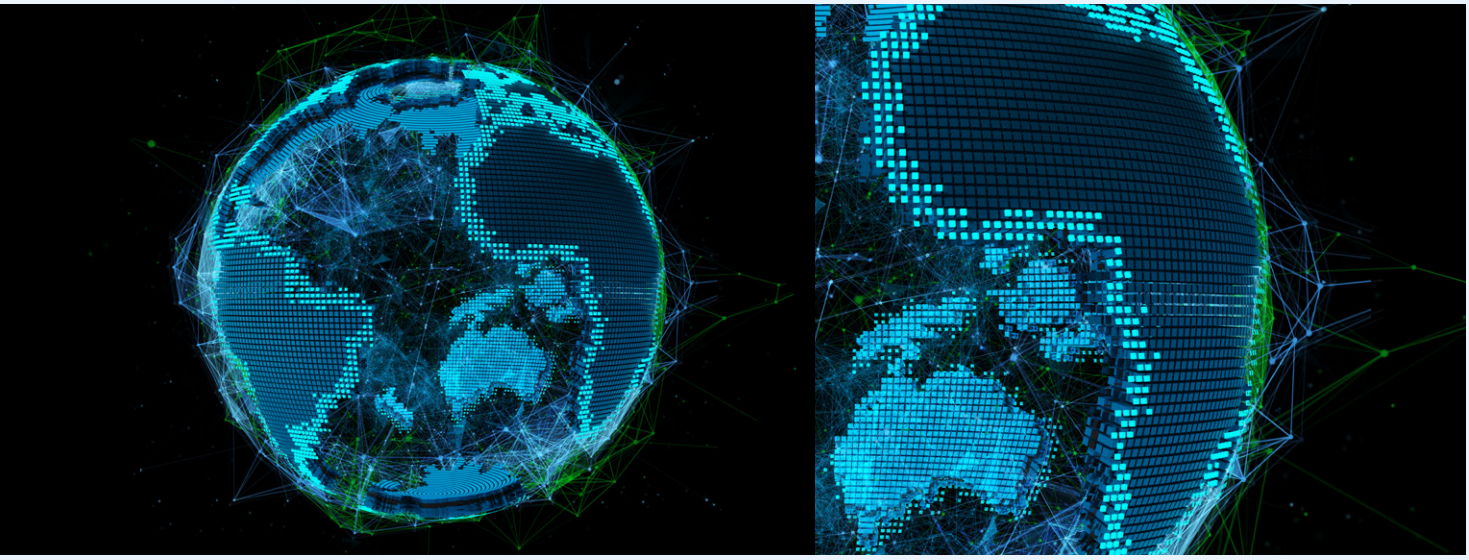
01. INTRODUCTION

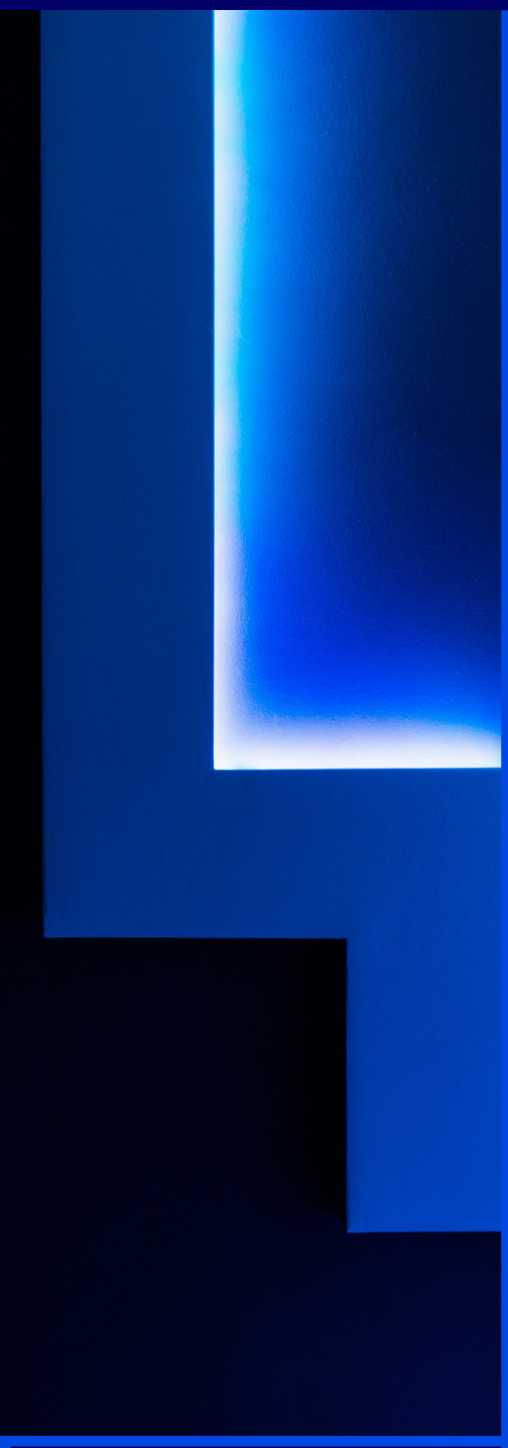
The digital era defines the 21st-century global landscape, bringing opportunities for innovation and economic growth but also posing significant challenges in governance and geopolitics. The emergence of powerful digital technologies has resulted in competing visions for digital governance, primarily led by the United States and China, each embodying fundamentally different principles and practices. As these two digital superpowers vie for influence, the European Union (EU) positions itself as an independent actor with its own distinct regulatory framework. This policy paper explores the EU's potential as a regulatory superpower and its leadership in promoting digital governance based on human rights, democratic values, and ethical considerations.

> The clash between the US and Chinese models of digital governance presents both a challenge and an opportunity for the EU.

The US traditionally advocates for a laissez-faire approach that prioritizes innovation and market freedom, while China models a state-controlled system with strong surveillance capabilities, epitomized by the Digital Silk Road. Against this backdrop, the EU strives to establish a "Third Way" of digital governance, characterized by robust regulations such as the General Data Protection Regulation (GDPR), Digital Markets Act (DMA), Digital Services Act (DSA), Data Governance Act (DGA), Data Act, and AI Act. These measures aim to extend the EU's influence beyond its borders, showcasing the concept of the "Brussels Effect" where EU standards shape global practices.

This paper argues that to maintain its position as a pivotal player in the rapidly evolving geopolitical landscape, the EU must move beyond passive regulatory influence and actively forge strategic alliances with like-minded states across the Global North and South. These alliances are essential for fostering a competitive and sustainable digital economy that upholds fundamental values, human rights, and the rule of law.





REGIMES OF DIGITAL GOVERNANCE

02

02. REGIMES OF DIGITAL GOVERNANCE

Digital governance refers to the policies, regulations, and frameworks that guide the management and operation of digital technologies and the internet. These governance regimes shape a wide array of issues from data privacy and security to innovation and competition.[1] The geopolitical significance of digital governance is evident in the varying approaches adopted by major global players like the United States, China, and the European Union, each operating under distinct regulatory models influenced by their specific motivations and challenges. Recently, discussions around digital politics have increasingly focused on its geopolitical implications.

> The United States and China have emerged as key rivals on the global stage, each striving for technological leadership that will ultimately redefine global power relations.

2.1. THE US MODEL OF DIGITAL GOVERNANCE

The United States' approach to digital governance has traditionally prioritized economic liberty and innovation. The regulatory framework is relatively loose, granting technology companies significant freedom to innovate and grow. Government funding of key innovations[2], access to large amounts of venture capital, engineering talent and knowledge from universities, and techno-optimism coupled with the idea that a free internet advances freedom and democracy are essential components that drive technological advancement and foster a vibrant start-up environment enabling entrepreneurs to turn their ideas into viable products and services.

The US influences the international digital landscape primarily through its dominant GAFAM platforms — Google/Alphabet, Apple, Facebook/Meta, Amazon, and Microsoft—, and has historically adhered to a libertarian model that prioritizes free-market principles.[3] Despite rising public demand for stronger regulation of tech industries over issues such as data-privacy violations and harmful online content, corporate lobbying and political inefficiencies have stymied regulatory progress. As a result, it seems unlikely that there will be a federal privacy law or substantial reforms to Section 230 of the Communications Decency Act of 1996, which provides online intermediaries with immunity from liability for third-party content on their platforms. The country prioritizes maximizing technological potential, largely to maintain its competitive edge, particularly against China. National security interests, nonetheless, provide the government with access to data from internet platforms.[4]

However, under the Biden administration, there were noticeable shifts towards increased government and judicial oversight, as seen in the implementation of antitrust policies by the Federal Trade Commission and the Department of Justice and Biden's executive order on Artificial Intelligence.[5] Trump already repealed Biden's Order on AI. Whether and to what extent antitrust initiatives will continue under the second Trump administration is highly uncertain.[6] Moreover, the recent shift towards governmental subsidies and industrial policies, exemplified by legislation such as the CHIPS Act, which allocates billions in funding to incentivize domestic semiconductor manufacturing and R&D, and the Inflation Reduction Act, mark a significant pivot in the US approach to the tech industry. This signifies a departure from the traditional laissez-faire approach; it targets domestic competitiveness as well as national security, while increasing international rivalry.

> The interplay between Trump's government policy and private sector interests is also likely to drive significant changes in the future; as suggested by the strong alliance that has emerged between the president and Big Tech CEOs at the beginning of his second term.

A massive $500 billion investment has been announced to develop a new AI infrastructure codenamed "Stargate" over the next four years in the United States.[7] However, the release of China's DeepSeek AI chatbot has shaken up the tech industry, quickly becoming the most-downloaded free iOS app in the US and causing Nvidia's market value to drop by nearly $600 billion. Its Large Language Model rivals those of US companies but operates at a fraction of the cost and energy, offering a more environmentally sustainable alternative. This development highlights that sophisticated AI can be achieved with fewer resources, challenging the dominance of major US tech firms.[8] Smaller companies may play a key role in shaping future AI tools, and their influence should not be overlooked.

2.2. THE CHINESE MODEL OF DIGITAL GOVERNANCE

In contrast, China's model of digital governance is state-driven. It is characterized by a top-down approach that leverages technology for economic growth, social control, and political stability. Under this model, the Chinese government has greatly expanded efforts to modernize the economy and social life through digital technologies.[9] At its core, this model is predicated on the belief that state intervention and oversight are essential for maintaining stability and preserving the authority of the Chinese Communist Party (CCP). China has shielded its tech sector from foreign competition and nurtured the industry with state assistance, subsidies, tax incentives, and favorable policies. With intensified geopolitical tensions, China is pursuing technological self-sufficiency and digital protectionism. The country's internet is safeguarded by the Great Firewall, which has facilitated the rise of major Chinese platforms such as Baidu, Alibaba, and Tencent.

This model has been effective in pushing digital transformation forward. The ten-year program "Made in China 2025" strategically focused on high-tech manufacturing, has bolstered the country's "technological sovereignty".[10] However, it comes with significant social costs and infringes on individual rights and civil liberties.[11] The Chinese government exerts significant influence over the technological ecosystem, enables authorities to monitor online behaviors, control data flow, and censor divergent content. The state enforces compliance from technology companies through laws like the Cybersecurity Law and Data Security Law, ensuring government oversight. The Great Firewall exemplifies this centralized approach, serving as a digital barrier that restricts internet access to foreign sites. The government justifies these intrusions as necessary for maintaining order and security, framing them as means to uphold societal "harmony". For citizens who conform to state expectations, China's digital transformation has resulted in a seamless and convenient life. However, this development comes at the cost of stringent internet regulations and severe penalties for those who express dissenting opinions.[12]

While the government encourages certain technological developments for economic purposes, it also implements strict controls to prevent the emergence of powerful private actors that could challenge state authority. The shift toward greater oversight of the technology sector-including recent crackdowns on major tech companies such as Jack Ma's Ant Group in 2020, a large antitrust fine against Alibaba in 2021, and the prevention of a Tencent-backed merger-signals a re-evaluation of how the government engages with the private sector.[13]

China promotes its concept of Cyber Sovereignty internationally by advocating for territorial data localization framing it as an opportunity—especially for developing nations—to enhance their control over data flows. Despite its authoritarian nature, China's tech sector thrives on market-driven innovation, challenging the notion that political freedom is essential for technological advancement.

The external strategy offers an affordable path to digital development through the export of digital infrastructure under the Digital Silk Road that is part of the Belt and Road Initiative (BRI). This includes advanced technologies like 5G through Huawei's cellular infrastructure, networking solutions from ZTE, and various smart city applications. However, these projects often come with high levels of debt and dependencies, to be repaid with strategic minerals and raw materials.[14]

To sum up, China's approach to digital governance combines elements of digital authoritarianism with selective adoption of regulatory measures that are akin to those in the EU. The Chinese government tightly regulates the digital economy with objectives extending from technological superiority to economic growth and stringent political control. This model features data-privacy laws and antitrust regulations aimed at curbing the power of big tech, thus paralleling some EU policies. However, the Chinese model also operates under a framework that utilizes technology for censorship and surveillance, enabling the government to maintain social and political stability.

2.3. GLOBAL IMPLICATIONS OF US AND CHINA RIVALRY

Chinese technological influence has global implications: China's provision of digital infrastructure worldwide is driven by both competitive pricing and an authoritarian appeal to some nations. This growing global adoption of Chinese technology presents a strategic challenge for the US and its allies, threatening to tilt global digital norms towards digital authoritarianism and contradicting the vision of an open, free digital economy envisioned by liberal democracies. Overall, the global digital governance landscape is marked by these strategic alignments and tensions, influencing the trajectories of innovation, regulation, and international relations.

More recent infrastructural and innovation divides exacerbate inequalities. The digital rivalry between the US and China has intensified in recent years with "chip wars" and trade tensions.[15] Indeed, these two nations are also at the forefront of data value creation. They account for over half of the world's hyperscale data centers, possess the fastest internet connections, contribute to more than 94% of funding for AI startups, and encompass 90% of the market capitalization of the largest digital platforms.[16] The current promotion of artificial intelligence has further intensified these concentration processes within the data economy. Further, as the data-driven digital economy has evolved, a data-related divide has emerged. With factors such as water, electricity, local talent, and access to specialized chips becoming key materialities in the AI economy, new innovation divides are on the horizon.[17]

> The US and China as the major geopolitical players in the digital economy adopt markedly different approaches to data governance.

To simplify, the United States emphasizes data control through the private sector, while China's model prioritizes government control over data. In contrast, the European Union advocates for individual control of data based on fundamental rights and values, and more recently with the Data Governance Act and European data spaces, the EU has also promoted the utilization of data as public good. This context has resulted in significant tensions, especially between the US and China, but also between EU and the US, highlighting the divergent strategies employed by these key players in the governance of data flows and the broader digital economy.[18]

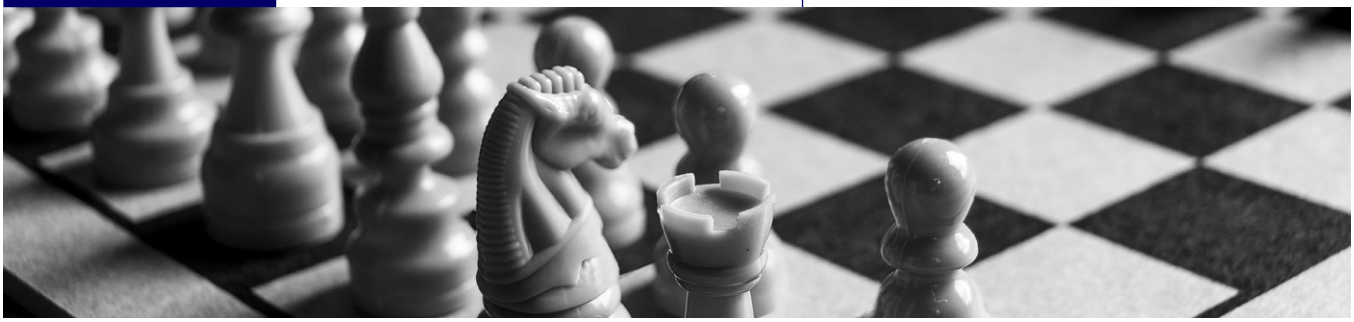
This evolving context prompts a critical question: Are Europe and the Global South caught in a geopolitical crossfire between the United States and China, left with the challenging choice of adopting one of two competing models in the international digital race? Alternatively, can they forge a distinct form of data governance and digital sovereignty, a "Third Way," as proclaimed by the EU?[19]

Given the immense market power held by major digital platforms, another important question arises:

- Who actually sets the rules, and who is expected to abide by them?
- Are these large digital platforms rule-makers or rule-takers?
- Do they exert more influence than states over digital business models, market value chains, and individual and collective behavior?

Table 1: Digital Governance Regimes: US vs China (key aspects)

	UNITED STATES	CHINA
Regulatory Approach	Minimal regulation: Hands-off approach with minimal government interference to foster tech industry growth.	State-controlled regulation: The government exerts strong regulatory oversight, ensuring alignment with national priorities.
Innovation Focus	Strong emphasis on maintaining technological leadership by prioritizing innovation over regulation.	Technology is used as a tool for economic growth, but state oversight ensures compliance with government goals.
Market Dynamics	Relies on market forces to address imbalances, avoiding heavy regulations unless necessary.	Government intervention plays a key role in market control, ensuring tech firms align with state policies.
Economic Development	Market-driven approach to economic growth, with tech companies leading innovation and expansion.	Government-driven technology sector supports national economic strategies and growth plans.
Social Control	Limited direct government control over digital platforms, but rising concerns over misinformation and platform accountability.	Technology is a means for social and political control, reinforcing digital authoritarianism through surveillance.
Data Governance	Decentralized data governance, with private firms playing a key role; regulations like GDPR are largely absent.	Mass collection and centralized state control of citizen data to ensure security and stability.
Global Influence	Focus on global tech dominance through private firms like Google, Apple, and Microsoft, rather than state-led initiatives.	China promotes its digital governance model globally through initiatives like the Digital Silk Road, exporting its approach to partner countries.

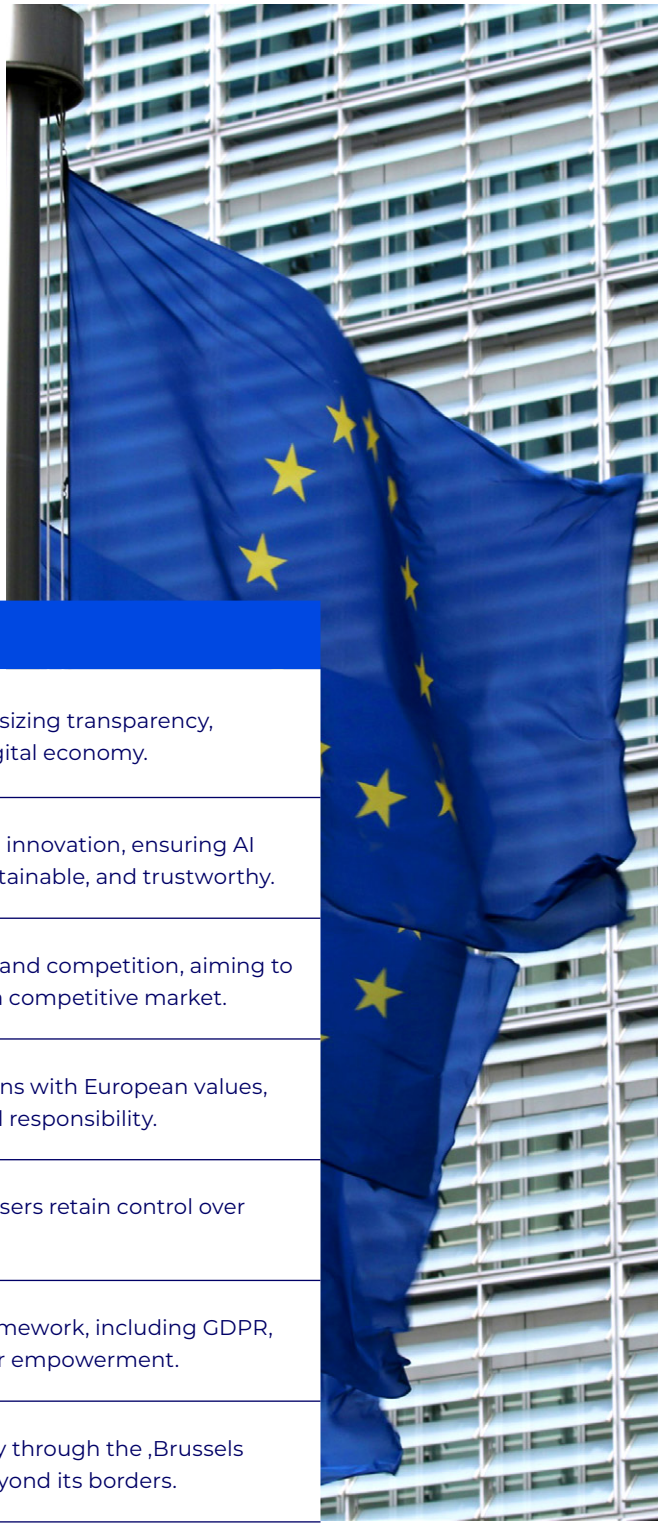


THE EUROPEAN UNION'S DIGITAL GOVERNANCE FRAMEWORK

03

03. THE EUROPEAN UNION'S DIGITAL GOVERNANCE FRAMEWORK

The European Union's digital governance regime offers a structured approach to addressing the overpowering influence of large tech companies and stands as a corrective to the perceived regulatory shortcomings of the United States and the excesses of China's authoritarian model.



The EU's framework is characterized by its emphasis on promoting public interest, balancing corporate power, and safeguarding democratic values.

Table 2: The EU's digital governance framework

EUROPEAN UNION	
Regulatory Approach	Strong regulatory framework emphasizing transparency, fairness, and accountability in the digital economy.
Innovation Focus	Prioritizes ethical and human-centric innovation, ensuring AI and digital technologies are safe, sustainable, and trustworthy.
Market Dynamics	Seeks a balance between regulation and competition, aiming to prevent monopolies while fostering a competitive market.
Economic Development	Promotes a digital economy that aligns with European values, emphasizing sustainability and social responsibility.
Social Control	Emphasizes digital rights, ensuring users retain control over their data and digital interactions.
Data Governance	Comprehensive data governance framework, including GDPR, to enhance privacy, security, and user empowerment.
Global Influence	Exports regulatory standards globally through the ‚Brussels Effect,' influencing digital policies beyond its borders.

3.1. KEY REGULATORY INITIATIVES OF THE EU

The European Union has sought to position itself as an aspiring regulatory superpower, aiming to establish a distinct third path that sets it apart from the models of the United States and China.[20] In this context, the EU seeks to serve as a reference model for other nations. By leveraging its market size and regulatory influence, it has established globally impactful standards. It introduces a unique framework of digital governance that emphasizes human rights, privacy, consumer protection, and fair competition.

In recent years, the European Union has rolled out several comprehensive legislative frameworks to address various aspects of digital governance, reflecting its commitment to creating a fair, secure, and innovative digital environment.[21]

Key regulations include:
The General Data Protection Regulation (GDPR), introduced in 2018, enforces strict data protection rules in the EU, requiring transparency, user consent, and accountability, with heavy fines for non-compliance. The Digital Markets Act (DMA) promotes fair competition by curbing anti-competitive practices of major platforms, while the Digital Services Act (DSA) enhances transparency and user safety, focusing on very large online platforms and search engines. The Data Governance Act (DGA) and Data Act aim to unlock the EU's data economy by facilitating secure and voluntary data sharing, fostering innovation, and ensuring data sovereignty. Lastly, the AI Act establishes ethical and safety standards for AI, categorizing risks and imposing regulations on high-risk systems to balance innovation with citizen protection.

Together, these regulations form a robust framework for digital governance, positioning the EU as a leader in setting global standards for data protection, market fairness, and technological innovation.

> The EU's approach strives to balance the benefits of digital advancement with the protection of citizens' rights and competitive markets.

The digital regulatory acts aim at establishing a level playing field to foster innovation, growth, and competitiveness, both in the European Single Market and globally.

European governments face the dual burden of fostering tech industry growth while safeguarding citizens' fundamental rights versus national security imperatives and foreign control. In its "Path to the Digital Decade" strategy, the EU has set ambitious targets for its digital transformation by 2030: The "Digital Compass" outlines the vision and targets for EU digitalization, while the policy program establishes the governance framework to achieve these objectives.[22] By implementing this multifaceted approach, the EU aims to balance innovation, economic growth, and the protection of citizens' rights in the digital age. However, it is important to note that this balancing act may be coming to an end, with some suggesting that the EU may begin to imitate other models, particularly that of the United States.

3.2. THE "BRUSSELS EFFECT": CONCEPT AND IMPLICATIONS

The "Brussels Effect," as articulated by Anu Bradford, describes how the EU's regulatory measures have extraterritorial impact.

It encapsulates **two key processes:**

First, the EU's high regulatory standards are often applied globally by digital platforms because it is impractical for them to customize their systems for different countries.

Second, these EU regulations serve as a reference model for the legislation of third countries. The Brussels Effect represents a form of unilateral regulatory globalization where the EU externally emulates its laws through market mechanisms. As a result, companies tend to comply with EU standards, even outside the EU, due to several factors: the EU's large market size, regulatory capacity, and the tendency of its stringent regulations to become global benchmarks. Bradford outlines five reasons for this regulatory authority: The EU's market size enables it to exert influence over foreign entities; its substantial regulatory capabilities allow for effective regulation enforcement; EU regulations can unlock access to all markets; their relevance in global consumer market regulation; and the promotion of uniform production standards among multinational corporations to minimize regulatory costs. This leads to what Bradford terms the "de facto Brussels Effect," where companies choose to apply high EU standards worldwide. She also describes the "de jure Brussels Effect," where export-oriented firms lobby for global standards to create a level playing field against domestic competitors.[23]

The GDPR,[24] in particular, causes extraterritorial effects that extend beyond the EU's jurisdiction. First, under the principle of market location enshrined in the GDPR, providers of digital products and services to the EU must comply with EU data protection regulations, regardless of their company's location. Second, EU privacy principles are embedded in international trade agreements with third countries, thus promoting global standards.[25]

> For global digital behemoths, leaving the lucrative European market is not feasible. Organizing business around many separate legal frameworks would be burdensome, and the mobility of data requires de facto transnational harmonization.

Bradford argues that it is more efficient for these companies to implement stringent European regulations globally than to align with various national laws, thus fragmenting their service's architecture and design. Consequently, these digital service providers tend to offer consumers in other jurisdictions the same level of protection as they do for Europeans. This situation results in the EU effectively extending its data protection laws beyond its borders, compelling foreign market players to adhere to EU rules, regardless of whether they serve EU, US, or other countries' customers.

3.3. THE EU'S APPROACH FOR RIGHTS-BASED AND HUMAN-CENTERED DIGITAL GOVERNANCE

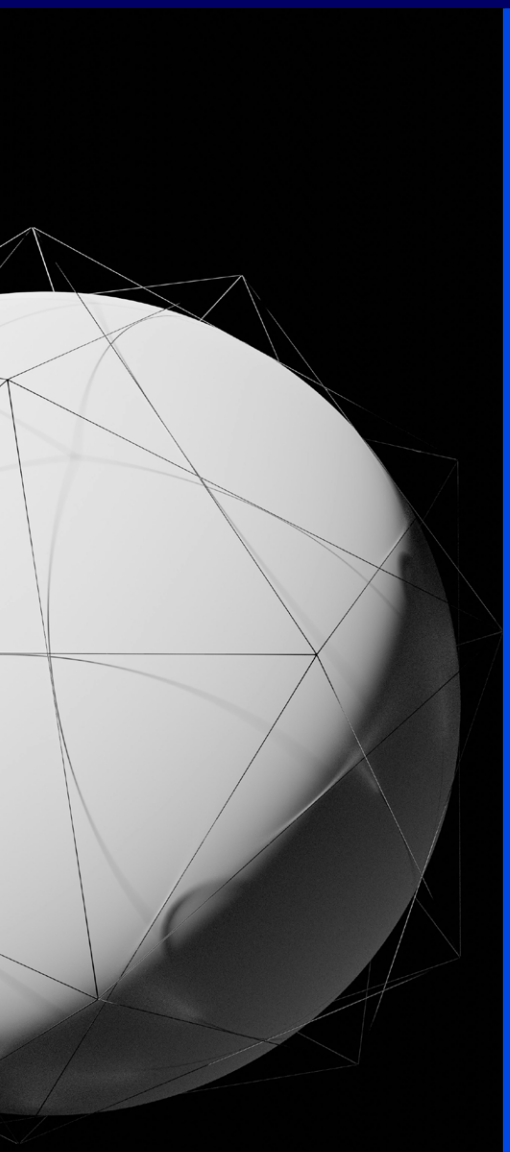
The EU's digital governance framework prioritizes principles that align with human rights and democratic values. It is based on a social contract that enshrines fundamental rights, democracy, solidarity, fairness and redistribution, and the impetus to create a digital single market.[26]

The opportunities of the EU's approach lie in its public interest orientation and maintaining democratic societal structures. But the EU's approach also encounters significant challenges. Most pronounced are innovation concerns: Critics argue that the stringent nature of EU regulations might stifle innovation, pointing to the relative scarcity of leading tech firms originating in the EU as potential evidence. The recent Draghi Report points to under-investment, private and public, in digital technologies (see below). However, Bradford suggests that issues like a fragmented digital market and underdeveloped capital resources may bear more responsibility for this innovation gap than regulation itself.[27]

A major challenge lies in effectively enforcing regulations.[28] Instances such as the protracted enforcement of the GDPR, which has left some data protections wanting, signal potential weaknesses in actualizing regulatory goals.[29]

It took until 2022/2023 for the Irish Data Protection Authority to impose substantial fines on platforms that registered their European headquarters in Ireland. To date, the highest fine was EUR 1.2 billion against Meta Platforms Ireland for insufficient legal basis for data processing. The Irish DPA also imposed another fine of EUR 345 million on TikTok. Luxembourg sanctioned Amazon Europe with another fine of EUR 746 million for insufficient legal basis for data processing. [30]

The success of newer regulations like the Digital Services Act (DSA), the Digital Markets Act (DMA) and the AI Act will heavily depend on the EU's ability to effectively and coherently implement and enforce these regulations. This requires both vertical and horizontal policy-coordination between the European Commission and the national member states, as well as cross-sectoral policy coordination (see below).



THE ROLE OF THE GLOBAL SOUTH IN DIGITAL GOVERNANCE DYNAMICS

04

04. THE ROLE OF THE GLOBAL SOUTH IN DIGITAL GOVERNANCE DYNAMICS

The Global South, particularly rising powers such as Brazil, India, Mexico, and South Africa, is playing an increasingly significant role in shaping the dynamics of digital governance. BRICS, the informal coalition of states founded in 2006, which has included South Africa since 2010 alongside Brazil, Russia, India, and China, has now expanded to include ten nations ("BRICSplus"), including Indonesia in January 2025, with forty additional countries expressing interest in membership.[31] Some states, particularly Russia and China, are attempting to shape BRICS into a bloc that politically and economically challenges "the West." Other nations, such as India and Brazil, view BRICS as part of their multi-alignment strategy, aiming to assert their national interests through participation in BRICS as well as in other alliances, such as the G20 and OECD.

The BRICS countries can be seen as embodying a desire for an alternative global order, and some scholars position it as a new Non-Alignment Movement[32], representing the "rise of the rest".[33] However, the heterogeneity of the BRICS is often overlooked. They differ fundamentally in terms of their political systems, their attitudes toward the enforcement of human rights, their economic and geopolitical interests and resources, and their assessments of international conflicts. What unites them is their explicit criticism of the international order shaped and dominated by the "West" and their emphasis on the principles of national sovereignty, territorial integrity, and non-interference. The fact that its founding member Russia is flagrantly violating these principles with its aggression against Ukraine may cause discomfort behind closed doors, but shared economic and geopolitical interests take precedence.

The question for Europe is how to deal with BRICS as an increasingly important actor. The answer will depend on whether the BRICS coalition is perceived primarily as a China-dominated challenger or whether its heterogeneity is seen as an opportunity to build bridges with those countries in the Global South that criticize Western hegemony but also see little to gain from a Chinese or Russian-dominated international order.

Engaging with these countries on an equal footing, without compromising one's own values and interests, would be an important step toward enhanced multilateral cooperation.

4.1. IMPACT OF THE BRUSSELS EFFECT ON DATA PROTECTION

The EU's regulatory power in digital foreign policy, derived from its economic power and lucrative consumer market, has led US digital technology companies to adjust their terms of service to secure access to the European internal market.[34] This has indirectly influenced digital governance in Global South countries, as at least some of the platform's design choices have been rolled out internationally. As for digital trade, the OECD is fostering cross-border data flows with trust.[35] However, agreements like the Regional Comprehensive Economic Partnership (RCEP) in ASEAN countries and efforts to implement data localization policies show that Global South countries are seeking to maintain control over data flows, potentially diverging from EU standards.[36]

> Data Protection is the major showcase for the Brussels effect. The GDPR has inspired similar legislation in many countries and is widely recognized as the international gold standard for data protection.

In fact, GDPR represents a global success story, with to date 160 countries having enacted data protection laws and over 94 nations having established data protection authorities. To date, approximately 82% of the world's population resides in jurisdictions with comprehensive data protection regulations.[37] In all four countries considered, privacy is recognized as a fundamental right for citizens. However, data protection's practical application in these countries faces considerable challenges.[38]

Mexico

Mexico has two data protection laws: one for the private sector, established in 2010, and another, for the public sector. The **2010 Federal Law for the Protection of Personal Information in Possession of Individuals** (Ley Federal de Protección de Datos Personales en Posesión de Particulares, or "LFPDPPP") applies to the private sector. In 2017, **the General Law on the Protection of Data in the Possession of Obligated Subjects** (Ley General de Protección de Datos en Posesión de Sujetos Obligados) was enacted for the public sector and is modeled after the GDPR. This bifurcation creates a certain degree of inconsistency. Moreover, in 2018, Mexico signed **Convention 108 of the Council of Europe on data protection**, marking a significant step towards harmonizing international data exchange.

The **National Institute for Transparency, Access to Information, and Personal Data Protection** (INAI—(Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales) employs around 100 staff members strongly dedicated to implementing data protection laws. Since 2014, INAI has functioned as an autonomous authority. However, this autonomy has been contested, and the very existence of INAI as autonomous constitutional body is currently dissolved, after a constitutional amendment enacted by a Presidential Decree.[39]

Challenges for the enforcement of data protection in Mexico are a weak culture of data protection and significant violations. The United States-Mexico-Canada Agreement (USMCA/T-MEC 2020) includes a data protection clause but also prohibits national data localization, allowing companies to easily sidestep Mexican regulations by relocating their servers to the US. Consequently, forum shopping has become a common practice. Other challenges include a lack of awareness regarding the legal implications of data processing, low sensitivity to information misuse, and widespread ignorance among citizens about their personal rights.[40] When INAI imposes penalties, companies typically contest them through administrative channels, which can be lengthy and involve multiple levels of appeal.[41] NGOs criticize the INAI for being insufficiently proactive and for low enforcement actions.

Brazil

Brazil has been a pioneer in digital rights regulation. In 2014, Brazil introduced the **Marco Civil da Internet,** a foundational law that codified essential digital rights, including net neutrality. The 2018 **Brazilian General Data Protection Law** (LGPD—Lei Geral de Proteção de Dados) entered completely into force in 2020 and broadly aligns with the GDPR.[42] Brazil's **National Data Protection Authority** (ANPD-Autoridade Nacional de Proteção de Dados) established in November 2020, gained formal administrative and decision-making autonomy in October 2022.[43] Despite its growth from 50 staff members in 2021 to 141 employees in 2024, the agency still faces resource constraints.[44] Though receiving thousands of complaints regarding data breaches, the ANPD has been slow in imposing any sanctions.[45] Until autumn of 2024, ANPD has issued seven sanctioning decisions, primarily targeting the public sector and data security incident management.

Challenges in compliance and cooperation with the ANPD have been observed in both the public and private sectors. Nevertheless, data protection is getting a more significant concern for companies as it is affecting their reputation. The ANPD's few but stringent actions also highlight the necessity for organizations to improve their compliance practices and internal processes to ensure effective data protection. Under the new administration of President Luiz Inácio Lula da Silva (since 2023), there is potential for the ANPD to become more assertive and credible, especially as it navigates pressure to meet OECD requirements, of which Brazil aspires to be a member.[46]

Another actor is Brazil's Supreme Court. On 30 August 2024, Judge Alexandre de Moraes ordered the suspension of X (formerly Twitter) because it had failed to adequately address the spread of hate speech and had violated regulations requiring a legal representative in the country. Elon Musk ultimately complied, paid a fine, named a representative, and the ban was lifted on October 9, 2024.[47]

In July 2024, ANPD ordered Meta to stop processing personal data to train AI, including personal data from non-users. In November 2024, the Brazilian government started to investigate TikTok for its handling of children's data. In this context, the ANPD is assessing whether the platform collects and processes data from children and adolescents improperly and has banned the use of the app without age registration.[48] Also in November 2024, ANPD launched a public consultation process to help shape the country's AI regulations, particularly focusing on automated decision-making systems and data protection.[49] A company co-founded by Sam Altman, CEO of OpenAI, has registered the iris data of 400,000 Brazilians in exchange for cryptocurrencies, but in January 2025, ANPD ordered Tools for Humanity (TFH) to stop this practice, citing risks to users' consent and violations of data protection laws. The company argues that its biometric data collection enhances digital security and adheres to privacy standards, but the ANPD finds the practice particularly concerning due to the irreversibility of gathered data and the vulnerability of participants.[50]

India

India's long journey towards data protection legislation took off in 2017 when the Supreme Court of India recognized the **right to privacy as a constitutional protected fundamental right** ("Puttaswamy Judgment)". After four draft legislative texts and several revisions, both houses of India's Parliament finally passed the **Digital Personal Data Protection Act (DPDP)** in 2023.[51] However, to date, India's data protection law is still not in force, as the Rules to be issued by the government have only been published as draft Rules on January 3, 2025. Moreover, a data protection board needs to be assigned by the government, as well as mechanisms for audit, and rules for cross-border data transfers.

The final version of the DPDP bill omitted a data localization requirement—a provision that India had long championed on the international stage —and instead introduces notification of a list of "trusted geographies" to which data of Indian citizens may be transferred, potentially creating a blacklist for data transfers. In the new draft rules, Rule 12(4) suggests that significant data fiduciaries may have to localize certain categories of personal data, thus bringing data localization back into consideration.

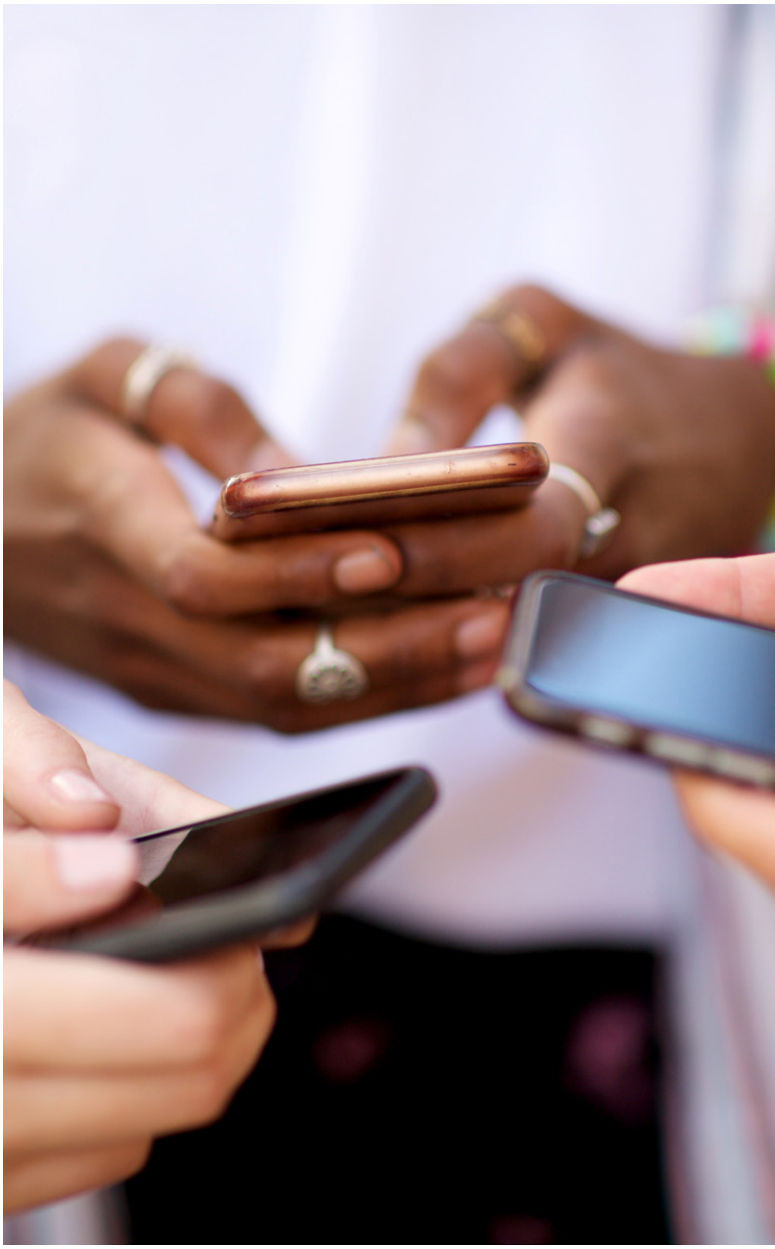
Furthermore, the DPDP includes extensive exemptions permitting government access to personal data under broad grounds related to "the interests of sovereignty and integrity of India, the security of the state, friendly relations with foreign states, [or] the maintenance of public order".[52] Ultimately, as academics and civil society organizations have criticized, the law seems to provide the government with enhanced powers rather than empowering individuals with greater autonomy. Due to several aspects mentioned, India's data protection framework may substantially struggle to meet the EU's adequacy standards for cross-border data transfers.

South Africa

The evolution of data protection in South Africa is emblematic of a broader global trend towards privacy legislation in Africa. Since 2001, 35 African countries have enacted data protection laws. Region-wide agreements, such as the **African Union Convention on Cybersecurity and Personal Data Protection** (Malabo Convention) highlight the acknowledgment of comprehensive data protection laws, but not all member countries have ratified the convention.[53]

South Africa's **Protection of Personal Information Act (POPIA)** enacted in 2013 was fully implemented in 2020, and the subsequent enforcement measures launched in 2021. POPIA contains many elements similar to the GDPR. Central to POPIA's enforcement is the **Information Regulator,** South Africa's data protection authority. It is an independent statutory body responsible for promoting compliance with the act. In its initial operational phase, the 2022/2023 financial year, it received 895 complaints relating to alleged violation of POPIA. Of these, 616 (68.8%) have been resolved.[54] This remarkable rate of resolution highlights the Regulator's commitment, particularly in addressing issues within governmental agencies, as some high-profile cases demonstrate. In 2023, the Information Regulator issued its first fines under POPIA, signaling accountability. The fines, notably imposed on governmental departments such as the Ministries of Justice, Education, and the police, reflect the serious lapses in data security and the handling of personal information.[55] In 2024, the Information Regulator issued further enforcement notices, among others to the Electoral Commission.

The Information Regulator has made significant progress. It is composed of dedicated professionals and is currently on a sound path toward establishing a robust framework for data protection. Operating as an independent authority under the law, the Regulator has demonstrated its capacity to "show teeth" also in confronting violations against entities with significant power in the data economy like Meta.[56] Despite these positive developments, several challenges persist. The Information Regulator faces constraints in terms of personnel and funding. With a budget of approximately 100 million ZAR and a staffing level of only 90 employees, it struggles to extend its reach across the country. Moreover, there is an urgent need to address widespread security breaches and improve compliance levels. Additionally, a low culture of privacy awareness among citizens and organizations presents an ongoing hurdle to enforcing compliance and responsibility. The investigation of social media platforms, while underway, remains in its infancy. The enforcement threshold of 10 million ZAR for penalties is insufficient to deter large tech companies.



Key observations

In summary, while the Brussels Effect has significantly influenced data protection legislation in these four countries, its implementation varies due to the limited enforcement capabilities of local authorities, which are often constrained by financial and organizational challenges, as well as competing political priorities.

Mexico's government has yet to prioritize a digital strategy, while Brazil faces uncertainty as it recently focuses on BRICS. India's Digital Public Infrastructures (DPIs), initially developed in the financial sector, are also being adopted in Brazil's Pix system. Aligning somewhat with China's model, India's ambitious techno-nationalist agenda, despite its rivalry with China, seeks to establish a unique path prioritizing state control over technology, exemplified by its TikTok ban.

India is actively positioning itself as a leader in digital governance by proposing a "Fourth Way" presented during its G20 presidency in 2023, aiming to promote DPIs as a transformative model and emphasizing digital infrastructure as a public good. [57] In collaborating with the UNDP and the UN's adoption of the Global Digital Compact in 2024, India aims at leadership in a multipolar global constellation.[58] DPIs are gaining traction internationally and synergies arise with the EU's Data Governance and Data Act.[59] Conversely, South Africa emphasizes enforcing existing regulations to combat corruption and enhance government's accountability. The Information Regulator has begun sanctioning government agencies to foster compliance. While South African authorities acknowledge the value of EU regulations, they prefer adapting these principles to their socio-political context instead of implementing a one-size-fits-all model. This divergence underscores different priorities: India seeks to innovate and establish a global digital framework that promotes equity and access, while South Africa focuses on enforcing data protection laws amidst historical distrust and socio-economic challenges.

The geopolitical landscape, influenced by Russia's invasion of Ukraine and conflicts in the Middle East, has distanced Global South countries from the West, aligning them closer to China and Russia within BRICSplus. This shift may also affect the digital arena.

If the Brussels Effect is viewed as unilateral, skepticism arises; countries prefer flexible adaptations to EU regulations to fit their contexts, emphasizing collaborative partnerships at eye level and mutual dialogue.

Lastly, further research is needed to explore claims that Big Tech platforms align their designs with high EU standards globally. Preliminary anecdotal evidence indicates that these platforms may exploit legal ambiguities in individual countries, leading to fragmented operations in response to varied regulatory environments.

4.2. FURTHER CHALLENGES IN IMPLEMENTING EU-STYLE REGULATIONS

Global South countries encounter several challenges in adopting EU-style digital governance regulations, including significant economic disparities, a pronounced digital divide in connectivity and internet access, and low digital literacy. The disparity in digital development and available resources makes it difficult to implement similar regulatory frameworks. Establishing sophisticated digital governance requires considerable technical expertise, strong institutions, and regulatory capacity, which are often limited. Political will and governance structures vary widely, complicating the uniform adoption of standards. Additionally, there is a growing emphasis on digital sovereignty, with countries like Brazil and India aiming to create their own digital governance strategies.[60] South Africa, like many others, relies on China for affordable hardware and the US for software applications, often struggling to balance the pursuit of rapid digital innovation and economic growth with the need for robust regulation.

On a broader scale, both Europe and the Global South face similar challenges, such as rising geopolitical tensions and dependencies on foreign tech giants, underscoring the need for greater digital sovereignty. Europe should engage in genuine dialogue with Global South countries, which tend to be more tech-optimistic and aspire for digital leapfrogging and recognition as global powers.

Discussing European lessons from state surveillance can foster mutual understanding. Europe must recognize that, for the Global South, priorities include addressing connectivity issues, bridging digital divides, and enhancing digital inclusivity and access, all aligned with the Sustainable Development Goals. The emphasis on collective rights, development, and global goods is stronger in these regions. Consequently, addressing different narratives, cultural contexts, and urgent concerns is essential for fostering mutual understanding.

In conclusion, while the Global South is becoming more assertive in shaping digital governance, it faces unique challenges and often seeks solutions tailored to its specific contexts. The EU's regulatory influence is present but not straightforward. Countries that maintain strong economic ties with the EU may be more inclined to adopt its regulations, while shared values on democracy and human rights play a role, as seen in younger democracies like Brazil and South Africa. The EU's support in capacity building and knowledge transfer could assist these nations in implementing effective digital governance.

GEOPOLITICAL RIVALRIES AND DIGITAL GOVERNANCE

05

05. GEOPOLITICAL RIVALRIES AND DIGITAL GOVERNANCE

5.1. ESCALATING TECHNOLOGICAL TENSIONS AT THE GLOBAL LEVEL

The landscape of global digital governance is shaped by geopolitical rivalries, particularly between the United States and China. Additionally, the rise of BRICS and the EU's efforts to assert its digital sovereignty add complexity to this dynamic. These evolving factors could be leveraged to develop alternative scenarios and solutions.

The intensifying technological tensions between the United States and China are reshaping global power structures and digital governance. This competition is characterized by:

01.
A shift from territorial control to digital dominance;

02.
The transcendence of geographical boundaries in geopolitical conflicts;

03.
The evolution from traditional political alliances to strategic technological partnerships;

04.
Competition over setting international standards.[61]

The escalating technological tensions between the US and China are creating a new paradigm of techno-economic competition that extends beyond these two nations. The rivalry has led to a bifurcation of digital ecosystems, increasing the costs of doing business and global communication and has particularly affected countries in the Global South. It is also driving a wedge in the global digital landscape, potentially leading to distinct US-led and China-led ecosystems and techno-spheres. Three key examples illustrate this shift:

- **First**, the semiconductor war, marked by export controls and heavy investments in domestic chip production by both nations, is fragmenting global supply chains and compelling other countries to choose sides.[62]
- **Second**, the battle for dominance in artificial intelligence has led to increased restrictions on technology transfers, exemplified by the US Executive Order limiting American investment in China's AI sector.[63]
- **Third**, the competition to set international standards for emerging technologies, such as 5G, AI and the Internet of Things, is intensifying, with both powers seeking to impose their values and interests on the digital domain.

This technological divide is reshaping economic relationships and challenging global digital governance, potentially resulting in a more fragmented and less interoperable digital future. However, the growth of BRICS indicates that multiple players are emerging in this multipolar world.

5.2 EU STRATEGIES FOR NAVIGATING GEOPOLITICAL RIVALRIES AND DIGITAL COMPETITIVENESS

> The Draghi report on EU competitiveness identifies pressing challenges in Europe's digital landscape and offers key recommendations that, interestingly, contradict the EU's perception as a global leader in digital regulation.

Despite rightfully acknowledging an innovation gap compared to the US and China, marked by deficiencies in AI, cloud computing, and venture capital, the report suggests simplifying regulations—particularly around GDPR and competition policies. While the intent is to lower compliance burdens and catalyze the emergence of new European digital champions, lowering these regulations could undermine trust and stability in the digital environment. Instead of fostering growth, diluting existing regulations risks reverting to a regulatory framework that may not adequately support a sustainable and competitive digital economy. To enhance Europe's digital capabilities, the report calls for increased investment, a focus on key sectors, and improved data sharing initiatives. Additionally, it emphasizes developing digital skills and streamlining enforcement of existing regulations.[64] Ultimately, while addressing these recommendations may improve competitiveness, the EU must reconcile them with its commitment to being a benchmark for global digital regulation, ensuring that any changes bolster a trustworthy and robust digital ecosystem for all stakeholders.[65]

As Europe develops its industrial policy on AI, significant public and private investments are being proposed, necessitating public scrutiny and critical discourse. Crucial questions regarding resource allocation and decision-making processes include the impact of large-scale AI on previous strategies for digital independence, Europe's dependence on dominant tech incumbents, and whether public investments in AI align with social and sustainability goals. Europe is lagging behind in AI development, and certain frontrunners appear unreachable.[66] Draghi advocates for a robust industrial policy and significant investments. Effective competition policies are essential to curtail the market and informational power of digital giants. However, a public-interest vision in the EU's AI strategy is needed, to prevent reinforcing existing power concentrations in the AI sector, and to align AI with climate objectives. Cautious AI integration in sensitive sectors, fostering innovation alongside regulatory enforcement, and ensuring that EU policies consider their global implications is called for.[67] Public procurement is another crucial strategy for promoting digital technologies that align with human values. In some sectors, it may be more beneficial to focus on foundational research rather than trying to compete with American and Chinese technology leaders. It is vital to impose conditions on AI tech companies and direct technological advancements towards societal objectives, such as equity and fairness.[68] AI should not be seen as an end in itself; numerous publications highlight the biases and discrimination issues associated with its use.[69]

Moreover, China's apparent success in reining in its tech companies raises significant stakes. If the EU does not demonstrate its ability to manage the tech industry effectively, it will likely lead to the conclusion that the governance of the digital economy is dominated either by authoritarian regimes (like in China) or by tech companies themselves (in the US and the EU), rather than by democratic governments.

RECOMMEN-DATIONS FOR THE EU

06

06. RECOMMENDATIONS FOR THE EU

The Draghi Report has triggered studies to envision alternative strategies and recommendations for reducing Europe's dependencies on foreign tech platforms and for building a more resilient, sovereign and inclusive European digital ecosystem.[70] While discussion of these proposals is very worthwhile, it is noteworthy that these focus on Europe inwards, and do not adequately account for Europe's outwards strategies to build alliances.

> Complementary to internal efforts to build European resilience and strengthen its competitiveness and thus digital sovereignty, the EU must also build strategic alliances.

The Commission's 2030 Digital Compass, approved in March 2020, acknowledged that the EU needs a "comprehensive and coordinated approach to digital coalition-building and diplomatic outreach".[71] The European Union must develop strategies to navigate these geopolitical rivalries and assert its position in global digital governance.

TO THIS PURPOSE, THESE RECOMMENDATIONS ARE CRUCIAL:

1. Foreign Policy: Strengthen the EU's digital diplomacy strategy to defend fundamental rights and values, enhance security, and foster digital markets abroad

To safeguard its interests, values, and global reputation, the EU should integrate its fundamental rights-based, open-market and human-centric technology approach into its alliances, partnerships, and multilateral organizations. In an era where technology is contested and weaponized, the greater the technological sovereignty of like-minded countries, the more secure the EU's own sovereignty and global standing becomes. Protecting allies from foreign influence, cyberattacks, and coercion stemming from technological vulnerabilities will enhance alignment and cooperation with the EU on the global stage. Consequently, the EU should focus not on achieving technological independence but on cultivating a mutually reinforcing and shared technological sovereignty with its allies.[72] The Council's Conclusions on EU Digital Diplomacy point to the right direction.[73]

In addition, digital leadership needs a face and a name. The European Council could designate an ambassador-at-large for digital affairs to lead a new team of digital attachés in EU delegations worldwide. This restructuring is vital for enhancing Europe's technology diplomacy and directing attention towards safe and resilient critical technologies. The ambassador would help partner countries in their digital transformation, spanning infrastructure financing to public digital infrastructures, adaptive AI application development, and supporting regulatory capacities. This proactive approach aims not only to extend the EU's regulatory influence but also to engage with local tech ecosystems, fostering mutually beneficial opportunities for citizens, business and innovation.[74]

2. Unify an International Digital Policy Strategy

While the European External Action Service (EEAS) has begun to focus on digital diplomacy, its effectiveness has been limited by insufficient resources, poor integration of member states' efforts, and internal conflicts within the Commission.

> To address this gap, the high representative should initiate the development of a comprehensive EU international digital policy strategy, aligned with the recent Council of the EU's call to clarify the principles and tools of its digital diplomacy.[75]

This strategy should unify diverse Commission portfolios—such as trade, internal market, and economic affairs—under the leadership of a new ambassador-at-large for digital. Additionally, European Parliament committees should enhance their roles in promoting EU digital norms and engaging in regulatory discussions with global partners, through foreign affairs, civil liberties, industry committees, and inter-parliamentary forums.[76]

Policymaking is also about narratives. Some scholars have argued that the EU needs another figure, a "storyteller in chief" to provide political leadership, secure resources, articulate core concerns, and foster dialogue. To achieve this, the EU should appoint a special representative or envoy for the digital future with strong digital credentials and diplomatic skills. This role could be established in one of two ways: Either as a representative under the EU foreign policy chief for access to the EU's diplomatic machinery, or as an envoy under the European Commission's executive vice president for tech sovereignty, security, and democracy, given the Commission's control over digital policies. The appointee should serve as a bridge builder, utilizing the EU delegations to identify key issues influencing partners' digital policies. This requires a shift from mere reporting to uncovering critical connections, necessitating new working methods, talent development in the EEAS, and strategic use of EU funding for international cooperation.[77]

3. Offer alternatives to Global South countries

The EU 's "Global Gateway" program aims at presenting an alternative to China's Digital Silk Road initiative. It aims at investing in infrastructure projects globally. Launched by the EU Commission, it plans to invest €300 billion between 2021 and 2027. Africa is the primary focus of the initiative, with half of the funds directed toward projects that promote green and digital transitions, sustainable economic growth, healthcare, and education on the continent. In 2023, ninety projects were launched, also in Asia-Pacific and LAC regions.[78] However, Global Gateway has faced strong criticism for being largely aspirational, and for relying heavily on existing programs.[79] While focusing on digital connectivity, equivalent investments in AI and semiconductors would be necessary. The Global Gateway initiative must also be linked more closely to the EU's digital policy and digital diplomacy objectives. Thus, it should incorporate a robust regulatory component in close collaboration with partner countries to support rules-based institutions.[80] Regulatory convergence could also be promoted, focusing on secure and ethical international data flows. Allocating funds to enhance cooperation in scientific research and the development of critical technologies and strengthening connections with civil society organizations will also foster mutual understanding and support.

4. Promote fundamental rights, values and European regulatory standards through effective enforcement

The EU can use the attractiveness and power of its internal market to shape global standards for data protection, competition in digital markets, and AI regulation according to universal human rights and values. The successful, yet complex international proliferation of the GDPR showed how EU democratic norms shape global standards on data protection and privacy issues. The Digital Services Act (DSA) and the Digital Markets Act (DMA), which "aim to create a safer digital space where the fundamental rights of users are protected and to establish a level playing field for businesses", as well as the EU's regulations on artificial intelligence and data governance, have the potential to yield similar global effects.[81] To facilitate compliance, the Commission can provide technical support and guidance to businesses, particularly SMEs, to help them comply with legislative requirements.

> However, to achieve global resonance, the EU must implement these digital regulations in a comprehensive and coherent manner.

This requires effective cross-coordination and cross-compliance between these legislative frameworks. New EU agencies like the AI Office must be staffed with sufficient resources and competent workforce to implement the AI Act effectively. As the European Commission is the sole enforcer of the DMA, the joint team in DG COMP and DG CONNECT must efficiently implement the DMA, in cooperation with stakeholders and civil society. For not only the DSA and DMA, but all these new legislative frameworks, it is essential that coherent horizontal cooperation between the Directorates and vertical cooperation with the EU's member states takes place. Coordination with the EDPS and national data protection authorities is also pivotal to safeguard the fundamental rights-based standards and principles. Antitrust and data protection policy must be more closely tied.[82] Only strong institutions and relatively autonomous regulatory agencies with sufficient capacities to effectively enforce the legislation will be able to succeed in achieving the goals of protecting fundamental rights and establishing a more diverse and sustainable digital ecosystem.

5. Building alliances with like-minded countries in the Global North and in the Global South

Europe is not alone in its regulatory efforts to counter the powers of global tech giants. Several countries are implementing or considering measures to address the growing influence of large tech platforms. Just to give some examples: Australia's News Media Bargaining Code (2021) and News Bargaining Incentive (2025) require Meta and Google to pay Australian outlets for news content shared on their platforms, addressing issues of AdTech models and fair compensation. Canada, Indonesia, South Africa and many other countries are also planning to implement similar rules.[83] South Africa's and India's Competition Authorities are investigating anti-competitive behavior of large platforms. Several governments including Brazil, India, and South Korea are considering implementing a framework of ex-ante rules to regulate online platforms, inspired by the EU's Digital Markets Act.[84] The UK is introducing the Digital Markets Competition and Consumers Act (DMCCA) and Online Safety Regulations. Japan has also taken similar steps in its 2021 Act on Improving Transparency and Fairness of Digital Platforms. The Act aims to promote fair competition and protect smaller businesses that rely on these platforms. Australia has banned use of social media for children under 16 years.[85] The EU and other countries are introducing digital workers' rights and consumer protection standards.

These examples demonstrate that European regulations are part and parcel of a broader worldwide move towards taming digital gatekeepers and setting new rules and standards for a better, more sustainable digital economy. The EU should act as an alliance-builder with like-minded countries and foster mutual exchange about best practices and assessment of regulatory experiences. In this context, the EU should expand its digital alliances with like-minded countries to counter US dominance and Chinese and Russian influence. The EU has already formed partnerships with Japan, South Korea, Singapore, and Canada to foster a safe and inclusive digital space and create global standards.[86] These partnerships should be intensified and extended to more countries to strengthen collective efforts and enhance global impact.

6. Enhance multilateral cooperation and develop with the Global South an alternative path to digital development:

A new approach to coalition building would involve forming diverse partnerships based on shared support for specific policy frameworks, such as the human-centric digital transition, which is fundamental to the EU's international engagement. To maximize global impact, the EU must forge extensive dialogue and coalitions with both state and non-state actors. The idea of digital public infrastructures, originating in India, has been taken up by many stakeholders. It holds potential to be developed further in the direction of public digital infrastructures in different sectors such as media, finance, traffic, health and education. Hand in hand with other initiatives, a new digital economy could be stimulated, based on innovation in the public interest and safe and accountable governance structures.[87] The EU-Latin America and Caribbean Digital Alliance, launched in March 2023[88], exemplifies a strategic framework for fostering bi-regional cooperation, similar initiatives should be developed to enhance collaboration with the African Union and ASEAN.

More inclusive and globally aware digital policies, achieved through proper consultations and peer-review mechanisms, would mark a significant shift toward greater openness in EU policymaking.[89] By investing in its narrative and regulatory power and building effective coalitions, the EU can strengthen multilateralism and shape global governance in the digital domain. Proactive advocacy for democratic values and human rights in international digital policy arenas will be necessary to both counter digital authoritarianism and digital libertarianism.

07. CONCLUSION

As the global digital landscape evolves amid growing geopolitical complexities, the European Union finds itself at a pivotal crossroads. By harnessing its market power alongside its steadfast commitment to democratic principles, the EU has the unique opportunity to spearhead a "Third Way" of digital governance—one that stands distinct from the libertarian approach of the United States and the authoritarian model of China. This approach aims to balance market dynamism with robust regulatory frameworks that protect fundamental rights and promote fairness. Reaffirming the EU's leadership potential in this arena involves not only the coherent enforcement of its existing regulations but also the strategic crafting of new policies that reflect the EU's core values, which are constitutionally protected. These include privacy, transparency, freedom, equity, solidarity, accountability, the protection of individual rights, and social cohesion. The EU must double down on these values to solidify its role as a regulatory superpower capable of setting global standards.

Central to this effort is the importance of collaboration for a sustainable digital future. By forming strategic alliances with like-minded nations in both the Global North and South, the EU can forge a united coalition in advocating for fair and ethical digital governance practices. Such collaboration is critical for amplifying the EU's influence on the world stage and ensuring that its regulatory models gain traction globally. Moreover, by actively engaging in and nurturing dialogues with the Global South, the EU can promote inclusivity and alignment with the Sustainable Development Goals. This collaborative approach must also extend to fostering multilateral partnerships that encourage sustainable innovation, competitiveness, and industrial cooperation.

> By leveraging private-public partnerships and multi-stakeholder networks, the EU can stimulate advancements in research, education, and sustainable digital products and services. In this respect, the EU will not only be a referee but a player too.[90]

Ultimately, the EU's ambitious embrace of a "Third Way" will enable it to shape a digital future that prioritizes fairness, innovation, and human rights. This vision not only positions the EU as a beacon of ethical governance but also empowers it to redefine global narratives, offering a sustainable and just digital landscape that resonates with the diverse needs and aspirations of a connected world. By embedding these principles into the heart of its digital strategy, the EU sets a powerful example, championing a balanced path forward in an increasingly digital age.

ENDNOTES

1 Jia, K., Chen, S. Global digital governance: paradigm shift and an analytical framework. *GPPG 2*, 283–305 (2022). https://doi.org/10.1007/s43508-022-00047-w

2 Mazzucato, Mariana (2013). The Entrepreneurial State: Debunking Public vs. Private Myths in Risk and Innovation (PDF). London: Anthem Press.

3 Bradford, Anu 2023: Digital Empires. Oxford University Press; Barbrook, R., & Cameron, A. (1996): The Californian ideology. *Science as Culture,* 6(1), 44–72.

4 Bradford, Anu 2023: Digital Empires.

5 Massarotto, Giovanna/ Yoo, Christopher S. 2024: Antitrust at a Crossroads. The Challenge of Digital Platforms, Journal of Law & Innovation (JLI), Vol. 7, pp. 1-9: DOI: 10.58112/jli.7-1.1;
Biden, Joseph 2023: Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, 30.10.2023, 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

6 JD Vance rails against 'excessive' AI regulation in a rebuke to Europe at the Paris AI summit, 11.02.2025, https://apnews.com/article/paris-ai-summit-vance-1d7826affdcdb76c580c0558af8d68d2

7 https://openai.com/index/announcing-the-stargate-project

8 https://www.economist.com/leaders/2025/01/23/chinese-ai-is-catching-up-posing-a-dilemma-for-donald-trump

9 Arcesati, Rebecca 2022: China's rise in digital governance, MERICS, https://merics.org/sites/default/files/2022-03/MERICS-Primer-Digital-Governance-2021_final.pdf

10 Made in China 2025, https://merics.org/en/report/made-china-2025

11 Bradford 2023: Digital Empires; Kostka, Genia 2023: Digital governance in China, in: Ergenc, C., & Goodman, D. S. (Eds.). (2023). *Handbook on Local Governance in China*. Cheltenham, UK: Edward Elgar, 178–207.

12 Chin, Josh/Lin, Liza 2022: Surveillance State. Inside China's Quest to Launch a New Era of Social Control. Macmillan.

13 Bradford 2023, 94ff.

14 Cheney, Clayton 2019: China's Digital Silk Road: Strategic Technological Competition and Exporting Political Illiberalism, in: Council on Foreign Relations, 26.09.2019, https://www.cfr.org/blog/chinas-digital-silk-road-strategic-technological-competition-and-exporting-political; Kurlantzick, Joshua et al. 2020: Assessing China's Digital Silk Road Initiative, https://www.cfr.org/china-digital-silk-road ; China's Digital Colonialism: Espionage and Repression Along the Digital Silk Road, in: Recorded Future, 27.07.2021, https://go.recordedfuture.com/hubfs/reports/cta-2021-0727.pdf

15 Miller, Chris. Chip War: The Fight for the World's Most Critical Technology. Simon & Schuster, 2022.

16 UNCTAD—United Nations Conference on Trade and Development (2021): Digital Economy Report 2021. New York, https://unctad.org/page/digital-economy-report-2021

17 UNCTAD 2024: Digital Economy Report 2024, Shaping an environmentally sustainable and inclusive digital future, UNCTAD/DER/2024

18 UNCTAD 2021: Digital Economy Report 2021, Cross-border data flows and development: For whom the data flow, UNCTAD/DER/2021.

19 Schneider, Ingrid (2020): Democratic Governance of Digital Platforms and Artificial Intelligence? Exploring Governance Models of China, the US, the EU and Mexico. In: JeDEM—EJournal of EDemocracy and Open Government, 12(1), S. 1–24; https://doi.org/10.29379/jedem.v12i1.604; European Commission: A European Strategy for data, https://digital-strategy.ec.europa.eu/en/policies/strategy-data; de Bastion, Geraldine/Mukku, Sreekanth (2020): Data and the Global South: Key Issues for Inclusive Digital Development. HBS-Study. Washington; 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, 383–402 (2022). https://doi.org/10.1007/s41358-022-00316-4

20 Hobbs, Carla 2020: The EU as a digital regulatory superpower: Implications for the United States, https://ecfr.eu/article/commentary_the_eu_as_a_digital_regulatory_superpower_implications_for_the_u

21 For an Overview of EU Legislation in the Digital Sector see: https://www.bruegel.org/sites/default/files/private/2023-07/Tables_Scott_Kai.pdf

22 European Council 2024: A digital future for Europe, https://www.consilium.europa.eu/en/policies/a-digital-future-for-europe

23 Bradford, Anu 2019: The Brussels Effect: How the European Union Rules the World. Oxford University Press, pp. 67-68 for de jure, de facto 83-84; Bradford, Anu 2012: 'The Brussels Effect' 107 Northwestern University School of Law Review 1, 3.

24 General Data Protection Regulation, https://eur-lex.europa.eu/eli/reg/2016/679/oj

25 Annegret Bendiek and Magnus Römer, "Externalizing Europe: the global effects of European data protection." Digital Policy, Regulation and Governance 21, no. 1 (2019): 32-43.

26 Bradford, Anu 2023: Europe's Digital Constitution, 6.9.2023, Verfassungsblog, https://verfassungsblog.de/europes-digital-constitution

27 Bradford, Anu 2024: The False Choice Between Digital Regulation and Innovation, Northwestern University Law Review, 118(2).

28 Andersdotter, Amelia / Lakshané, Rohini 2024: European Introspection Standing in the Way of Global Leadership, 24.06.2024, https://botpopuli.net/european-introspection-standing-in-the-way-of-global-leadership

29 GDPR Enforcement Tracker, https://www.enforcementtracker.com

30 GDPR Enforcement Tracker Report, https://cms.law/en/int/publication/gdpr-enforcement-tracker-report/numbers-and-figures; Statistics: Highest individual fines (Top 10), https://www.enforcementtracker.com/?insights

31 What Is the BRICS Group and Why Is It Expanding? https://www.cfr.org/backgrounder/what-brics-group-and-why-it-expanding

32 Reclaiming digital sovereignty, UCL Institute for Innovation and Public Purpose, 12/2024, https://www.ucl.ac.uk/bartlett/public-purpose/publications/2024/dec/reclaiming-digital-sovereignty; Kennedy, Ian 2024: Non-Alignment in the 21st Century: Indonesia and Brazil's Strategic Convergence amidst the US-China-Bipolarity, Indonesian Quarterly, 52 (1), 19-37.

33 Amsden, Alice 2001: The Rise of "The Rest": Challenges to the West From Late-Industrializing Economies, https://doi.org/10.1093/0195139690.001.0001.

34 Bendiek, Annegret/ Stürzer, Isabella 2022: Advancing European Internal and External Digital Sovereignty. The Brussels Effect and the EU-US Trade and Technology Council, SWP Comment 2022/C 20, 11.03.2022, doi:10.18449/2022C20.

35 OECD (2022), "Fostering cross-border data flows with trust", *OECD Digital Economy Papers*, No. 343, OECD Publishing, Paris, https://doi.org/10.1787/139b32ad-en.

36 Empowering the Global South: Seizing the Opportunity for Digital Rights Governance in G20 and Beyond, 16.11.2023, https://www.dataprivacybr.org/empowering-the-global-south-seizing-the-opportunity-for-digital-rights-governance-in-g20-and-beyond; CERRE 2024a: Global Governance of Cross-Border Data Flows (September 2024), https://cerre.eu/publications/global-governance-of-cross-border-data-flows; UNCTAD 2021: Digital Economy Report 2021, Cross-border data flows and development: For whom the data flow, UNCTAD/DER/2021.

37 Banisar, David, National Comprehensive Data Protection/Privacy Laws and Bills 2024 (January 27, 2024). Available at SSRN: http://dx.doi.org/10.2139/ssrn.1951416

38 The data for this section has been collected in 11 months of fieldwork in these four countries from 2020 to 2025 in the context of the PRODIGEES project. This research has received co-funding from the European Union's Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie Grant Agreement No 873119, PRODIGEES (Promoting Research on Digitalisation in Emerging Powers and Europe towards Sustainable Development).

39 El ejercicio de derechos y libertades está en riesgo com una eventual desaparición del INAI, 13.11.2024, https://home.inai.org.mx/wp-content/documentos/SalaDePrensa/Comunicados/Comunicado%20INAI-329-24.pdf; INAI's Dissolution Threatens Mexico's Digital Rights, 9.6.2024, https://mexicobusiness.news/tech/news/inais-dissolution-threatens-mexicos-digital-rights; Newsflash—Constitutional reform dissolving the autonomous constitutional body—INAI, 08.01.2025, https://www.ritch.com.mx/en/read/1015/newsflash-constitutional-reform-dissolving-the-autonomous-constitutional-body-inai

40 Mendoza Enríquez, Olivia Andrea 2018: Protection of Personal Data in Companies Established in Mexico, *Revista del Instituto de Ciencias Juridicas de Puebla*, Mexico, Vol. 12, No. 41: 267-291, at p 289

41 Spotlight: how are data protection laws enforced in Mexico? 25.10.22, https://www.lexology.com/library/detail.aspx?g=b21e9b60-240c-42ed-a64c-fe2377a5415e

42 Brazilian General Data Protection Law (LGPD, English translation), https://iapp.org/resources/article/brazilian-data-protection-law-lgpd-english-translation

43 Brazilian Government, National Congress adopts Law No. 14.460 which transforms ANPD in an autarchy of special nature (Oct. 26, 2022), https://www.gov.br/anpd/pt-br/assuntos/noticias-periodo-eleitoral/congresso-nacional-promulga-a-lei-no-14-460-que-transforma-a-anpd-em-autarquia-de-natureza-especial.

44 ANPD, Balanço de 4 Anos, November 2024, https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/anpd-balanco-4-anos.pdf

45 Lessons from Brazilian DPA sanctions to date, 8.10.2014, https://iapp.org/news/a/lessons-from-brazilian-dpa-sanctions-to-date

46 ANPD, https://www.gov.br/anpd/pt-br

47 The Right Lessons from the Flap Over X in Brazil 9.10.24, https://www.techpolicy.press/the-right-lessons-from-the-flap-over-x-in-brazil; Brazil Took on Musk and Won. Now Lula Is Sharing Notes With Europe, 03.02.2025, https://www.yahoo.com/news/brazil-took-musk-won-now-100000060.html

48 Governo investiga TikTok por tratamento de dados de crianças, https://www.dw.com/pt-br/governo-investiga-tiktok-por-tratamento-de-dados-de-crian%C3%A7as/a-70687997

49 ANPD abre Tomada de Subsídios sobre IA, 6.11.2024, https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-abre-tomada-de-subsidios-sobre-ia; https://www.gov.br/participamaisbrasil/tomada-de-subsidios-inteligencia-artificial-e-revisao-de-decisoes-automatizadas

50 ANPD proíbe pagamento por coleta de íris no Brasil, 25.01.2025, https://www.dw.com/pt-br/anpd-pro%C3%ADbe-pagamento-de-criptomoedas-por-coleta-de-%C3%ADris-no-brasil/a-71404849

51 Digital Personal Data Protection Act 2023, https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

52 Chapter IV, 17, 2(a) of PDPB; Radhika Jhalani 2022: India's Data Protection Bill: the hits and misses, 07 Dec 2022, https://www.context.news/surveillance/opinion/indias-data-protection-bill-the-hits-and-misses

53 Access Now 2024: Strengthening data protection in Africa. Key issues for implementation, https://www.accessnow.org/wp-content/uploads/2024/01/Strengthening-data-protection-in-Africa-key-issues-for-implementation-updated.pdf

54 Sibahle Malinga 2023: InfoReg resolves 70% of POPIA complaints, Johannesburg, 05 Apr 2023, https://www.itweb.co.za/article/inforeg-resolves-70-of-popia-complaints/LPp6VMrByz4MDKQz

55 Information Regulator 2023: Annual Report 2022 – 2023, https://inforegulator.org.za/wp-content/uploads/2020/07/Information-Regulator-Annual-Report-2023-Compressed.pdf; Simnikiwe Mzekandaba 2024: POPIA violation lands education dept in hot water, 14 Nov 2024, https://www.itweb.co.za/article/popia-violation-lands-education-dept-in-hot-water/KzQenvjynNyqZd2r

56 Simnikiwe Mzekandaba 2024: WhatsApp privacy policy fails POPIA compliance, says watchdog, 11.09.2024, https://www.itweb.co.za/article/whatsapp-privacy-policy-fails-popia-compliance-says-watchdog/Gb3BwMWaV1ov2k6V

57 Felix Sieker 2024: Aadhaar and the rise of Digital Public Infrastructure in India, 13.11.2024, https://www.reframetech.de/en/2024/11/13/aadhaar-and-the-rise-of-digital-public-infrastructure-in-india

58 UN Releases Universal DPI Safeguards Framework to Promote Safe and Inclusive Digital Public Infrastructure, 24.09.2024, https://www.undp.org/press-releases/un-releases-universal-dpi-safeguards-framework-promote-safe-and-inclusive-digital-public-infrastructure

59 Dang, Vy / Aliasger Bootwalla / Eva Maria Lynders / Wulf Reiners 2024: Synergising digital public infrastructure and digital commons for sustainable development: the governance of digital resources in India and the EU, https://www.gatewayhouse.in/synergising-dpi-digital-commons

60 Belli, Luca / Jiang, Min 2024: Contesting Digital Sovereignty: Untangling a Complex and Multifaceted Concept . http://dx.doi.org/10.2139/ssrn.4966346

61 Liu, Hong / Miao, Chunzi 2024: Digital geopolitics in a VUCA world: China encounters a new global order, https://doi.org/10.1111/1758-5899.13435

62 Tech wars: US-China rivalry for electronics out to 2035, 19.11.2024, https://www.coface.com/news-economy-and-insights/tech-wars-us-china-rivalry-for-electronics-out-to-2035

63 Tech Policy Trends 2024: The US-China rivalry's impact on global trade, 07.02.2024, https://accesspartnership.com/tech-policy-trends-2024-the-us-china-rivalrys-impact-on-global-trade

64 The future of European competitiveness—A competitiveness strategy for Europe, Report by Mario Draghi, 09.09.2024, https://commission.europa.eu/topics/strengthening-european-competitiveness/eu-competitiveness-looking-ahead_en

65 Benizri, Itsiq/ Fakirova, Ekaterina 2024: Is Europe About to Slow the Pace on Digital Regulations?,26.11.2024, https://www.lawfaremedia.org/article/is-europe-about-to-slow-the-pace-on-digital-regulations; Martens, Bertin 2024: Draghi disappoints on digital, 11.09.2024, https://www.bruegel.org/first-glance/draghi-disappoints-digital; Kirkwood, Megan 2024: Draghi's European Competitiveness Report: Key Findings, 10.09.2024, https://www.techpolicy.press/draghis-european-competitiveness-report-key-findings; European leaders risk increasing inequalities by turbo-charging failed "competitiveness" models, A civil Society briefing, 04.09.2024, https://static1.squarespace.com/static/65c9daef199ea70aa66592fe/t/66d8260c56345378e5e10611/1725441549103/BEP+-+LobbyControl+-+Rebalance+Now+Competitiveness.pdf

66 Luitse, D. (2024). Platform power in AI: The evolution of cloud infrastructures in the political economy of artificial intelligence. Internet Policy Review, 13(2). https://doi.org/10.14763/2024.2.1768

67 AINow 2024: Redirecting Europe's Ai industrial policy. From competitiveness to public interest, https://ainowinstitute.org/redirecting-europes-ai-industrial-policy

68 Conditional Computing: A new paradigm for public-interest AI in the EU, https://brussels.fes.de/e/policy-study-time-to-build-a-european-digital-ecosystem.html

69 O'Neil, Cathy 2016: Weapons of Math Destruction; Ghost in the machine. Addressing the consumer harms of generative AI, 2023, https://storage02.forbrukerradet.no/media/2023/06/generative-ai-rapport-2023.pdf

70 Policy Study: Time to build a European digital ecosystem, 09.12.2024, https://library.fes.de/pdf-files/bueros/bruessel/21688.pdf

71 Digital Compass: the European way for the Digital Decade, COM/2021/118 final, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52021DC0118

72 Ringhof, Julian/ Torreblanca José Ignacio 2022: The Geopolitics of technology: How the EU can become a Global Player, https://ecfr.eu/publication/the-geopolitics-of-technology-how-the-eu-can-become-a-global-player

73 Council Conclusions on EU Digital Diplomacy, 11406/22, 18.07.2022

74 Torreblanca José Ignacio/ Vergi, Giorgos 2024: Control-Alt-Deliver: A digital grand strategy for the European Union, https://ecfr.eu/publication/control-alt-deliver-a-digital-grand-strategy-for-the-european-union

75 European Commission 2024: International outreach for human-centric artificial intelligence initiative, https://digital-strategy.ec.europa.eu/en/policies/international-outreach-ai

76 Torreblanca José Ignacio/ Vergi, Giorgos 2024: Control-Alt-Deliver: A digital grand strategy for the European Union.

77 Hofmann, Stephanie C. / Pawlak, Patryk 2024: Harnessing Europe's Narrative Power to Shape the Digital Future, https://carnegieendowment.org/research/2024/10/harnessing-europes-narrative-power-to-shape-the-digital-future?lang=en&center=europe

78 https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/stronger-europe-world/global-gateway_en

79 Focus harder to rival China's vast global investment plan, Brussels is told, 23.04.2024, https://www.politico.eu/article/focus-hard-rival-china-investment-plan-belt-road-initiative-brussels-eu-global-gateway; Torreblanca / Vergi 2024: Control-Alt-Deliver: A digital grand strategy for the European Union.

80 Börzel, Tanja A. / Krüsmann, Valentin / Langbein, Julia / Wu, Lunting 2023: Colliding Scripts in Asia? Comparing China's Belt and Road Initiative and the EU Global Gateway Strategy, SCRIPTS Working Paper No. 34, Berlin.

81 The Digital Services Act package, https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

82 Lomas Natasha 2023: CJEU ruling on Meta referral could close the chapter on surveillance capitalism, https://techcrunch.com/2023/07/04/cjeu-meta-superprofiling-decision

83 Radsch Courtney C. 2022: Making Big Tech Pay for the News They Use, https://www.cima.ned.org/publication/making-big-tech-pay-for-the-news-they-use

84 Competition Commission South Africa, https://www.compcom.co.za

85 A social media ban in Australia for children under 16 is first in the world, 28.11.2024, https://www.npr.org/2024/11/28/g-s1-36142/australia-social-media-ban-children

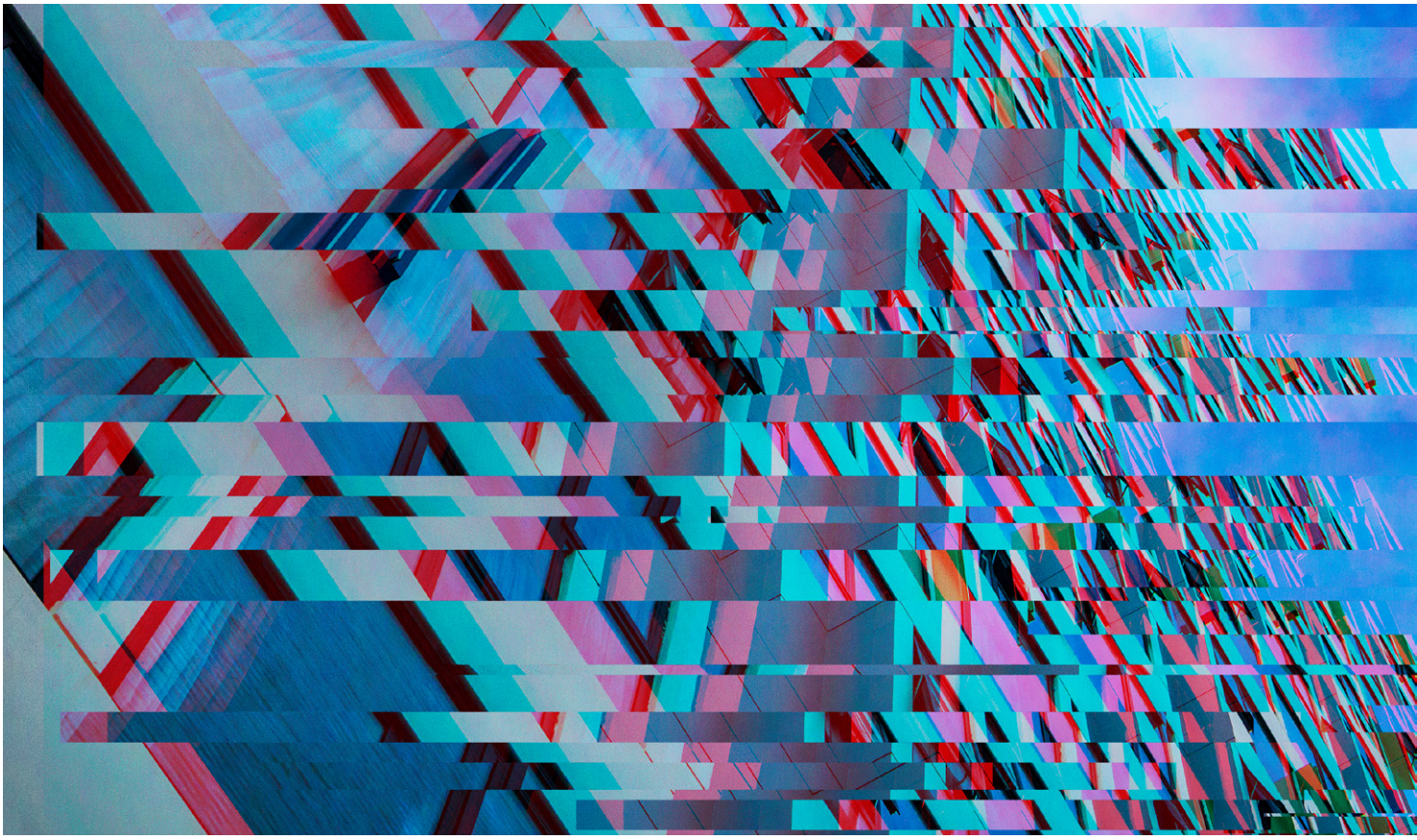
86 European Commission: Digital Partnerships, https://digital-strategy.ec.europa.eu/en/policies/partnerships

87 IT for Change 2024: Beyond Big Tech: A Framework for Building a New and Fair Digital Economy. https://itforchange.net/beyond-big-tech-a-framework-for-building-a-new-and-fair-digital-economy

88 EU-Latin America and Caribbean Digital Alliance, https://international-partnerships.ec.europa.eu/policies/global-gateway/eu-latin-america-and-caribbean-digital-alliance_en

89 Hofmann, Stephanie C. / Pawlak, Patryk 2024: Harnessing Europe's Narrative Power to Shape the Digital Future.

90 Otero-Iglesias, Miguel/ Rodríguez, Gonzalo 2025: Europe's Digital Dilemma: Referee or Player? 14.01.2025. https://www.ie.edu/insights/authors/miguel-otero-iglesias/



IE UNIVERSITY
CENTER FOR THE GOVERNANCE OF CHANGE

AUTHORS:
Ingrid Schneider, Professor for Political Science at University of Hamburg, Department of Informatics (ingrid.schneider@uni-hamburg.de)

RECOMMENDED CITATION:
Schneider, I., *Reclaiming Digital Sovereignty: The EU's Role in the Geopolitics of Digital Governance*, IE CGC, February 2025

Design: epoqstudio.com

Images: Shutterstock; Cover image generated with AI tools

cgc.ie.edu