Digital Sovereignty in a Fragmented World

27 MARCH 2026

Sofia Zanin



Digital sovereignty is a politically determined concept, and its implications vary significantly depending on each country. In recent years, however, the issue has gained renewed urgency as hybrid warfare, cyber operations against critical infrastructure, semiconductor export controls, and the weaponization of digital supply chains have demonstrated how technological dependence can translate into strategic vulnerability. The following article will firstly address why digital sovereignty is such a crucial aspect across multiple domains and is key to most countries in the world. The second part of the article will then outline different approaches, comparing Chinese,

Indian, South African, and European perspectives, while also mentioning the American perspective as a major player in the field. These countries' strategy for controlling the digital domain reflects internal politics, social concerns, and economic status. It is therefore not surprising that China adopted a state-centred attitude, the US a market-based approach, Europe a regulatory and value-based strategy, India created a public infrastructure, and South-Africa a hybrid system that balances forced reliance on foreign infrastructure with strong internal regulation. Lastly, the presented models will be used to outline a likely future outlook on digital sovereignty dynamics.

By comparing these models, the article contributes to understanding how digital governance is reshaping geopolitical competition and offers insight into how states may navigate the tension between security, economic integration, and technological autonomy. The analysis focuses specifically on state-level governance models and geopolitical dynamics shaping digital sovereignty debates; it does not provide a technical cybersecurity assessment nor a detailed examination of private-sector compliance frameworks, as the emphasis lies on strategic positioning rather than operational implementation.

Sovereignty is the most precious element for a nation; it is the core element that defines a country as such. Traditionally, it refers to control over a territory, with borders within which the country can exercise its power over a specific population. With the digital era and the advancement of technology, however, we have seen the rise of a new key domain that transcends traditional geographic borders. This new borderless domain has become the centre of every aspect of a country's social and economic life. In a world where social interactions, markets, businesses, innovation, health, and much more rely on technology, power is derived from controlling digital infrastructure (ECDPM, 2025). This is why controlling how data flows within a territory, i.e. digital sovereignty, becomes essential.

Figure 1: The Digital Technology Stack

This represents a major vulnerability that many actors have been trying to address. In the following paragraphs, an overview of the different approaches adopted will be provided.

In China, digital sovereignty takes on a distinct meaning. It isn't about protecting individuals, it's about protecting the state. China therefore adopts a state-security model, and it is the only country that has achieved an almost total digital independence. The Chinese approach is one of overarching control by the state; we see this in the social and political dimension, but also in the technological one through the Great Firewall (Jiang, 2024). The latter includes several initiatives that filter data and block out multiple foreign digital platforms. Beyond reducing reliance on foreign companies, China has used this framework to create its own, state-led digital ecosystem where everything is home-made and controlled internally. The only crack in the stack is at the chip layer. China still can't produce enough semicon-

ductors to meet its massive domestic demand. This is one of the reasons for the dispute of Taiwan, which is the undisputed leader in semiconductor manufacturing with Taiwan Semiconductor Manufacturing Co. (TSMC) singlehandedly produces roughly 50% of the world's semiconductors. The claim over Taiwan goes beyond territorial disputes; it represents a strategic interest (World Population Review, 2026).

Through a state-centered, self-sufficient model, China keeps tight control over data flow and the population. From an operational point of view, control is close to complete. Beijing secures its digital borders normatively through the Personal Information Protection Law (PIPL). This law resembles the GDPR in some respects. It protects individual rights and has extraterritorial reach. However, the logic is different. Dzigal et al. (2025) call this system cybernetic citizenship, meaning compliance is a state obligation. The biggest provision is data localization. All data must be stored and remain inside China.

The state-based model clearly reduced the vulnerability of digital dependency on foreign infrastructure; however, it also imposes high burdens on foreign companies, significantly reducing foreign investment. For this reason, in 2024, the Cyberspace Administration of China (CAC) introduced some exemptions for foreign parties and created Free Trade Zones (FTZs) in specific cities like Shanghai (Dzigal et al., 2025).

India and South Africa are considered middle powers – albeit at different levels of development. They do not have the same capacity to create their own version of everything, like China, but they also don't want to fully rely on US giants like GAFAM (Google, Apple, Facebook, Amazon, Microsoft). These two countries have been pioneering two very different models; however, Kupchan (2023) categorized them both as swing states, that is, they allow foreign services as long as they adhere to internal regulations, in the case of South Africa, or they use state-led public infrastructure, in the case of India.

India adopts a system based on public infrastructure. They limit the control of foreign companies and services, especially US platforms that are extremely popular in the country, by creating an Indian Stack (Jiang, 2024). The stack built by the state is thought of as a sort of rail track that provides for a network of public infrastructure that private companies can then use to deliver services and manage data. Its key components include Aadhaar, the world's largest biometric identification system; the Unified Payments Interface (UPI), through which international circuits such as Visa and Mastercard operate, forcing foreign banks and systems to use a single public infrastructure; and the Data Empowerment and Protection Architecture (DEPA), which establishes a standardised system for digital consent and data sharing (Jiang, 2024). While the Indian approach seems to have cracked the code between digital sovereignty and foreign investment appeal, serious concerns have been raised about its centralised nature, particularly regarding Aadhaar. Because social and economic participation is tied to a single

digital identifier, exclusion from the platform could effectively result in exclusion from society.

South Africa, on the other hand, faces a serious challenge and mirrors a reality for most Global South countries. As a growing middle power, it confronts what Jiang (2024) describes as two digital paradoxes. First, connectivity is essential for economic growth but simultaneously exposes the country to external control and cyber threats. Second, the tools used to build cybersecurity systems are often the same as those used to conduct cyber attacks. South Africa lacks the capacity to build its own digital stack and has therefore adopted a multilateral model, relying primarily on Chinese hardware and American software. This positioning allows South Africa to remain geopolitically non-aligned – a swing state. South Africa seeks to maintain digital sovereignty through regulatory power. In 2013, it adopted the Protection of Personal Information Act, largely modelled on Europe's GDPR, which recognized the right to privacy as a fundamental and constitutional right (Jiang, 2024). Additionally, in 2021, the country introduced the Cybercrimes Act and a Draft National Policy on Data and Cloud, further reinforcing its regulatory approach (Jiang, 2024).

The EU has been focusing extensively on regulating the digital sphere adopting pioneering legislation and policies like the GDPR (General Data Protection Regulation), the DSA (Digital Services Act), the DMA (Digital Markets Act), the Cybersecurity Act, and the AI Act. All of these regulations and policies are part of a broader effort to ensure digital sovereignty and strengthen strategic autonomy. Given its nature as a union composed of multiple states with differing national interests and approaches, the EU has implemented a quasi-federal system in which supranational legislation is used to regulate and control digital services and infrastructure, ensuring that citizens' rights are protected and collective interests safeguarded (Hulkó et al., 2025). This is the foundation of Europe's value-based approach that preserves citizens' interests while also creating a framework that binds foreign companies and addresses today's digital threats.

However, regulation alone does not address Europe's most significant vulnerability. More than 80% of Europe's digital technologies are imported, three foreign companies (Amazon, Microsoft, and Google) dominate 70% of Europe's cloud infrastructure, and Europe produces only 9% of chips while consuming almost 20% of the worldwide supply (Bria et al., 2025). This clearly highlights a severe structural dependency on foreign infrastructure. As a result, policymakers proposed the EuroStack initiative in 2025 (Bria et al., 2025). The principles driving the initiative are open source, interoperability, and values. The key of the initiative is to create an interconnected system where knowledge is shared without infringing privacy, safeguarding democratic principles, and enhancing the competitiveness of the European economy (Bria et al., 2025). EuroStack adopts a Europe-first approach, similar initiatives in the defence domain.

The proposal gives an architectural blueprint that aims to build an independent and interconnected technology infrastructure. It organizes the digital ecosystem into seven functional layers, ranging from foundational EuroChips (semiconductors) and EuroConnect networks to SovereignCloud, DataCommons, and a digital control center known as EuroOS, which includes a Digital ID Wallet and the Digital Euro. To power this transition, the initiative proposes a €300 billion European Sovereign Tech Fund over ten years to scale homegrown, open-source, and federated systems, thereby reducing *digital colony* dependencies on foreign providers (Bria et al., 2025).

Ultimately, the initiative seeks to modernize the Single Market by mandating "Made-in-Europe" standards and interoperable digital public infrastructures that prioritize privacy, sustainability, and democratic values.

Figure 2: Five models of digital strategy.

From a global perspective, it is important to note that the American approach remains largely market-oriented and sector-specific. The US lacks comprehensive federal legislation, and companies have overall control over the digital arena. Protection is mostly guaranteed through a patchwork of legislation enforced on a state level, like the California Consumer Privacy Act of 2018 and later amendments (Dzigal et al., 2025).

Despite their differences, these approaches reflect a shared understanding: control over digital infrastructure and data flows is essential to safeguarding sovereignty, national interests, and economic growth. Each country has adopted approaches that mirror its political history and current conditions. China adopted a state-centric model with parallel Chinese-made version of each and every platform; the US maintained a market-driven model adopting a laissez-faire approach where companies are in control; India has developed a public digital infrastructure; South Africa relies on regulatory control alongside foreign infrastructure; and Europe has prioritised democratic values while seeking to enhance strategic autonomy through initiatives such as EuroStack.

In the foreseeable future, these strategies are likely to persist. China will continue to retain strong state control and seek higher levels of independence, thus tensions with Taiwan region are bound to remain high, as it represents one of the missing pieces in China's domestically built digital sphere. The US is unlikely to revert course in favour of a more federated approach; however, in terms of regulation, several states are constantly enacting legislation to enhance data protection and privacy (DLA Piper, n.d.). Middle powers will probably take on the South African approach, as it is both economically sustainable and efficient in terms of guarantees. Europe will most certainly keep focusing on the normative aspect; however, it will need to choose whether to move forward with the massive investment required to promote Europe-led services and platforms. As these divergent strategies consolidate, regulatory fragmentation is likely to deepen, reducing global interoperability and increasing compliance burdens for

companies operating across jurisdictions. Yet this fragmentation is itself a reflection of a broader structural shift: digital control is increasingly understood as a core component of state power.

In conclusion, digital sovereignty and strategic autonomy are no longer optional. In a world where growth depends on digital services, control over the digital stack directly translates into political power, digital dependency is a vulnerability, and the digital domain becomes a target of hybrid warfare. To avoid becoming a digital colony, digital sovereignty is crucial.

Bibliography:

Bria, F., Timmers, P., & Gernone, F. (2025). *EuroStack: A European alternative for digital sovereignty*. Bertelsmann Stiftung.

DLA Piper. (n.d.). *United States – Data protection laws*. *https://www.dlapiperdataprotection.com/?t=law&c=US*

Dzigal, N., Safarpour, D., Godolja, D., & Süßlin, L. (2025, February). *Digital sovereignty and geopolitics in the field of data protection: A comparison of the EU, China, and the USA*.

ECDPM. (2025, July 9). *What is digital sovereignty and how can Europe achieve it?* [Video]. YouTube. *https://www.youtube.com/watch?v=LdEZlw7KiYs*

Hulkó, G., Kálmán, J., & Lapsánszky, A. (2025). *The politics of digital sovereignty and the European Union's legislation: Navigating crises*. **Frontiers in Political Science, 7**, Article 1548562. *https://doi.org/10.3389/fpos.2025.1548562*

Jiang, M. (2024), Models of State Digital Sovereignty From the Global South: Diverging Experiences From China, India and South Africa. Policy & Internet, 16: 727-738. *https://doi.org/10.1002/poi3.427*

Kupchan, C. (2023, June 6). *6 swing states in the Global South will decide geopolitics*. Foreign Policy. *https://foreignpolicy.com/2023/06/06/geopolitics-global-south-middle-powers-swing-states-india-brazil-turkey-indonesia-saudi-arabia-south-africa/*

World Population Review. (2026). Semiconductor manufacturing by country. https://worldpopulationreview.com/country-rankings/semiconductor-manufacturing-by-country

Zenner, K., Berjon, R., Caffarra, C., Bonfiglio, F., Toffaletti, S., Chivot, E., Lili, D., Shepura, N., Carrilho, G., Kuzev, P., Parsons, C., Styma, F., Minutillo Turtur, C., Meyers, Z., Kamath, G., Munoz, K., Hacker, P., Rodríguez, A. G., Kahembwe, E., Hallensleben, S., Piatkiewicz, P., Meckel, M., Steinacker, L., Muñoz Ferrandis, C., Klein, T., Goll, F., Rothe, R., Bienert, J., Westerheide, F., Gläser, M., Schwartmann, R., & Ommer, B. (2025, May 12). *The European way: A blueprint for reclaiming our digital future* [Preprint]. SSRN. *https://doi.org/10.2139/ssrn.5251254*