International Journal of Education and Social Development
ISSN: 3078-9931 (Print), ISSN: 3078-2287 (Online) | Vol. 2, No. 3, 2025

Research on the Governance of Cross-border Data Flow Under the Holistic View of National Security

Linqi Li, Xiaoyu Li

School of Law, Henan Normal University, Xinxiang 453007, China

Abstract: The increasing frequency of cross-border data flows has brought new momentum to globalization, but it has also brought many challenges. In the context of the holistic view of national security, in order to better maintain international security, overall development and security, it is imperative to improve China's governance model for cross-border data flow. Through scientific and reasonable legal regulations to effectively safeguard national security, a set of cross-border data flow governance model reflecting Chinese wisdom and Chinese solutions is proposed, that is, the "China Blueprint" : improve the top-level design of cross-border data flow and formulate security norms for cross-border data flow; Combined with the progress of the pilot work, summarize the experience, explore the leading scheme of cross-border data flow in key areas, and form a unified organization model for reference; We will strengthen technical support for data security governance, cope with risks brought by technology, and provide Chinese solutions and Chinese wisdom for global data flow and economic development.

Keywords: The holistic view of national security, cross-border data flows, top-level design, Pilot areas.

1. Introduction

In the era of the rapid development of big data and artificial intelligence, data has become an important factor of production today. The cross-border flow of data is becoming more and more frequent. More and more enterprises and institutions are using cross-border data flow for cross-border trade and information transmission, which is promoting the development of China's new quality productivity. However, the cross-border flow of data involves a large number of data from different countries and regions, including a large amount of sensitive data and personal information data. Due to the differences in data security standards and privacy protection laws of each country and region, it is very easy to lead to data information leakage in the process of cross-border data flow, which threatens national security, giving Cross-border data flow has brought great challenges. Therefore, it is necessary to establish a perfect cross-border data flow governance system to protect the security of cross-border data flow. Under the holistic view of national security, China can solve the problems in cross-border data flow governance through the following measures, and describe the "Chinese blueprint" of cross-border data flow governance: improve the top-level design of cross-border data flow and formulate security norms for cross-border data flow; explore the advance plan of cross-border data flow in key areas, combined with Summarize the progress and experience of the pilot work; strengthen the technical guarantee of data security governance, and deal with the risks brought by technology.

2. Improve the Top-level Design of Cross-border Data Flow

The "Opinions of the Central Committee of the Communist Party of China and the State Council on Improving the Institutional Mechanisms for Market-Oriented Allocation of Factors of Production" not only put data on an equal footing with land, labor, capital and technology, but also put forward the importance of data to the development of productivity. Major strategic plans such as the "14th Five-Year Plan" also point out the establishment of relevant systems for cross-border data flow to promote the safe and orderly cross-border data flow. Therefore, it is imperative to improve the top-level design of cross-border data flow.

2.1. Refine the Specialized Legislative Norms of Cross-border Data Flow

With the further development of China's economic situation, the proportion of the digital economy in China's overall economic share is increasing, and only by improving the relevant legal system can we promote the healthy development of the digital economy. Since the official implementation of the National Security Law of the People's Republic of China, China has clarified the importance of information systems and data security control in key areas for the first time in national legislation, which is crucial to safeguarding the sovereignty, security and development interests of the country. However, China's cross-border data flow legislation does not have a clear framework, and the laws and standards that have been introduced or have not been introduced with fragmented knowledge. In addition to basic laws such as the Data Security Law, the Personal Information Protection Law and the Network Security Law, others are mainly scattered in some regulations and normative documents. The problems are obvious, their effectiveness level is relatively low, the content of some laws is not clear enough, the supervision ability and protection level are insufficient, and the cross-border data flow involved There are fewer international treaties.

First of all, under the background of the holistic view of national security, China's cross-border data flow governance should take into account the factors of all parties when legislating to ensure that the legislative norms are operational. The key to the holistic view of national security lies in "holistic", emphasizing the systematic thinking and methods of doing a good job in national security, highlighting the concept of "great security", covering many fields such as politics, military and land, and constantly expanding with social development[1]. Secondly, with the promulgation of the Measures for Data Exit Safety Assessment, China has

formed a top-level design framework for data classification and grading management, which clarifies the rules for cross-border flow of data according to the sensitivity and risk of different types of data. In the legislation of cross-border data flow, the classification management of cross-border data classification should be clarified, and the legality, legitimacy and necessity of data processing by data exit and overseas recipients should be clarified. The specific implementation path of the data cross-border flow governance system should be further clarified to build a data cross-border flow governance body with Chinese characteristics department. Finally, in terms of cross-border data flow governance mechanism, bilateral and multilateral agreements and regional trade agreements have become the main forms of international governance cooperation, and unilateral legislation has become the main mode of domestic governance[2]. Actively participating in the signing and formulation of bilateral and multilateral treaties on international cross-border data flow can not only learn from the advanced experience of foreign countries, but also export successful domestic experience to other countries in a timely manner, narrow the gap between domestic and international, and provide Chinese wisdom in the formulation of international rules.

2.2. Optimize Policies and Norms Related to Cross-border Data Flow

China possesses extensive expertise in policymaking and has established a comprehensive regulatory regime for cross-border data flows. Key measures include the Measures for Security Assessment of Cross-Border Data Transfers and the Measures on Standard Contracts for the Export of Personal Information, which institutionalize risk assessment mechanisms for data exports and standardize procedures for transferring personal information. The Regulations on Facilitating and Regulating Cross-Border Data Flows promulgated and implemented in March 2024, aim to advance secure and orderly cross-border data mobility while balancing data free flow with robust safeguards for data security and personal information rights and interests. This dual focus fosters the growth of the global digital economy by aligning regulatory rigor with market dynamism.

First, following land, sea, air, and outer space, cyberspace has emerged as humanity's fifth sovereign domain. However, China's current legal and policy frameworks have yet to fully integrate cutting-edge technological advancements, such as AI-driven data analytics and quantum encryption. Existing regulations exhibit gaps in technological neutrality and future-proof legislative design necessitating systematic updates to ensure scientific rigor, regulatory rationality, and strategic foresight in governance. Secondly, the security governance and regulation of cross-border data flow also require international cooperation and coordination. When formulating relevant policies, it is not only necessary to fully consider international factors, refer to relevant international standards and practices, and connect with the international, but also to communicate and consult with other countries and regions to ensure that China and other countries in the future The cross-border cooperation between is smooth. In addition, in order to conform to the development trend of the times, China has published many drafts for comments to widely listen to the opinions of the public, but some drafts for comments have not been officially promulgated and implemented until now. The reasons behind this are worth considering. Cross-border data flow governance is a systematic project that requires the cooperation of multiple departments. In the process of soliciting opinions, it is necessary to conduct in-depth discussion and consultation on the content of legal provisions to ensure a clear and consistent division of responsibilities between departments, coordinate the relationship between domestic data governance and cross-border data flow, coordinate security and development, and ensure that policies keep pace with the times.

2.3. Strengthen Information Infrastructure Development for Cross-Border Data Flows

The introduction of the holistic approach to national security holds significant and profound implications for the legal development of national security in the People's Republic of China[3]. Against this backdrop, China's cross-border data flow governance must rigorously implement this holistic approach to address emerging practical challenges and achieve multidimensional coordination. Strengthening information infrastructure development for cross-border data flows will not only optimize data transmission networks and enhance the efficiency of cross-border data mobility but also reinforce data storage and transmission security. By establishing a robust data security framework and advancing privacy-preserving technologies, this infrastructure enhancement will fortify the security and privacy protections during cross-border data transfers, thereby advancing secure governance of transnational data flows while systematically safeguarding and shaping national security.

Strengthening information infrastructure development for cross-border data flows constitutes a systematic project requiring coordinated advancements across multiple dimensions, encompassing technical innovation, policy alignment, and international collaboration. At the technical level, sustained investment in R&D resources is imperative to drive technological breakthroughs that enhance infrastructure performance and security. A multi-layered security architecture must be established to ensure data integrity and confidentiality during cross-border transfers, while accelerating the integration of cutting-edge technologies such as cloud computing, data interoperability, and next-generation machine learning into infrastructure frameworks to elevate capabilities in data transmission networks[4], processing capacity, and storage security. On the policy front, refining legislation and regulatory measures is critical to provide unambiguous legal safeguards and governance standards for cross-border data flows, including clarifications on data sovereignty and compliance thresholds, thereby establishing a transparent legal framework. Internationally, collaborative mechanisms must be institutionalized. The Digital China Development Master Plan jointly issued by the Central Committee of the Communist Party of China and the State Council in February 2024 emphasizes expanding digital cooperation under multilateral frameworks such as the UN and WTO, advocating high-caliber platforms for global digital engagement and proactive contributions to shaping international rules on cross-border data governance.

3. Explore Pilot Initiatives for Cross-Border Data Flow Governance in Priority Sectors

Coordinating development and security constitutes the core principle of the holistic approach to national security. Since

the 18th CPC National Congress, the CPC Central Committee has consistently emphasized the integration of development and security, underscoring that greater openness necessitates stronger coordination between the two. The pilot initiatives for cross-border data flow governance in priority sectors operationalize this principle by tailoring governance models to specific industries, designated regions, and scenario-specific contexts, thereby exploring pathways aligned with China's national conditions. These pilots serve as a strategic mechanism to advance the high-quality development of digital trade while refining a sovereignty-compatible governance framework for cross-border data flows.

3.1. Scaling Pilot Experiences to Priority Sectors

China's cross-border data flow pilots have been implemented across multiple regions and industries. Firstly, the Lingang New Area of Shanghai released the nation's inaugural scenario-specific general data catalogs for cross-border transfers, covering three sectors: intelligent connected vehicles (ICVs), publicly offered funds, and biopharmaceuticals. Secondly, leveraging platforms like the Hengqin-Guangdong-Macao Deep Cooperation Zone and the Qianhai-Shenzhen-Hong Kong Modern Service Industry Cooperation Zone, the Greater Bay Area has pioneered a cross-border data flow mechanism for Hong Kong/Macau enterprises, including a "whitelist" system to facilitate secure and efficient intra-regional data mobility. Additionally, under the guidance of the Cyberspace Administration of China (CAC), Beijing has emerged as a demonstration zone for security assessments of outbound data transfers, mandating risk self-assessments for key enterprises in sectors such as social media, healthcare, and finance, while advancing cross-border data flows through its International Information Industry and Digital Trade Hub.

Synthesizing pilot experiences reveals that China's cross-border data flow governance primarily focuses on priority sectors such as ICVs, biopharmaceuticals, and publicly offered funds, where urgent data mobility demands and distinct industry characteristics endow pilot models with replicable value. All pilots explicitly pursue objectives to facilitate cross-border data flows, ensure data security, and foster digital economic growth, supported by sector-specific data catalogs and operational guidelines tailored to practical needs and industry profiles, thereby providing clear compliance pathways. Regional pilots have further instituted hierarchical data classification frameworks and scenario-specific catalogs to codify rules for secure, compliant, and efficient cross-border transfers. Distinctive governance innovations include mechanisms such as the Jiangsu Province Guidance on Filing Standard Contracts for Personal Information Exports (First Edition), which introduced contract filing review procedures, offering novel regulatory approaches to cross-border data governance.

3.2. Develop Scalable and Replicable Compliance Governance Frameworks

The establishment of cross-border data flow governance pilots, tailored to regional realities through localized data management regulations, strengthens data security safeguards and enhances the protection of data during transnational transfers. These pilots not only drive the harmonization and refinement of relevant laws and policies—clarifying critical issues such as regulatory standards for cross-border data flows to eliminate systemic barriers—but also enable targeted expansion by selecting new pilot zones and sectors based on data mobility dynamics. Priority should be given to regions and industries with robust digital economies and acute cross-border data demands, coupled with the formulation of granular pilot implementation plans that specify objectives, operational protocols, and interagency coordination mechanisms to ensure procedural integrity and regulatory alignment.

Cross-border data flow governance pilots can adopt diverse modalities, focusing on critical sectors such as artificial intelligence, industrial internet, and cross-border e-commerce[5], while leveraging institutional innovations like data export negative lists in designated zones such as free trade pilot areas to enhance facilitation and support for transnational data mobility. For instance, the Lingang New Area of Shanghai capitalizes on its institutional openness and international technological collaboration ecosystem to expand pilot scopes, explore alignment with global cross-border rules, and develop replicable compliance governance models. Under security-controlled conditions, these pilots test pioneering data flow mechanisms to inform national policy frameworks. By integrating existing international science and technology cooperation networks, China deepens governance experimentation in cross-border data flows, amplifying the global influence of its regulatory norms[6]. Initiatives like the Negative List and General Data Catalog released by Tianjin and Shanghai Lingang Free Trade Zones exemplify early efforts to relax non-essential data export restrictions, optimize foreign investment environments, and offer novel methodologies for data governance in future pilot regions and sectors.

4. Strengthen Technological Safeguards for Cross-Border Data Security Governance

The asymmetric capacities in cross-border data security governance among nations, coupled with threats such as data hegemonism and extraterritorial jurisdiction, necessitate urgent enhancement of China's capabilities in securing cross-border data flows. Modern technological advancements provide robust impetus for transnational data mobility, demanding increased investment in modern IT infrastructure and R&D to counter technical risks with technical safeguards[7]. Concurrently, targeted capacity-building programs and technical workforce development must address existing gaps in expertise and talent shortages. Strengthening research in advanced technologies—such as homomorphic encryption, zero-trust architectures, and AI-driven anomaly detection—while upskilling professionals to mitigate cross-border data security risks, is critical to aligning governance capabilities with evolving technological landscapes.

4.1. Strengthen Modern Information Technology Research

The development of modern technology has provided strong driving support for cross-border data flow, and the expansion of big data, artificial intelligence and other fields has also made cross-border data flow more efficient. The rapid development of technology is both an opportunity and a challenge. The balance between data security and data circulation is the core issue that needs to be discussed in cross-border data flow governance[8]. In the digital age, we must

consider the influence of technology, use technology to help realize the governance of cross-border data flow, use modern information technology to deal with technical risks, and ensure the safe flow of cross-border data. For example, develop automated compliance inspection tools; use modern information technology to implement data classification and sensitivity assessment, and carry out real-time monitoring of sensitive data such as sensitive data in cross-border data circulation by abnormal data cross-border detection technology[9].

Strengthen the research and development and innovation of modern information technology, improve the security and controllability of data encryption, security authentication and transmission technology, and reduce the risk of cross-border data flow. First of all, strengthen technological innovation and application with the guidance of adhering to the overall national security concept, and coordinating security and development. Pay attention to the supervision and governance of cross-border data flow under the application of new technologies, use emerging technologies such as algorithms, artificial intelligence and other technologies to strengthen the grading and classification processing ability of data, enhance the security of data flow, and improve the efficiency of cross-border data flow. We can also use Blockchain and other technologies to ensure data integrity while realizing According to the cross-border transmission. Secondly, advanced encryption technology can be used to encrypt cross-border data using high-strength encryption algorithms to ensure the confidentiality and integrity of data during transmission, and regularly update encryption algorithms and keys to improve the security of data[10]. In addition, secure high-speed transmission protocols such as HTTP, QUIC, etc. can be applied for cross-border data transmission and regular evaluation and optimization, which can more effectively ensure the integrity and confidentiality of cross-border data in the flow process and improve the ability to prevent risks.

4.2. Promote the Relevant Training and Capacity Building of Technical Personnel

With the continuous progress of technology and the emergence of new tools, methods and standards, strengthening the research and development and practice of modern information technology is inseparable from the training of professional and technical personnel. Improving their ability not only helps technical personnel understand industry trends and adapt to industry changes, but also stimulate the creativity and innovative thinking of technical personnel. In addition, technical personnel analyze actual data cross-border compliance cases through practical learning, which helps to enhance the ability of technical personnel to manage cross-border data flow security and improve the level of talents in cross-border data flow management[11].

First of all, we should have an in-depth understanding of the actual needs of the cross-border data flow industry, absorb senior personnel from various fields, and target their professional training to ensure that they can cope with the complex and changing data environment. Secondly, set up practical courses. By simulating the actual cross-border flow scenario of data, let technicians experience it themselves and try to meet various data security and privacy protection challenges. In addition, industry experts can be invited to teach and share experiences and provide guidance for technical personnel. In addition, cross-border data flow involves multiple countries and regions. Technical personnel need to have good international vision and cross-cultural communication skills in order to better understand and cope with the data environment of different countries and regions. Finally, establish a training evaluation and ability testing system. Through regular evaluation of the learning achievements of technicians, we can understand their learning progress and mastery, so as to adjust the training content and method in time.

5. Conclusions

Cross-border data flow governance is not only a game of concepts and rules, but also a game of China's international discourse. China's improvement of cross-border data flow governance is also improving China's right to speak and introducing the world to the process of "China's plan" to participate in international rule governance. Under the overall national security concept, to maintain national security and improve China's right to speak in the governance of international cross-border data rules, it is necessary to establish a perfect cross-border data flow governance system, that is, the "China Plan", to maintain the security of cross-border data flow.

References

[1] The Publicity Department of the Central Committee of the Communist Party of China, Study Outline of Xi Jinping's Thought on Socialism with Chinese Characteristics for a New Era, People's Publishing House, Beijing, 2019, p.178.

[2] Ying Chen, Lan Xue, The evolution and trends of global cross-border data flow governance, Int. Econ. Coop. 40 (2024) 55-66+93.

[3] Xiang Li, An outline of national security law in the new era, China Leg. Sci. (2024) 144-163.

[4] Xin Li, Jianbin Su, Toward data good governance: A case study of earth science data governance, Sci. Bull. 69 (2024) 1149-1155.

[5] Jun Wang, Xiaolin Zhou, Yunyi Shen, et al., Current status, reflections, and prospects of cross-border scientific data flow governance, Sci. Bull. 69 (2024) 1846-1856.

[6] Qin Zhu, Yue Liu, International governance of cross-border data flows and China's exploration in the context of digital trade development, Sci. Technol. Manag. Res. 43 (2023) 151-157.

[7] Sihui Tang, Research on the protection of information fairness in the big data era: A rights-based perspective, China University of Political Science and Law Press, Beijing, 2017, p.9.

[8] Xiaodong Li, Shaoping Dong, Jing Wu, Path selection for data security governance under the perspective of overall national security, Forum Sci. Technol. China (2024) 147-157+167.

[9] Xiaobin Yu, Construction of a government data security framework, Cybersecur. Res. 8 (2022) 1061-1068.

[10] Yichang Song, Han Wu, A review of cross-border anomalous data monitoring technologies, Telecom World 31 (2024) 55-57.

[11] Jun Wang, Xiaolin Zhou, Yunyi Shen, et al., Current status, reflections, and prospects of cross-border scientific data flow governance, Sci. Bull. 69 (2024) 1846-1856.