International Journal of Leading Research Publication (IJLRP)

E-ISSN: 2582-8010 ● Website: www.ijlrp.com ● Email: editor@ijlrp.com

Data Sovereignty and Cross-Border Data Flows: Balancing National Security with Global Interoperability

Srinivasa Kalyan Vangibhurathachhi

Srinivasa.Kalyan2627@gmail.com

Abstract:

In the era of digital globalization, cross-border data flows have become essential for economic growth, innovation and international collaboration. However, the growing concerns about privacy, cybersecurity and state control have intensified national efforts to assert data sovereignty through restrictive policies like data localization. This research investigates the tension between national security imperatives, data sovereignty and the benefits of global data interoperability.

While data sovereignty helps in protecting privacy, infrastructure and state interests, the research found that rigid data localization can fragment the internet and hinder global innovation. Key drivers and challenges in data sovereignty include national security and law enforcement, privacy and data protection, strategic economic resource and cybersecurity. Comparative legal and regulatory frameworks analyses revealed that flexible systems such as the GDPR's adequacy model or the US Cloud Act's bilateral mechanisms provide more adaptive paths than unilateral restrictions. Additionally, the research study showed that encryption, federated learning and data classification tools can significantly reduce cross-border data risks.

To balance national security and global interoperability in cross-border data flows, international cooperation and agreements, harmonisation of legal standards and addressing legitimate security needs offer a diplomatic path towards convergence. The study concluded that a balanced model which is anchored in trust, transparency and accountability is feasible and necessary. Such a model should integrate legal, technical and cooperative tools to secure national interests while preserving the benefits of an open and interconnected digital economy.

Keywords: global interoperability, data governance, cross-border data flows, national security.

1. INTRODUCTION

In the current digital era, the global exchange of data across borders has become a defining aspect of economic growth, international connectivity and technological innovation (Kaya & Shahid, 2025). From e-commerce and international financial transactions to cloud computing and online communication platforms, cross-border data flows present immense influence. Accordingly, these data flows enable seamless operation of global firms, facilitate productivity and innovation, encourage academic collaboration and act as the engine for digital economies. At present, the growing volumes of transnational data is considered as strategic asset for global economies.

However, as countries and corporations become more reliant on data, Chin and Zhao (2022) observed that concerns over access, protection and control of data have increasingly intensified resulting in contentious debates on data sovereignty and national security. By definition, data sovereignty is the state's control over data generated within its territory (Koch, 2025). Governments worry about data privacy protection, cybersecurity threats and lawful access to data once it leaves their jurisdiction. This forces governments to pursue data sovereignty through legislative policies that focus on data localisation, limit reach over digital service providers and restrict cross-border data transfers (Koch, 2025). However, a key challenge remains on

how to balance these national interests with global interoperability, which is the free flow of data and seamless integration of digital services across borders which brings significant economic and social benefits (Gulia, 2024).

To this end, this research takes a global perspective by examining legal frameworks, technological infrastructures and the economic impacts related to data sovereignty. The study compares multiple jurisdictions' approaches and draw on case studies, academic research, government policy papers, and technical standards to explore how to reconcile national security concerns with the demands of a connected digital world.

2 PROBLEM STATEMENT

At the heart of the issue is a key tension: As nations seek to protect the security and data privacy of their citizens, outright restrictions on data flows can lead to internet fragmentation and slow global productivity and innovation (Joel, 2023). On one hand, a country may be exposed to risks such as espionage and cyberattacks when sensitive information or government data are stored in foreign servers that are unchecked (Joel, 2023). Accordingly, law enforcement and intelligence agencies fear losing access to critical data as adversaries may gain access to the data when it is housed abroad. On the other hand, Cory and Dascoli (2021) noted that imposing strict data localization (forcing data to stay within country borders) may disrupt international business, raise costs and stifle the economic opportunities that are generated from a globally connected digital ecosystem. In light of these arguments, the problem statement guiding the research is: How can countries safeguard national security and personal data through sovereign control, without undermining economic and collaborative benefits of global data interoperability? To address this problem, the researcher analyses the motivations for data sovereignty measures, the risks of action and inaction, and the frameworks that might bridge the gap between security and openness.

3.0 KEY DRIVERS AND CHALLENGES TO DATA SOVEREIGNTY

It is crucial to understand why governments implement data sovereignty measures. according to De Jong-Chen (2015), the fear of foreign surveillance or unauthorized access to sensitive data on military, intelligence or personal data have motivated countries to keep data locally. Some authorities cite the need to prevent espionage and secure critical information infrastructure as reasons for local data storage (Cory & Dascoli, 2021). Besides, quicker access to data for crime and terrorism investigations without relying on foreign cooperation have motivated law enforcement agencies to keep data at home. Yun (2025) adds that during incidents like mass surveillance revelations, democratic countries seek to ensure that citizens' personal data enjoys strong protection even when transferred abroad. This is exemplified by the European Union's GDPR which restricts international transfers unless the destination guarantees adequate data protection (Voss, 2019). The bone of contention is that once data leaves originating jurisdiction, it may be subjected to weaker privacy laws or misuse.

Apart from the above, Hulvey (2021) noted that authoritarian regimes may invoke cyber-sovereignty to control and monitor data for political stability. By localizing data and controlling cross-border exchange, governments can easily censor content and survey communications. This driver has led to a trend toward "splinternet" where there is fragmented national internets (Perarnaud et al., 2022). For example, Hulvey (2021) reported that China's Great Firewall and data laws aim to maintain strict oversight of data leaving or entering the country in the name of social stability and national security. Further, some governments view data as a strategic economic resource. Cory and Dascoli (2021) highlights that restricting data flows or requiring local storage can stimulate the growth of domestic data centres and local tech sector. In some cases, this crosses into digital protectionism where data localization shields local companies from foreign competition or to compel multinational firms to invest locally. In India, calls for data sovereignty promotes home-grown digital services by keeping data and its value within national borders (Cory & Dascoli, 2021). Overall, these drivers illustrate the threats and challenges that policymakers perceive. This sets the stage for analysing how different jurisdictions respond through laws and policies.

3.2 Comparative analysis of the global legal and regulatory frameworks

Globally, governments have adopted various legal frameworks to govern cross-border data flows which reflects different balances between sovereignty and openness. In the European Union, the General Data Protection Regulation (GDPR) is one of the most stringent data transfer legal framework in the world as it outlines the specific conditions under which personal data may leave the European economic area thus ensuring high level of protection abroad (GDPR Advisor, 2025). Mechanisms include adequacy decisions which recognises that another country's laws offer comparable protection, standard contractual clauses, and binding corporate rules. Qin (2025) argues that the recent EU–US Data Privacy Framework (2023) restored a legal basis for EU–US data flows after the previous Privacy Shield was invalidated over U.S. surveillance concerns. The EU's approach highlights a legal interoperability solution which requires trading partners to meet European privacy standards in order to enable data interoperability.

In the US, Joel (2023) reported that the government historically advocates for free flow of data and opposes data localization in trade agreements as they view open data flows as essential to free and open Internet. Domestically, the US lacks comprehensive data privacy law at the federal level but instead uses sectoral laws to develop national security measures that affect data flows. For example, the CLOUD Act (2018) allows US law enforcement to access data held by U.S. companies overseas via legal process and more recently Executive Order 14117 (2024) seeks to restrict sensitive US data from being accessed by adversary nations (Cory & Chen, 2025). These policies show the US efforts to balance openness with targeted security measures. In the global arena, the US supports initiatives like the OECD privacy guidelines and has played a key role in the new Global Cross-Border Privacy Rules framework which facilitates data transfers among like-minded countries (Cory & Chen, 2025).

Comparing the EU and the US to China, the Chinese government emphasizes cyber sovereignty by implementing strict laws that assert state control over data. The 2017 Cybersecurity Law and the 2021 Data Security Law require certain data like personal, financial and sensitive data to be stored on servers in China and mandate security assessments for transferring important data abroad (Yan, 2022). Besides, the personal information leaving China is subject to compliance checks under the Personal Information Protection Law (PIPL). These measures are rooted in national security and regime control concerns like protecting state secrets, guarding against foreign influence and enabling government access to data. However, in late 2024, Chinese government announced a Global Initiative on Cross-Border Data Flow Cooperation positioning itself as supportive of non-discriminatory data sharing (Cory & Chen, 2025). This can be seen as a response to international pressure and to US moves to curtail Chinese access to data. China's dual stance, that is, strict domestic controls coupled with a call for global cooperation on its own terms, reflects the complex geopolitics of data governance.

Beyond the national laws, there are emerging international frameworks. As noted by Cory and Dascoli (2021), trade agreements like the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) include provisions that prohibit forced data localization, with exceptions for legitimate public policy objectives. The G20's concept of Data Free Flow with Trust (DFFT) focusses on enabling cross-border data movement while retaining trust through common rules and safeguards (Joel, 2023). Multilateral efforts, though nascent, seek to develop norms that reconcile different approaches. For example, the OECD has updated its guidelines on privacy and data flows to encourage interoperability and the Global Cross-Border Privacy Rules (GCBPR) Forum (involving economies from APEC and beyond) provides a certification system to foster trusted data transfers without requiring identical laws (Cory & Chen, 2025). By examining these legal and regulatory approaches, opportunities (mutual recognition agreements or harmonized standards that ease data exchange) and remaining gaps or conflicts (incompatible laws that hinder interoperability) can be identified. Table 1 below comparatively analyses the global legal and regulatory frameworks that affects data sovereignty and interoperability.

Region / Jurisdiction	Key Legal Instruments	Core Principles	Data Transfer Mechanisms	International Stance	Notable Developments
European Union (EU)	GDPR (2018)	Privacy, Sovereignty, Legal Interoperability	- Adequacy Decisions - Standard Contractual Clauses - Binding Corporate Rules	Requires foreign nations to meet EU standards for data protection	EU–US Data Privacy Framework (2023) restored legal basis for transatlantic data flows
United States (US)	CLOUD Act (2018), EO 14117 (2024), sectoral laws	Free Flow of Data, National Security	No federal framework; sectoral and executive instruments control data transfer in context of national security	Promotes open Internet; opposes forced data localization	Supports OECD Guidelines, GCBPR, and DFFT; contributes to shaping global norms
China	Cybersecurity Law (2017), Data Security Law (2021), PIPL (2021)	Cyber Sovereignty, National Security, Regime Control	Data localization required for sensitive data; outbound transfers require security assessments	Supports global cooperation on its own terms; cautious of foreign influence	Global Initiative on Cross-Border Data Flow Cooperation (2024) indicates a shift in tone
International / Multilateral	CPTPP, OECD Guidelines, GCBPR Forum, G20 DFFT	Interoperability, Trust, Non-Discrimination	Voluntary certification (GCBPR), trade provisions (CPTPP), policy principles (OECD, G20)	Facilitate trusted data flows without harmonizing national laws	Efforts still emerging; focus on bridging diverse regulatory models

4. TECHNOLOGICAL INFRASTRUCTURE AND STANDARDS THAT SUPPORT DATA GOVERNANCE

Technology plays critical role in enabling or hindering the balance between data sovereignty and global data flows. Borra (2024) noted that the rise of global cloud service providers such as Amazon AWS and Microsoft Azure means data can be stored and processed in distributed data centres around the world. In response to sovereignty concerns, cloud providers offer region-specific hosting by allowing clients to choose data residency. Besides, cloud service providers are partnering with local firms or governments to create sovereign cloud solutions. In Europe, the **Gaia-X** initiative is a federated cloud framework which aims at giving users control over where and how data is stored and processed thus aligning with European values and standards for data handling (Baur, 2025). Importantly, cloud service providers can deliver global interoperability through common technological interfaces and standards while adhering to local requirements.

Apart from cloud service providers, encryption and privacy enhancing technologies play crucial role in balancing the data sovereignty and global data flows. Jamil (2025) points out that strong encryption both in transit and at rest present a means to mitigate some security and privacy risks of data flows. If data is encrypted, the argument goes, it can safely transit across borders because it remains unintelligible to

unauthorized parties. Advanced privacy-enhancing technologies like homomorphic encryption, secure multi-party computation and federated learning helps in extracting insights from data without sharing the underlying raw data across borders (Garcia et al., 2024). These technologies could offer solutions where data stays in country A but can be used by a service in country B while preserving privacy thus maintaining sovereignty over raw data.

Moreover, technological tools can automatically classify data by sensitivity and apply appropriate controls which only allows certain categories of data to leave the country while localising sensitive data (Fratini & Musiani, 2025). Currently, many organizations use data loss prevention systems and geo-fencing technology to enforce compliance with data transfer rules in a specific country. By examining technical standards like ISO/IEC 27001:2022 (information security management), organizations can structure their systems to meet divergent legal requirements and facilitate compliance for cross-border data management (ISO, 2022). While technological tools and standards can create solutions that allow data to be shared safely to enhance global interoperability, they can become tools of control that reinforce siloed national networks.

5.0 BALANCING APPROACHES TOWARDS NATIONAL SECURITY AND GLOBAL DATA INTEROPERABILITY

Having examined the problems, drivers and legal frameworks, this section looks at the solutions and frameworks that attempt to balance national security with global data interoperability. One balancing approach is through diplomacy and international agreements that set common rules. According to Christakis (2024), the ongoing negotiation of global digital trade rules at the world trade organization and G20's endorsement of principles for data flow like Data Free Flow with Trust (DFFT) play a crucial role in balancing national security with global interoperability. Additionally, mutual legal assistance treaties and new mechanisms like the US Cloud Act bilateral agreements are being updated to facilitate lawful cross-border access to data for law enforcement while respecting privacy – a key aspect of balancing security needs with sovereignty of other nations (Galbraith, 2018). It is important to note that many of these agreements involve like-minded countries thus raising the question of how to include states that have fundamentally different approaches such as China or Russia (Cory & Chen, 2025).

Another approach is striving for a degree of harmonization and mutual recognition in laws and standards. Kaya and Shahid (2025) report that if countries converge on high-level principles around privacy, cybersecurity and government access to data, they can build trust to exchange data. This is exemplified by the EU–US negotiations that led to improved US surveillance safeguards and an arbitration mechanism so that EU countries could considers the US data privacy framework as adequate (Qin, 2025). Frameworks like the Council of Europe's Convention 108+ which is open globally and how adoption of common privacy principles like transparency, accountability, necessity/proportionality for security access across jurisdictions can reduce regulatory distance between nations (De Terwangne, 2021).

Even without formal treaties, there are practical measures that can be deployed to balance national security concerns with global interoperability. As noted earlier, widespread use of encryption features can ensure data remains secure in transit and during storage thus mitigating some security fears (Chen, 2021). Multinational companies that have strong access controls, auditing and transparency reports can reassure governments that foreign entities are not misusing data. With the emerging concept of data trusts or fiduciaries where independent institutions hold and govern cross-border data on behalf of others under strict rules can provide a neutral ground for data sharing (Rinik, 2020). Adhering to certifications like ISO 27701 for privacy management or government-backed certifications is a credible strategy to build cross-border confidence. Accordingly, a combination of legal guarantees and technical safeguards can create the trust needed for interoperability even when underlying laws differ.

Importantly, a balanced solution requires acknowledging and addressing real national security requirements. Yu (2025) argues that carving out narrow exceptions for sensitive data like defence or intelligence that are localised while keeping most commercial and personal data flows open but protected can balance national security concerns. Governments can invest in domestic cybersecurity so they feel more confident in allowing data out while knowing they can secure what stays and monitor what leaves for threats (Chen, 2021). For

instance, improved international processes for lawful data access like expanding membership in agreements such as the Budapest Convention on Cybercrime or crafting new protocols for digital evidence exchange can reduce the temptation for data localization (Spiezia, 2022). By solving the underlying security concerns through cooperation, flexible laws and technology, nations can relax some of the restrictions to promote global cooperation. Overall, stakeholders focussing on building interoperability in the global digital economy should develop and use different tools at various technological layers and integration levels as shown in figure 1 below.

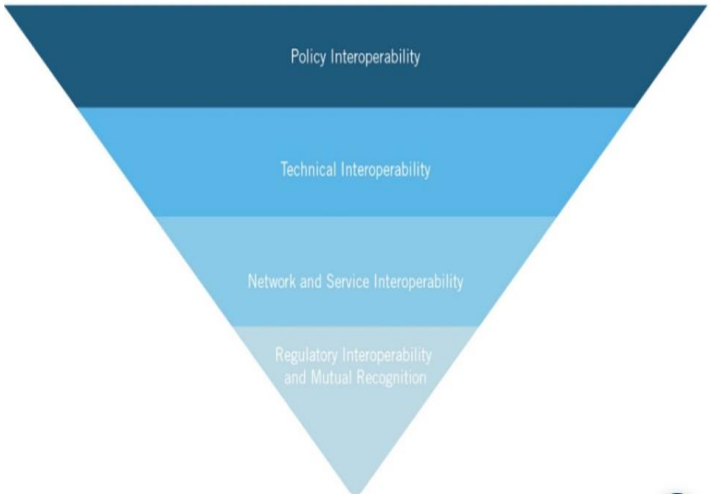

Figure 1: Various layers of global digital interoperability (Cory & Dascoli, 2021)

7.0 CONCLUSION

The findings above highlight the complex interplay between national security and global data interoperability. While data sovereignty is increasingly invoked to protect privacy, infrastructure, and state interests, rigid data localization can fragment the internet and hinder global innovation. Comparative legal analyses reveal that flexible yet accountable systems such as GDPR's adequacy model or the US Cloud Act's bilateral mechanisms, provide more adaptive paths than unilateral restrictions. Moreover, technology that includes encryption, federated learning, and data classification tools can reduce cross-border data risks. Notably, international norms and mutual recognition frameworks offer a diplomatic path toward convergence. Overall, a balanced model that is anchored in trust, transparency, and accountability is feasible and necessary. Such a model should integrate legal, technical and cooperative tools to secure national interests while preserving the benefits of an open, interconnected digital economy.

REFERENCES:

1. Baur, "European ambitions captured by American clouds: digital sovereignty through Gaia-X?," *Information, Communication & Society*, pp. 1–18, 2025. https://doi.org/10.1080/1369118X.2025.2516545
2. Joel, *"Trusted Cross-Border Data Flows: A National Security Priority,"* https://www.lawfaremedia.org/article/trusted-cross-border-data-flows-a-national-security-priority#:~:text=economic%20development%2C%20financial%20inclusion%2C%20health%2C,of%20law%2C%20that%20is%20rights [accessed: 30th June 2025]
3. Koch, "Digital Sovereignty and Cross-border Data Flows: Macroeconomic Challenges and the Shaping of International Economic Law," 2025. Doi:10.13140/RG.2.2.21242.40641
4. De Terwangne, "Council of Europe convention 108+: A modernised international treaty for the protection of personal data, "*Computer Law & Security Review*, vol. *40*, 105497, 2021.

5. Perarnaud, J. Rossi, F. Musiani & L. Castex, "'Splinternets': Addressing the renewed debate on internet fragmentation," *Doctoral dissertation*, Parlement Européen; Panel for the Future of Science and Technology (STOA)), 2022. P. 81-96.
6. Rinik, "Data trusts: more data than trust? The perspective of the data subject in the face of a growing problem,' *International Review of Law, Computers & Technology*, vol. 34, no. 3, pp. 342-363, 2020.
7. e-Estonia, *"e-Governance in Estonia: 100% Digital, 100% Trusted,"* https://e-estonia.com/solutions/e-governance/data-embassy/ [accessed: 2nd July 2025]
8. Spiezia, "International cooperation and protection of victims in cyberspace: welcoming Protocol II to the Budapest Convention on Cybercrime," *ERA Forum*, vol. 23, no. 1, pp. 101-108, 2022.
9. H. Qin, "Regulatory Conflict and the Struggle for Digital Sovereignty: A Critical Analysis of the EU-US Data Privacy Framework," *Studies in Law and Justice*, vol. 4, no.1, pp. 46-59, 2025.
10. H. Yun, "China's data sovereignty and security: Implications for global digital borders and governance," *Chinese Political Science Review*, vol. 10, no. 2, pp. 178-203, 2025. https://doi.org/10.1007/s41111-024-00269-9
11. ISO, *"What is ISO/IEC 27001?,"* https://www.iso.org/standard/27001 [accessed: 1st July 2025]
12. J. Galbraith, "Congress enacts the Clarifying Lawful Overseas Use of Data (CLOUD) Act, reshaping US law governing cross-border access to data," *The American Journal of International Law*, vol. 112, no. 3, pp. 487-493, 2018.
13. J. de Jong-Chen, "Data sovereignty, cybersecurity, and challenges for globalization," *Geo. J. Int'l Aff.*, vol. 16, pp. 112-117.
14. J. Gulia, "Cross-Border Data Transfers: International Cooperation and Conflicts," *Legal Lock Journal, Vol. 4*, no. 2, pp. 263- 281, 2024.
15. M. Kaya & H. Shahid, "Cross-Border Data Flows and Digital Sovereignty: Legal Dilemmas in Transnational Governance," *Interdisciplinary studies in law and politics,* 4(2), pp. 219-233, 2025. Doi: 10.61838/kman.isslp.4.2.20
16. N. Cory & L. Dascoli, "How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them," https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/ [Accessed: 30th June 2025]
17. N. Cory & Z. Chen, "China Unveils New Framework to Stimulate Cross-Border Data Flows: Risk or Opportunity for Multinational Companies," *Crowell,* https://www.crowell.com/en/insights/client-alerts/china-unveils-new-framework-to-stimulate-cross-border-data-flows-risk-or-opportunity-for-multinational-companies#:~:text=China%E2%80%99s%20announcement%20comes%20at%20a,exempt%20transactions%2C%20such%20as%20financial [Accessed: 1st July 2025]
18. P. Borra, "Comparison and analysis of leading cloud service providers (AWS, Azure and GCP)," *International Journal of Advanced Research in Engineering and Technology (IJARET)*, vol. 15, pp. 266-278, 2024.
19. R.D. Garcia, G. Ramachandran, K. Dunnett, R. Jurdak, C. Ranieri, B. Krishnamachari & J. Ueyama, "A Survey of Blockchain-Based Privacy Applications: An Analysis of Consent Management and Self-Sovereign Identity Approaches, 2024 *arXiv preprint arXiv:2411.16404*.
20. R.A. Hulvey, "Cyber sovereignty: How China is changing the rules of internet freedom," *IGCC Working Paper*, no. 2, 2021. https://escholarship.org/uc/item/7sg3716k
21. S. Chen, "Research on data sovereignty rules in cross-border data flow and Chinese solution," *US-China Law Review*, vol. 18, 261, 2021.
22. S. Fratini & F. Musiani, "Data localization as contested and narrated security in the age of digital sovereignty: The case of Switzerland," *Information, Communication & Society*, 28(8), pp. 1368-1386.

23. S. Jamil, "Cross-border data flow and privacy: addressing global privacy challenges in big data," *Journal of Big Data Privacy Management*, vol. 3, no. 1, pp. 41-49, 2025.
24. T. Christakis, "Data free flow with trust: current landscape, challenges and opportunities," *Journal of Cyber Policy*, vol. 9. no.1, pp. 95-120.
25. Y.-C. Chin & J. Zhao, "Governing Cross-Border Data Flows: International Trade Agreements and Their Limits," *Laws*, vol. 11, no. 4, pp. 63-77, 2022. https://doi.org/10.3390/laws11040063
26. W.G. Voss, "Cross-border data flows, the GDPR, and data governance," *Wash. Int'l LJ*, vol. 29, 485, 2019.
27. Z. Yan, "The Dual Foundation of Cybersecurity Legislation," *Social Sciences in China*, vol. 43, no. 3, pp. 4-20, 2022.