

Digital sovereignty and global data governance: A comparative study of European and American regulatory frameworks

Shaheen Tabassum¹, Dr. Tansif Ur Rehman² and Shah Murad³

Abstract

Digital sovereignty is an emerging policy priority of the 21st century, particularly in light of the importance of data as a pillar of economic growth, national security and geopolitical influence. The EU and the U.S. have taken different, but comparable, steps to control and control the export of data abroad. The European approach are data protection and privacy and regulatory oversight, with extensive legal frameworks; while the United States more innovative approach, market based or governance, with concerns pertaining to national security. They are contradictory policies which affect multinational businesses, cross-border trade, international relations, and have an influence on digital governance and control throughout the world. The debate over digital sovereignty is a broader one of openness and control, privacy and surveillance, and economic integration and state sovereignty. It presents an historical overview of digital sovereignty, and discusses formal regulation, theory, problems and prospects of digital sovereignty in the framework of global governance and developing states in the digital order.

Keywords: challenges, historical context, laws, opportunities, theoretical context

Introduction

Digital sovereignty is defined as a state's control of its technological ecosystem, data flow and digital infrastructure. In the era of big data, AI and cloud that means power goes to the one who has control over the data (Budnitsky, 2017; Gao & Chen, 2025). Increasingly, States see digital governance in terms of autonomy, as

¹Department of Law, Dadabhoy Institute of Higher Education – Pakistan

²Department of Sociology, University of Karachi / Department of Law, Dadabhoy Institute of Higher Education – Pakistan

³Faculty of Law, Federal Urdu University of Arts, Sciences and Technology, Karachi – Pakistan

depending on technologies imported from elsewhere in the world can create vulnerabilities in the country in terms of cybersecurity, economic power and democracy (Abdulkarim et al., 2025; Koutsias, 2025). Thus, digital sovereignty is not just about data protection, it's also about hardware supply chains, telecommunications infrastructure and platform governance (Taylor, 2023).

The European Union (EU) has become a digital governance super regulator, setting standards through legislation and judicial means (De Gregorio, 2020; Smuha, 2024). Europe is attempting to guarantee that the personal information of its residents will be protected, wherever it is utilized, for example in the General Data Protection Regulation (GDPR) (Burri, 2025; Gao & Chen, 2025). Asia, Latin America and Africa, have not only experienced regulatory changes due to the GDPR, but the GDPR too has continued the normative influence of the EU in global governance frameworks (Burri, 2020; Roger et al., 2025). This is a sign of Europe's regulatory assertiveness, which is rooted in the constitutional and human rights traditions of the continent, and in which privacy is recognized as a fundamental right of citizens (De Gregorio, 2020; Smuha, 2024).

The U.S., however, has been a more market-oriented place, with an emphasis on innovation, economic competitiveness and strategic management of digital infrastructure (Bradford, 2023; Budnitsky, 2017). There is still a patchwork federal privacy regime, U.S. security regimes and trade agreements, and corporate influence all influencing the U.S. privacy landscape (Abdulkarim et al., 2025; Taylor, 2023). They are large tech companies that are operating in the digital world, including Google, Meta Platforms (previously called Facebook), Microsoft and Amazon. One can ask the question about the data governance framework at the global level when balancing the sovereignty, economic development and data integration processes is required in developing countries (Burri, 2020; Gao & Chen, 2025).

Review of the Literature

The work of digital sovereignty focuses on transnational corporations, globalization and technological dependence and is a response to these concerns (Bradford, 2023; Budnitsky, 2017). According to European researchers, the model of regulation of the EU will also provide more autonomy as it will limit external control of citizens' data, and strengthen democratic accountability (De Gregorio, 2020; Smuha, 2024). The launch of the GDPR was a turning point in the evolution of data protection practices

and marked a global shift in data protection regulations (Burri, 2025). This is typically referred to as the “Brussels Effect” – the spread of EU standards across the globe because of size of the market and regulatory capacity (Burri, 2020; Gao & Chen, 2025; Roger et al., 2025).

In the area of data transfers and surveillance, too, tensions appear between the United States and the rest of the world (Koutsias, 2025; Taylor, 2023). However, a few issues arose regarding fundamental issues of surveillance laws and individual rights when the EU's Privacy Shield was declared invalid by the Court of Justice of the European Union in Schrems II (De Gregorio, 2020). European critics argue that the U.S. surveillance systems, including under the USA PATRIOT Act, don't offer as much data protection guarantees as EU law requires (Abdulkarim et al., 2025; Budnitsky, 2017). These legal conflicts reflect more contrasting normative views on issues of privacy, security, and state power (Gao & Chen, 2025; Smuha, 2024).

The concept of digital sovereignty, however, in the United States equates with technological superiority and economic wealth and competitiveness, particularly against China (Bradford, 2023; Budnitsky, 2017). Significant efforts have been made in the U.S. to consolidate their geopolitical power in the areas of cloud computing, semiconductors and artificial intelligence (AI) (Abdulkarim et al., 2025; Taylor, 2023). In the meantime, Europe has started to focus on “strategic autonomy” to reduce Europe's reliance on non-European, technology-led companies, and to develop digital capabilities in Europe (Smuha, 2024). Some projects to improve the European cloud infrastructure and semiconductors are viewed as an indication of this policy change (Roger et al., 2025).

Furthermore, researchers doubt the protectionist and internet ‘fragmentation’ connotations of digital sovereignty (Budnitsky, 2017; Gao & Chen, 2025). Others have pointed out that data localization and different regulatory environments are likely to lead to a ‘new internet divide’, which would risk disrupting interoperability and innovation on the internet across the globe (Burri, 2025; Taylor, 2023).

Some say that data sovereignty is key to upholding democratic principles, to maintain cyber security and to stop large corporations or foreign governments from using data (Abdulkarim et al., 2025; Koutsias, 2025). What the literature does offer, however, is a set of conflicting perspectives – the concept of empowering

sovereignty and normative leadership, versus that of digital fragmentation and economic protectionism (De Gregorio, 2020; Smuha, 2024).

Historical Context of Digital Sovereignty

Digital sovereignty developed in tandem with the burgeoning of the internet in the 1990s when the virtual space was commonly described as a sovereign and borderless area beyond the control of the state (Budnitsky, 2017; Gao & Chen, 2025). Early cyber-libertarian thinkers foresaw that the digital networks would put a strain on the constraints of national borders, and would make the role of government in regulating information flows smaller (Bradford, 2023; De Gregorio, 2020). This hopeful outlook was based on the notion that the private sector and technological development would create the digital world—without much political meddling (Burri, 2020; Taylor, 2023).

States were becoming more aware of the strategic value of data and infrastructure control as digital platforms started to play an increasing role in trade, communication and governance (Abdulkarim et al., 2025; Burri, 2025). Concerns about the vulnerability of states to cybercriminals, economic dependence and foreign manipulation entered into policy debates, slowly leading to the reassertion of state control of the digital domain (Koutsias, 2025; Smuha, 2024).

One of the most significant events of 2013 was the mass surveillance scandal that came to light thanks to Edward Snowden and his report on the United States' intelligence agencies (Budnitsky, 2017; Taylor, 2023). The news generated a worldwide debate over privacy, national security and data transfers between countries, particularly Europe (De Gregorio, 2020; Gao & Chen, 2025). European policy-makers saw the revelations about surveillance as a threat to individual rights and national strategic autonomy to foreign digital infrastructure (Koutsias, 2025; Smuha, 2024).

The EU has been increasing its regulatory activities and has taken the normative leadership in the field of global data governance (Burri, 2020; De Gregorio, 2020). This resulted in the introduction of the General Data Protection Regulation (GDPR) in 2018, with strict compliance requirements, hefty financial sanctions and cross-border jurisdiction (Burri, 2025; Roger et al., 2025). It was an overall change in

Europe's perspective from privacy as a consumer protection issue to privacy as a right (De Gregorio, 2020; Smuha, 2024).

The vision of digital governance, on the other hand, in the U.S. was more business oriented and focused on innovation and competitiveness, highlighting the adaptability of national security (Bradford, 2023; Budnitsky, 2017). State and federal privacy laws were divorced and covered various agencies and industries (Abdulkarim et al., 2025). Meanwhile, the power of the corporations was consolidated and America's control of cyberspace strengthened through the use of sophisticated technologies, the use of trade agreements that permitted data to cross borders, and the power of corporations (Burri, 2020; Gao & Chen, 2025).

The intermingling of the notions of digital sovereignty and supply chain resilience, of technology dominance with geopolitical competition increasing, and of election interference and cyber activities becoming more alarming (Abdulkarim et al., 2025; Budnitsky, 2017). At the same time, Europe saw the development of several projects to boost cloud infrastructure, the development of artificial intelligence and the production of semiconductors in the framework of the strategic autonomy project (Roger et al., 2025; Smuha, 2024).

In the meantime, the United States was concerned about obtaining key technologies and limiting the movement of sensitive exports to protect national interests (Bradford, 2023; Taylor, 2023). All this together leaves room for a conclusion about the shift from theory to a defining principle of a twenty-first century economic planning, policy and geopolitical competition (De Gregorio, 2020; Gao & Chen, 2025).

Theoretical Context of Digital Sovereignty

The digital sovereignty theory is based on realism, liberalism and constructivism in international relations. According to the realist's theory, the importance of state control of strategic resources is emphasized and data is considered to be a source of national power. Digital sovereignty is thus crucial for national security and economic independence. Liberal theory championed by free markets and global crossovers of data, has come to the idea that innovation emerges in inter-connected environments. The US method is a liberal economic model, in large scale, of course,

with the leadership of the private sector. Norms and values are emphasized in the constructivist theory.

Finally, the emphasis on privacy as a human right in the EU shows the impact of choices of policy on identity and experience. Digital sovereignty is thus a normative process that is based on accountability and human rights in the democratic sphere. These theoretical perspectives provide an understanding of the reasons behind Europe's preference for regulation and the U.S.'s preference for freedom and strategic power.

Laws Regarding Digital Sovereignty

Several legal instruments define Europe and US digital strategies. In Europe, and in the United States, there are a number of different legal instruments that explain digital strategies:

- **General Data Protection Regulation (GDPR)** – Provides for strict obligations for data protection and its applicability beyond national borders.
- **Digital Services Act (DSA)** – Rules for online platforms to increase accountability and transparency.
- **Digital Markets Act (DMA)** – Draws the focus on the large tech “gatekeepers” and their anti-competitive practices.
- **USA PATRIOT Act** – Increases government surveillance for national security purposes.
- **CLOUD Act (2018)** – Provides U.S. government with the power to access data outside the United States that American companies hold.

The EU legal framework has a consumer rights, privacy-oriented focus, while the US has a national security and flexibility of business operations focus. Such differences have an impact on cross-border data negotiations and cross-border data relationships.

Challenges for Digital Sovereignty

One of the significant challenges is the lack of uniformity in regulations. Non-uniform regulations make compliance even more challenging for multinationals.

Smaller states have difficulty keeping up with the other regulatory regimes. Second, digital protectionism is bound to fracture the Internet. Data localization rules may hinder innovation and increase costs of operations.

Third, the threat from the cyber world constitutes a challenge to the sovereignty effort. The states need to strike a balance between privacy protection and security. Fourth, the geopolitical tensions between the west and new digital actors intensify and expand strategic competition in the global arena, complicating cooperation.

Opportunities for Digital Sovereignty

Digital sovereignty can contribute to improving privacy and consumer confidence. The EU model has had an impact on worldwide standards of data protection, increasing awareness of data protection. Technological leadership helps to drive economic growth and innovation in the US. Planning partnerships for digital trade alignment. Strategic partnerships for digital trade alignment.

The debate on digital sovereignty can be used to put together a regulatory model in developing countries that is both balanced and safe for citizens, but at the same time it encourages foreign investment. International cooperation mechanisms can help reach interoperable standards and fragmentation can be minimized.

Discussion

EU and US are two contrasting, yet complementary, forms of digital governance. In view of the European regulatory activism, it is now being placed in a position to set standards in other regions of the world, and as European corporations dominate, technological leadership is assured. These dynamics influence the dynamics of world trade, cyber security and the norms of human rights. Digital sovereignty is one of the type of conflicts between globalization and States interventions. It's a balance of openness and accountability that's the challenge. Inappropriate regulations may be an obstacle to innovation and digital integration.

Conclusion

Digital sovereignty is changing the world of governance. The EU should have priorities of regulation and privacy and others say US priorities should be innovation

and strategic dominance. Both strategies have an impact on international data governance norms. Cooperation is crucial in the future to stop internet fragmentation and to guarantee digital development that is inclusive, secure and respecting of rights.

References

- Abdulkarim, A., Salihu, A., & Mahmud, M. A. (2025). The weaponization of economic interdependence: Sanctions, financial statecraft, and the fragmentation of the global economic order. *International Journal of Social Sciences and Management Review*, 8(4), 256–275. <https://doi.org/10.37602/IJSSMR.2025.8417>
- Baade, B., & Golz, L. (2023). An empirical analysis of credibility assessment in German asylum cases. *German Law Journal*, 24(2), 310–341. <https://doi.org/10.1017/glj.2023.15>
- Bradford, A. (2023). *Digital empires: The global battle to regulate technology*. Oxford University Press.
- Budnitsky, S. (2017). Will the internet fragment? Sovereignty, globalization, and cyberspace. *International Journal of Communication*, 11, 1–21.
- Burri, M. (2020). Data flows and global trade law. In M. Burri (Ed.), *Big data and global trade law* (pp. 11–41). Cambridge University Press. <https://doi.org/10.1017/9781108919234.003>
- Burri, M. (2025). Digital trade. In C. L. Lim & J. Trachtman (Eds.), *The Cambridge companion to world trade law*. Cambridge University Press.
- De Gregorio, G. (2020). The rise of digital constitutionalism in the European Union. *International Journal of Constitutional Law*, 19(1), 41–70. <https://doi.org/10.1093/icon/moaa038>
- Hylten-Cavallius, K., & Paju, J. (Eds.). (2024). Free movement of persons in the Nordic states. *Common Market Law Review*, 61(1), 260–261. <https://doi.org/10.54648/cola2024021>
- Koutsias, M. (2025). Privacy and data protection in the UK and in the EU: A long history of divergence even during EU membership—Brexit should not bring a divorce with the EU privacy regulatory regime so as to protect trade and human rights in the UK. *European Business Law Review*, 36(1), 103–132. <https://doi.org/10.54648/eulr2025004>
- Roger, M., Lopez, E., & Martin, C. (2025, July). Digital sovereignty in the European Union: Challenges and opportunities. Paper presented at the EU Digital World Series. <https://doi.org/10.13140/RG.2.2.22387.85281>
- Smuha, N. A. (2024). Digital sovereignty in the European Union: Five challenges from a normative perspective. In G. Barrett, P. C. Müller-Graff, J.-P. Rageade, & V. Vadasz (Eds.), *European sovereignty: The legal dimension*. Springer.
- Taylor, M. (2023). *Transatlantic jurisdictional conflicts in data protection law: Fundamental rights, privacy and extraterritoriality*. Cambridge University Press. <https://doi.org/10.1017/9781108784818>

Article Information:

<i>Received</i>	6-Jan-2025
<i>Revised</i>	27-Feb-2026
<i>Accepted</i>	18-Mar-2026
<i>Published</i>	30-Mar-2026

Declarations:

Authors' Contribution:

- All Authors **Conceptualization, and intellectual revisions, Data collection, interpretation, and drafting of manuscript**
- The authors agree to take responsibility for every facet of the work, making sure that any concerns about its integrity or veracity are thoroughly examined and addressed

- **Conflict of Interest:** NIL

- **Funding Sources:** NIL

Correspondence:

Dr. Tansif Ur Rehman

tansif@live.com
