Global Review of Humanities, Arts, and Society (GRHAS)

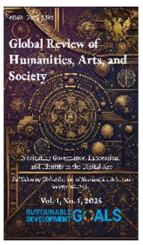
Vol. 1, No. 1, 2025 | pp. 49–58

EISSN: 3052-539X (Online Only)

GRHAS
Global Review of Humanities, Arts, and Society

Navigating Governance, Expression, and Identity in the Digital Age

grhas.centralunitedu niversity.de



Data Sovereignty and National Security: Governance Challenges and Pathways in t he Digital Age

Lin Li[1]

Incheon National University

Abstract

In the digital age, data has become an integral part of national security, and the issue of data sovereignty is increasingly b ecoming a global focus. The intensification of global data flow and the rapid development of information technology prese nt numerous challenges for countries in protecting their data, ensuring national security, and safeguarding economic inter ests. The maintenance of data sovereignty has become a part of international geopolitical competition. In response to these challenges, countries must strengthen their data governance frameworks, establish stringent data protection regulations, and promote international cooperation and coordination to ensure the security and controllability of data flow. This articl e analyzes the relationship between data sovereignty and national security in the digital age, explores the main dilemmas i n data governance, and proposes pathways such as strengthening laws, technology, and international collaboration to enh ance national security competitiveness in the global digital economy.

Keywords: data sovereignty, national security, governance, challenges, pathways

[1] **Lin Li**, Department of Political Science and International Studies, Incheon National University, 119 Academy-ro, Yeonsu-gu, Incheon 22012, Republic of Korea.

1. Introduction

The rapid advancement of information technology, coupled with the emergence of the digital economy, has rendered data an essential resource for the economic and social development of nations. Furthermore, data has assumed a pivotal role within the framework of global governance. Data significantly influences national governance models as well as a multitude of other factors, including economic growth, technological competition, national security, and the safeguarding of personal privacy. Data sovereignty is emerging as a significant focus for governments globally, particularly in response to the rapid advancements in technologies such as big data, artificial intelligence, cloud computing, and blockchain. Digital governance has entered a new stage of globalization, presenting a dual challenge of both opportunities and risks, while also reflecting the intertwining of order and freedom (Yao & Wang, 2025). Countries are increasingly enacting data protection laws and strengthening data governance to safeguard national security and economic competitiveness. However, the contradiction between the global trend of data flow and the territorial nature of national sovereignty has made the issue of data sovereignty a major challenge for national governance in the digital age.

Data sovereignty, based on the inherent powers of sovereign states, represents the highest authority of a state in the realm of data, characterized by core features such as independence, autonomy, and exclusivity (Wu, 2016). Countries strengthen their control over data by enacting data protection laws, establishing regulatory authorities, and reinforcing data localization requirements, thereby forming various models of data governance. Major global economies such as the United States, the European Union, and Russia have implemented legal frameworks governing cross-border data flows, data protection regulations, and relevant multilateral and bilateral economic cooperation agreements (Wan & Ma, 2025). To address the security risks associated with cross-border data flows, China has implemented a series of domestic laws and regulations to strengthen data flow control, including the Cybersecurity Law, Data Security Law, Personal Information Protection Law, Measures for Security Assessment of Data Exports, and Standard Contracts for Cross-Border Data Transfers. Moreover, under the framework of multilateral economic and trade cooperation, China actively promotes the development of a data governance system. Through its participation in international agreements such as the Regional Comprehensive Economic Partnership (RCEP), the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), and the Digital Economy Partnership Agreement (DEPA), China has developed a management framework centered on data localization. This framework extends the traditional standards of sovereignty into the domain of cyberspace governance, clearly defining cyber sovereignty as an extension of national sovereignty in the digital sphere (Zhou, 2025). Consequently, China is establishing a national regulatory system for critical information data.

Against the backdrop of the development of the global digital economy and large-scale cross-border data flows, data governance has become a key issue in the legislative systems and administrative regulatory frameworks of various countries (Sun, 2023). The global competition for data sovereignty is escalating, underscoring the tension between the increasing flow of data across borders and the inherently territorial nature of national sovereignty. Data functions as an intangible asset that frequently traverses international borders, engaging the legal systems of numerous countries and regions (Chai & Wang, 2024). This phenomenon presents considerable coordination challenges for national data regulations. Differences in national or regional stances on data governance have elevated the issue of data sovereignty beyond the scope of domestic governance. Countries need to protect their data sovereignty while also finding a balance between national security, personal privacy protection, and international data cooperation. Moreover, the lack of uniform

international data governance rules may lead to data fragmentation, exacerbating barriers to global digital economic development and impacting global trade and technological collaboration. Future efforts in data governance must extend beyond the mere enhancement of domestic legal frameworks. It is imperative to promote international coordination of data regulations and to establish a more equitable and transparent global data governance system. Such measures are essential for effectively addressing the complex challenges associated with data sovereignty.

2. Relevance of Data Sovereignty to National Security

2.1 The importance of data sovereignty

Data sovereignty is crucial for safeguarding national information security and strategic interests. Data not only reflects commercial value, but also has a direct impact on national security and social stability. Its importance is mainly reflected in the following aspects:

First, the extension of information security and national sovereignty. Information security has become one of the core elements of the national security system as the digitalisation process accelerates in modern society. Data collected from the government, businesses, and various sectors of society encompasses crucial aspects such as citizen privacy, national economic operations, public safety, and infrastructure management. If this data is controlled by external entities, particularly foreign governments or multinational corporations, it could pose a significant threat to the country's sovereignty, economic independence, and social stability.

Taking the US CLOUD Act as an example, the Act establishes a cross-border data governance framework and enshrines in law the principle of extraterritorial data jurisdiction. It creates a reciprocal data access mechanism that allows both the US and foreign governments to access each other's data. In practice, however, there is a notable imbalance: while foreign countries face severe restrictions when attempting to obtain data stored in the US, the US can easily obtain data stored overseas under the Act (Chai & Wang, 2024). This design strengthens US jurisdiction over global data flows and establishes a data governance system that supports its strategic interests. Not only does it increase other countries' concerns about limiting data sovereignty, but it also provides legal grounds for the US to implement global information flow control through its domestic technology companies, thereby presenting greater challenges to other countries in terms of data security and sovereignty protection. The liberalization of cross-border data access has, to a certain extent, weakened the ability of other countries to exercise autonomous control over their own data, especially in the area of information security, where any leakage of information or misuse of data may pose a major risk to national security.

Second, the strategic significance of data resources. In today's digital era, data is increasingly being regarded as a strategic resource of equal importance to land, energy, and capital. As a new type of production factor, particularly in the context of the rapid development of the digital economy, data has become one of the most valuable resources, widely applied in various economic and social activities (Gu, 2024). Countries that control data sovereignty can ensure that their domestic data resources are effectively developed and utilized within the national environment, providing support for the country's economic development. For example, in recent years, China has actively promoted the market-oriented allocation reform of data elements and implemented a series measures, including improving the data infrastructure system, promo

ting data circulation and transactions, accelerating th e construction of data infrastructure, tackling core te chnologies in the data field, and strengthening data security governance. Through these initiatives, China aims to efficiently utilize data resources to drive stea dy development of the digital economy, optimize ind ustrial structure, promote innovation-driven economic growth, and enhance the competitiveness of domesti c enterprises in the global market.

Third, preventing technological hegemony and digita l colonization. As the swift advancement of technolo gy, certain technologically advanced nations and mul tinational corporations have leveraged their strengths in technology and data processing to gradually exert control over global data flows, a phenomenon know n as "digital hegemony." By dominating global data infrastructure and network platforms, these tech pow ers harness data to secure market leadership, technol ogical superiority, and economic competitiveness, ther eby influencing the structure and developmental traje ctory of global industrial chains.

2.2. Impact of data sovereignty on national sec urity

With digital transformation accelerates, the concepts of "sovereignty," "territory," and "security" are being redefined within the realm of data processing and management (Yun, 2024). Data sovereignty empowers a nation to maintain control over its domestic data, preventing external entities from abusing, stealing, o r interfering with this information, which in turn saf eguards national independence and security. Effective management of data sovereignty not only fosters the growth of the domestic digital economy but also pro tects individual privacy, combats technological hegem ony, and ensures that the nation holds a competitive edge on the global stage. This can be understood f rom several perspectives:

First, cybersecurity and critical infrastructure securit y. Digital technologies and data systems are becomin g increasingly important for the management and op eration of critical national infrastructures (such as po wer grids, transport and health systems). Infrastructu re is essential for maintaining national operations an d social stability. However, cyberattacks, data breache s, or technical failures can significantly threaten criti cal infrastructure, jeopardizing national security and social order. Therefore, ensuring the data security of critical infrastructure—especially by preventing foreig n enterprises from controlling core data—is vital for protecting national security.

Second, political security and social stability. In tod ay's world, data serves as both a vital economic res ource and a fundamental component of political secu rity and social stability. Its influence is more signific ant than any other factor in the global economy (G u, 2024). The advancement of digital technology allo ws for the widespread use of data, which can be le veraged for purposes such as manipulating public op inion, interfering with elections, and mobilizing socia l movements. This presents a potential threat to nati onal political security.

Huawei's 5G technology in China is a prime examp le. In response to national security apprehensions, th e United States, Australia, New Zealand, Japan, and t he Czech Republic have imposed restrictions on the use of Huawei's 5G technology, while several Europe an countries are also deliberating similar actions. Th e primary worry for these nations lies in the potenti al ties between Chinese telecommunications firms an d their national intelligence agencies. This concern is exacerbated by China's legal and political framewor k, which requires companies to assist in government intelligence operations (Kaska, Beckvard & Minárik, 2 019; Friis & Lysne, 2021). Additionally, foreign actors might leverage big data and surveillance technologies to manipulate information and influence public opi

nion among specific social groups, further impacting social discourse and political landscapes. Thus, maint aining data sovereignty has become part of the glob al political competition, involving a deep struggle for power, interests and security between nations.

Third, economic security and industrial competitiven ess. Countries that depend on foreign data storage a nd computing services may face significant disadvant ages in the digital economy. Some technologically ad vanced nations and multinational corporations domin ate this space by controlling global data flows. For e xample, many American technology companies posses s vast quantities of data related not only to consum er behavior and market trends but also to competiti ve intelligence across various industries. When count ries rely on these services, their domestic companies may struggle with innovation, product development, and market decision-making, as they lack access to and control over the same volume of data. This imb alance can ultimately lead to a decline in the digital competitiveness of these countries.

In addition, data breaches and improper circulation pose significant risks for countries that rely on exter nal data storage and computing services. If critical t echnologies, industrial development plans, or other n ational economic secrets are leaked or misused, it co uld severely damage the country's long-term competi tiveness. By stealing sensitive data and implementing technological blockades or manipulations, external f orces could weaken a nation's capacity for independe nt innovation and economic sovereignty. The guarant ee of data sovereignty and the security of domestic data is therefore not only a crucial measure for the protection of national economic interests, but also a key factor for the maintenance of a country's compe titiveness in the digital economy.

3.The Governance Dilemma of Data Soverei gnty

The cross-border flow of data involves the develop ment of the global digital economy. However, the gr owing risks to data security have prompted countries to tighten regulations and implement restrictive poli cies, which to some extent have exacerbated conflicts over data governance rules between sovereign states, further triggering international competition (Jia & Z hao, 2024). Countries have to make trade-offs betwe en promoting the free flow of data and strengthenin g security protection. Finding a balance between glo balization and data security, and establishing effectiv e cross-national data governance mechanisms, has be come a major governance dilemma worldwide. Differ ences in national policies and inconsistencies in laws and regulations exacerbate this challenge. This is m ainly reflected in the following aspects:

First, the conflict between technological and politica l logic, particularly reflected in the decentralized nat ure of blockchain technology (Zheng, Xie, Dai, Chen, &Wang, 2017). Blockchain technology achieves data s torage and transactions through decentralization, freei ng data from the control of traditional central autho rities. These characteristics challenge the boundaries of national sovereignty, particularly in terms of data governance and control. Although data sovereignty is gaining increasing attention worldwide, decentralized technologies such as blockchain have made data ind ependent of any national central system or enterpris e, potentially weakening state control over data flow s. Moreover, the decentralized nature of blockchain t echnology results in data being stored in a distribut ed manner, making unified regulation and oversight difficult, which disrupts traditional theories of nation al sovereignty. The conflict between technology and politics means that, in the context of globalization a nd technological advancements, countries face unprec edented governance dilemmas.

Second, the balance between data protection and technological innovation. In the digital society, data privacy has become a critical issue for ensuring personal information security and data sovereignty (Ali, 2024). However, overly stringent data regulations and protection measures can negatively impact technological innovation and cross-border cooperation. While it is essential to safeguard data security and privacy and prevent data misuse, excessively strict data regulations may impede data flow and stifle research, development, and the market competitiveness of innovative enterprises. Many emerging technologies, such as artificial intelligence and big data analytics, depend on access to large volumes of data, and strict data protection could hinder their innovation and practical applications. Furthermore, international cooperation is increasingly important in the global digital economy. Countries must promote data security without resorting to isolationist policies. Strict domestic data protection regulations could hinder collaboration between multinational enterprises and global data sharing, ultimately affecting international trade, technological cooperation, and the establishment of global value chains.

Third, the dilemma of international coordination in data governance. Despite the rising cross-border flow of data and the ongoing process of globalization, there are still no unified global rules for data governance. The significant differences in data protection and privacy standards across various countries create numerous challenges for cooperation between multinational enterprises and governments regarding data (Dong, Chen, & Wu, 2025).

On one hand, the differences in legal frameworks for data protection in different countries require businesses to comply with multiple and complex requirements when operating across borders. For instance, the European Union's General Data Protection Regulation (GDPR) sets high standards for data protection, while regulations in other countries may be less stringent regarding privacy and data control. As a result, multinational companies must find a balance between various legal systems. This not only raises operational costs and legal risks but also creates institutional barriers to cross-border data flow, increasing the costs associated with transactions and data movement (Yue & Xu, 2024). On the other hand, differences in priorities, policy orientations, and economic interests regarding data governance among countries have made international coordination increasingly challenging. Conceptual differences also complicate cooperation in this area. This is particularly evident in sensitive data and national security, where varying national requirements for data access and usage further hinder cross-border collaboration. Therefore, there is an urgent need to establish globally unified data governance rules to ensure that countries can protect data security while also promoting cooperation and development in the global digital economy.

Fourth, technological dependence and digital hegemony. The dependence of some countries on foreign suppliers in key technology areas, especially in chip manufacturing, cloud computing platforms and operating systems, has left their data sovereignty subject to the control of other countries. When essential technologies are controlled by external entities, a country's digital infrastructure and data storage may become susceptible to outside interference. More technologically advanced nations, leveraging their technological and data capabilities, can exert "digital hegemony," applying political and economic pressure on less powerful countries. This situation not only diminishes the digital sovereignty of weaker nations but also heightens the disparities in competition within the global digital economy.

4. Pathways to Safeguard Data Sovereignty

4.1. Strengthen legal and policy protections for data sovereignty

Data protection laws are the foundation of data sovereignty. Many countries have begun to strengthen the formulation of data protection regulations. A notable example is the European Union's General Data Protection Regulation (GDPR), which was implemented in 2018 and established a framework centered on protecting individual data rights. This regulatory system strengthens mechanisms for personal information protection and creates a robust model for managing cross-border data flows (Chai & Wang, 2024). The GDPR not only enhances personal data safeguards but also delineates clear requirements for the transfer of data across borders. Countries can draw from international best practices like the GDPR and, taking into account their unique national contexts, develop laws and regulations that better serve their national interests.

When creating data protection laws, countries should focus on several issues. First, they need to clearly define the concept of data sovereignty and determine which types of data fall under national jurisdiction. Second, it is essential to establish basic requirements for data collection, storage, processing, and transmission, ensuring that data flows comply with security, privacy, and regulatory standards. Third, countries should strengthen control over cross-border data transfers, especially regarding sensitive data, to prevent data leakage, misuse, and outside interference. Additionally, governments should enhance their oversight of multinational corporations and foreign-funded companies. For instance, multinationals operating within a country should be required to adhere to local data protection laws and should not store data on foreign servers. Enforcing data localization through legal measures will help not only to prevent data breaches but also to stop foreign companies from using data to gain an unfair competitive advantage in local markets.

4.2. Enhancing technological autonomy and strengthening data governance capabilities

To mitigate excessive reliance on external technologies, countries should prioritize increasing their investment in domestic research and development, particularly in critical technological areas. In addition, bolstering the construction of network security infrastructure is important for safeguarding data sovereignty. Governments ought to invest in the advancement of sophisticated cybersecurity technologies and protective systems to enhance their ability to respond effectively to external attacks, data breaches, and various other risks. Moreover, it is crucial to strengthen the training of cybersecurity professionals due to the rising demand for talent in this sector. Related training initiatives and reserve systems should be enhanced to ensure that the nation has sufficient technical support in the realm of data security.

4.3 International cooperation and management of cross-border data flows

The safeguarding of data sovereignty is not solely a national responsibility; it also necessitates vital cooperation from the international community. To effectively address the challenges posed by cross-border data flows, it is essential to enhance the framework for data governance on a global scale. For instance, the United Nations could play a pivotal role in promoting the development of unified international data protection standards, ensuring that all countries adhere to consistent regulations during data transfers. Additionally, governments should pursue bilateral or multilateral data protection agreements that reflect their n

ational interests and the current international landsc ape. Regional data protection agreements also serve as a significant avenue for advancing international d ata governance. Through international negotiations, c ountries can resolve disputes related to data trade, t hereby mitigating the impact of disruptions on globa l economic cooperation. It is crucial for the internati onal community to foster a consensus on data trade rules and promote the establishment of a fair and tr ansparent environment for data exchange.

5. Conclusion

In the digital age, data has become an essential res ource for global governance and national security. D ata sovereignty not only signifies national sovereignty but also serves as a fundamental pillar of national security in the context of the digital economy. The i ntertwining of globalization and digitalization has le d to data flows that transcend national borders, brin ging unprecedented opportunities and challenges. The effective maintenance of data sovereignty has emerg ed as a critical concern for governments seeking to enhance their countries' competitiveness in the globa l digital economy.

Data sovereignty is closely related to national securi ty. Due to the development of information technolog y, data has become an essential resource for nationa l governance, economic development, and social stabi lity. Whether it is personal data, corporate data, or data related to critical national infrastructure, its sec urity and independence directly affect national securi ty. Risks such as data breach, misuse, and external c ontrol can lead to security vulnerabilities in various areas, including politics, economics, and culture.

At the same time, protecting data sovereignty faces many challenges. The ongoing conflict between techn ological logic and political logic, along with the bala nce between data protection and technological innov ation, the management of cross-border data flows, a nd the absence of global data governance are issues that countries must tackle when implementing data sovereignty. The decentralized nature of technology, c ombined with the complexities of cross-border data f lows, makes it challenging for countries to maintain complete control over their data movement. When a dvocating for data localization and implementing stri ngent data protection regulations, countries must bal ance the need for data security with the risk of hin dering technological innovation and international coll aboration. Moreover, the varying standards and polici es related to data flow across nations further compli cate data governance.

Overall, data sovereignty is intricately connected to national economic security, social governance, and po litical stability. To address both domestic and interna tional pressures, countries must implement comprehe nsive measures. This entails striking a balance betwe en the demands of technological innovation and the necessity for data protection, reinforcing digital techn ology autonomy, fostering international cooperation, and securing a competitive edge in the global digital arena. Only through a multi-faceted strategy can da ta sovereignty be effectively upheld, national security be preserved, and a robust system and technological foundation be established for the sustainable advance ment of the global digital economy.

Reference

Ali, D. A. (2024). Artificial intelligence and data privacy: B alancing innovation with security. *Frontiers in Artificial Int elligence Research, 1*(2), Article 2.

Chai, Y., & Wang, T. (2024). Legal regulation and optimiza tion path for the supervision of cross-border data flows in China. *Journal of Jiangsu Police Institute, 39*(04), 49–58.

Dong, K., Chen, X., & Wu, J. (2025). Research on policy at tention in cross-border data flow governance from the pers

pectives of isomeric and isomorphism. *Information Studies: Theory & Application*, 1–10.

Friis, K., & Lysne, O. (2021). Huawei, 5G and security: Tec hnological limitations and political responses. *Development and Change, 52*(5), 1174–1195.

Gu, H. (2024). Data, big tech, and the new concept of sov ereignty. *Journal of Chinese Political Science, 29*(4), 591–61 2.

Jia, K., & Zhao, J. (2024). "Dual-goal" sovereignty theory i nnovation and cross-border data flow ginzo. *Academia Bim estris*, 04, 105–113+215.

Kaska, K., Beckvard, H., & Minárik, T. (2019). *Huawei, 5G and China as a security threat*. NATO Cooperative Cyber D efence Center of Excellence (CCDCOE), 28, 1–26.

Sun, C. (2023). Comparative study on supervision and secu rity of cross-border data flow. *Journal of China Academy o f Electronics and Information Technology, 18*(1), 91–96+102.

Wan, G., & Ma, X. (2025). Review and improvement path of legal regulations on cross-border data flows in China. *J ournal of Zhengzhou University of Light Industry (Social S cience Edition), 26*(01), 59–68.

Wang, X. (2024). Discussion on the cultivation of professio nal talent in computer network security technology in the context of big data technology applications. *Computer Kno wledge and Technology, 20*(09), 148–150.

Wu, S. (2016). Studies on transnational data flow and data sovereignty. *Journal of Xinjiang Normal University (Edition of Philosophy and Social Sciences), 37*(05), 112–119.

Yao, T., & Wang, Y. (2025). Cross-border data flows from the perspective of data sovereignty and China's response. *I nternational Business*, 02, 141–156.

Yue, S., & Xu, C. (2024). Legal obstacles and innovative st rategies for data cross-border flow of RCEP. *Journal of Cha ngchun University, 34*(09), 80–85.

Yun, H. (2024). China's data sovereignty and security: Impl ications for global digital borders and governance. *Chinese Political Science Review*, 1–26.

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). A n overview of blockchain technology: Architecture, consensu s, and future trends. *2017 IEEE International Congress on Big Data (BigData Congress)*, 557–564. https://doi.org/10.110 9/BigDataCongress.2017.85

Zhou, M. (2025). Research on the extraterritorial data juris diction model and its improvement of data security law. *J ournal of Huaqiao University (Philosophy & Social Science s)*, 01, 116–127.

Copyright Statement for Online Publication

© 2025 by the author(s). This article is published by Global Review of Humanities, Arts, and Society (GRHAS) under an exclusive license for online publication and digital dissemination.

The authors retain full copyright of this work. GRHAS holds the exclusive right of first publication in electronic format.

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License (CC BY-NC-ND 4.0).

To view a copy of this license, visit: https://creativecommons.org/licenses/by-nc-nd/4.0/

All rights not granted under this license are reserved by the author(s) and the publisher.