

# The Research Review and Prospects of the Legal Issues of Cross-border Data Flow under the Holistic View of National Security

Linqi Li, Yujie Wang

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

---

**Abstract:** In order to give full play to the value of data, we should construct the governance of cross-border data flow according to the problems existing in the practice of cross-border data flow under the overall national security concept : improve the supervision system of cross-border data flow ; improve the classification system of cross-border data flow ; promote the legal protection of cross-border flow of personal information; establish an international cooperation mechanism for cross-border data flows ; describe the ' China blueprint ' for cross-border data flow governance. The research summary of the above problems is sorted out, and the prospects are expanded, and suggestions for improvement are put forward, to benefit the governance of cross-border data flow under the overall national security concept.

**Keywords:** Holistic View of National Security; Cross-border Data Flow; Data.

---

## 1. Introduction

In today 's era of globalization and digitization, data has rapidly become a key element of competition among countries and is regarded as a new generation of strategic resources after land, labor and capital. With the booming rise of the digital economy, the cross-border flow of data has become an irreversible trend. The free flow of data has improved the efficiency of resource allocation, promoted international trade and investment, and injected a strong impetus into global economic growth. However, the cross-border transmission of data has also brought unprecedented challenges, and problems related to citizens ' rights and interests and the bottom line of national sovereignty and security have occurred frequently. The report of the 20th National Congress of the Communist Party of China emphasizes that it is necessary to unswervingly implement the overall national security concept and to maintain national security throughout all aspects of the work of the party and the country. This concept requires the promotion of cross-border data flow to activate economic potential. At the same time, we must establish and improve a scientific and reasonable legal regulation system to effectively deal with security risks in the process of data flow.

In the overall national security concept, the " five overall plans " are emphasized. This paper will correspond the relevant legal issues in cross-border data flow with the five overall plans one by one. From the five dimensions of cross-border data flow supervision, legal protection of cross-border flow of personal information, data classification and classification, international cooperation mechanism, and cross-border data flow governance, this paper sorts out and summarizes the research literature on the legal issues of cross-border data flow under the overall national security concept.

## 2. Cross-border Data Flow Supervision System under the Overall National Security Concept

### 2.1. Cross-Border Data Flow Supervision Legislation

To build a scientific data cross-border flow supervision system, we should first improve the cross-border data flow supervision legislation to maintain data security, promote reasonable cross-border flow and promote international financial cooperation. The research on the supervision of cross-border data flow in China started late in China, but since the promulgation of the " Cybersecurity Law " in 2016, a large number of research results in this field have emerged one after another, mainly focusing on the extraterritorial data cross-border flow supervision rules, especially the specific system design of the EU, the United States, Japan and other countries and regions and the differences between countries, aiming to draw lessons from the experience that has reference significance for our country. There is a view that China should learn from some developed countries, such as the United States and the European Union, on the rules of cross-border data flow, and build a legal supervision mechanism for cross-border data flow. Most foreign literatures pay more attention to the interest distribution of developed economies such as the European Union and the United States in the cross-border flow of data, emphasize the strengthening of information technology advantages, expand ' long-arm jurisdiction ', and re-emphasize the dependence of countries on the regulatory system of cross-border flow of data in Europe and the United States. Few articles speak for developing countries or emerging economies. [1] Some scholars have proposed that there are two mainstream regulatory models for cross-border data flows in the world, the European Union and APEC, and any country participating in cross-border data flows must choose one of them.

However, in the current practice of cross-border data flow supervision, China has encountered many difficulties, such as insufficient coordination of regulatory basis, unclear review

and evaluation standards, etc. To solve these problems, China is striving to build a scientific and reasonable cross-border data flow supervision system. By improving legislation, emphasizing data security as the core, following the principle of giving priority to national security interests, and promoting the standardization of technical departments to indirectly improve the control of data flow; at the same time, a multi-level data regulatory framework has been established. On the one hand, China has initially formed a multi-level and all-round data regulatory framework, including the three basic laws of " network security law, " " data security law " and " personal information protection law, " as well as national standards and local and industry rules. These laws and regulations have clarified the basic principles of data protection, established a data classification and classification protection system, and strengthened data protection in key areas.

## **2.2. Full-chain Supervision of Cross-Border Data Flow**

Full-chain supervision refers to the comprehensive and systematic supervision and management of all aspects of cross-border data flow, ensuring that the entire life cycle from data collection, processing, transmission, storage to use is under effective supervision. The researchers not only deeply discussed the practice of data classification and hierarchical management, data localization storage and enterprise compliance in different countries and regions, but also put forward targeted strategies to solve the problems of data cross-border flow supervision in China. For example, it is pointed out that the differences in domestic regulatory models of core economies such as the United States, the European Union and China should be compared and analyzed from the three dimensions of industrial interests, regulatory focus and regulatory framework, to provide reference suggestions for China 's participation in cross-border data flow. Another point of view emphasizes that China should learn from the rules of cross-border data flow in developed countries such as the United States and the European Union and build a legal supervision mechanism that can not only protect national security but also promote the free flow of data. In addition, there are also studies that compare the differences in the rules of CPTPP (Comprehensive and Progressive Trans-Pacific Partnership Agreement) and RCEP (Regional Comprehensive Economic Partnership Agreement) on the issue of cross-border data flow and the reasons behind them, and explore the reasonable path for China to improve its cross-border data flow supervision system in this context.

Therefore, to promote the whole chain supervision of cross-border data flow, it is necessary to establish a unified cross-border data flow supervision model, which aims to solve the problem of unclear powers and responsibilities of the subject of review and evaluation. It is suggested to establish a unified and law enforcement authority, avoid conflicts between different departments, and give the network information department sufficient law enforcement authority, so that it can more actively participate in the data exit safety assessment, and improve the fairness and effectiveness of the entire assessment mechanism. To reduce the burden of enterprises and governments and improve the professionalism and objectivity of the assessment, it is also necessary to learn from the experience of the international organization CBPR system and Japan and introduce third-party professional institutions to conduct security assessment before data exit.

The establishment of a negative list system for cross-border data flow clarifies which types of data need special approval to be exported. Finally, strengthen the technical support of cross-border data flow, and explore the application potential of blockchain technology and artificial intelligence technology.

## **3. Legal Protection of Cross-Border Flow of Personal Information Under the Overall National Security Concept**

### **3.1. Legislation on Cross-Border Flow of Personal Information**

With the increasing attention to personal information protection and the rapid development of data trade, the research on cross-border personal information flow has gradually increased. Studies have pointed out that the institutional framework of cross-border personal information flow covers three dimensions: personal information privacy protection, corporate compliance, and international cooperation and competition, which constitutes a complex and extensive part of the personal information protection system. At the global level, there are three difficult choices for regulating personal information, that is, it is difficult to achieve data protection, cross-border data free flow and data protection autonomy at the same time. The policy shifts from free data flow to restricted data flow, which reflects the balance between the two legal interests of freedom and security. In data control, factors such as individual rights protection, national security, public order and economic development need to be considered. Since the cross-border protection legislation of personal information is still in its infancy in China, domestic research mainly draws on the relevant data protection legislation experience of the United States and Europe. The EU emphasizes compliance with its inherent data protection model in terms of data flow between the two parties and limits the amount of data flowing across borders to improve the level of data rights protection. [2]

Although China has achieved initial results in the legislation of cross-border flow of personal information, it still needs to be further deepened and improved. At present, basic laws such as the ' Network Security Law ' provide a basic framework for cross-border data flow, and detailed rules such as the ' Data Outbound Security Assessment Method ' and the ' Personal Information Outbound Standard Contract Method ' further refine the relevant rules. However, most of the existing regulations are principled and lack clear guidance at the specific operational level. Therefore, it is urgent to optimize the specific legislative regulation, refine the exit standards and methods, and strengthen the extraterritorial effect, so as to ensure that the specific operation process, safety assessment standards, professional organization certification standards and standard contract models of the cross-border flow of personal information are more clear, and consider introducing the concept of " personal information right " to give the subject of personal information a stronger foundation of rights.

### **3.2. Personal Information Outbound**

Since 2021, China has begun to strengthen the research on the legislation of personal information exit, with special attention to the security assessment system. It is pointed out

that the background of the ' security assessment approach ' is data security sovereignty, but there may be a risk of national security generalization. There are relatively few studies on standardized contract terms, but there are also views that the contract terms can not only restrain the import and export parties, but also have the function of protecting the third party. The standardized contract aims to build a trusted framework to coordinate the value contradiction between data security and data flow. In addition, there is also a point of view that in terms of the overall path balance of personal information exit, there is a dilemma in China 's data exit security system, which is mainly reflected in the unclear functional positioning of security assessment, standard contracts, professional certification and other systems, and the lack of cohesion in the content of the terms. Therefore, it is suggested that in the process of system construction, attention should be paid to the integration of internal and external rules to avoid the fragmentation and repetition of the security system caused by phased formulation. In terms of personal information outbound, relevant foreign literature mainly covers journal articles, supplemented by monographs and related reports, focusing on the differences in regulatory models between countries, and exploring international cooperation paths to promote cross-border data flows. [3]

Therefore, it is necessary to clarify the extraterritorial effect of legal norms, especially to supplement substantive provisions in the management activities before and after the exit of personal information, draw lessons from the EU 's ' adequacy determination ' rules, establish China 's ' white list ' system, include countries and regions that meet high data protection standards, and formulate a black list system to deal with the improper acquisition of personal information by other countries. In terms of global cooperation, China should uphold the concept of overall national security, actively seek international cooperation, implement China 's personal information protection certification ' whitelist ' system, and give priority to bilateral cooperation with ASEAN countries. Sign a memorandum of understanding, set up a unified data transmission format and standardized ' white list ' to ensure the traceability and interoperability of personal information outbound ; to build a ' China Program ' with internal and external linkages, while improving relevant laws and regulations at home, actively participate in international data governance, strengthen communication and cooperation with other countries and regions, and jointly promote the development of the global digital economy.

## **4. The Legal System of Cross-Border Data Classification and Classification under the Overall National Security Concept**

### **4.1. The Theoretical Framework of Cross-Border Data Classification and Classification**

At present, China 's research on cross-border data classification and classification is relatively scarce. The current research mainly focuses on the theoretical framework of data classification and classification system, and discusses its purpose, content and implementation methods. In terms of the purpose of data classification and classification, some views emphasize the important position of the system in national security protection and believe that its direct purpose

is to clarify the data characteristics and determine the level required for security. Another point of view points out that the data classification and classification system focus on the protection of data security, which is of great significance for the fine management and security protection of personal data. Other scholars believe that the data classification and classification system should pursue the dynamic balance between security protection and orderly flow, to further develop and strengthen the digital economy.

At present, although the ' State Council 's Opinions on Building a Data-based System to Better Play the Role of Data Elements ' put forward the requirements of exploring the classification and hierarchical management of cross-border data, China 's legal system in this field is still in the conceptual stage and needs to be improved urgently. Perfect legal system should establish five principles: scientific, clear, security, integrity and dynamic. These principles require setting standards based on inherent laws, ensuring clear boundaries, emphasizing national security priorities, considering the combined effects of data aggregation, and adjusting rules in a timely manner with technological development.

### **4.2. Rules for Classification and Grading of Cross-Border Data**

Regarding the content of data classification and grading rules, the existing research reveals the dual governance track of personal information and important data in parallel, which together constitute the rule system of data classification and grading system. The identification and catalogue of important data is the primary problem in the implementation process, which is very important to improve the implementation system of data classification and classification system. At the international level, most scholars ' research focuses on the realization path of personal data classification and grading, but the theoretical circle has not yet reached an agreement on this issue. For example, there is a view that personal data is divided into data associated with identified individuals and identifiable data. There is also a view that ' identifiability is temporary and unstable ', suggesting that the identifiable state of data may change as technology and environment change. A more radical view is that the classification boundary between personal data and non-personal data has begun to blur, and it is no longer necessary to deliberately distinguish between the two. These different perspectives reflect the profound understanding and continuous discussion of the complexity of personal data classification in the international academic community. In general, although scholars at home and abroad are trying to explore effective methods of data classification and grading, there are still differences on the specific implementation path and personal data classification standards. This shows that it still needs more research and practical exploration to construct a data classification and grading rule that is in line with international trends and can adapt to domestic needs. [4]

## **5. International Cooperation Mechanism of Cross-Border Data Flow under the Overall National Security Concept**

### **5.1. The Connection Between Domestic Regulations and Cross-Border Data Flow Rules under the RCEP Framework**

The existing research on the international cooperation of cross-border data flow mainly focuses on the data transmission rules in regional trade agreements. Researchers have conducted in-depth analysis of the data security and free flow provisions in Article 15 of the Regional Comprehensive Economic Partnership Agreement (RCEP) to which China is a party, explained the role of these provisions in China's data flow, and pointed out the importance of RCEP provisions in promoting electronic cross-border transmission of information. At the same time, some scholars put forward the specific path of China's participation in cross-border data transmission rules by comparing the Comprehensive and Progressive Trans-Pacific Partnership (CPTPP) and RCEP, emphasizing the necessity of establishing good interaction with neighboring countries and improving their own rule-making ability. At present, most of the research is from the perspective of economic development, and less combined with the overall national security concept to explore the governance of cross-border data flow.

As a developing country, China's legislation is conservative, emphasizing data localized storage and security assessment. However, with the signing of the Regional Comprehensive Economic Partnership Agreement (RCEP), China has also adopted its provisions on the free flow of cross-border data, aiming to balance the free flow of data and national security.

### **5.2. Build an International Cooperative Organization for TDF Regulation Along the Route**

As the international situation presents the characteristics of regional cooperation and multi-party co-governance, the United States, as one of the countries that proposed and regulated cross-border data flow issues earlier, its experience and lessons have attracted wide attention. The "Snowden" incident has revealed the security risks in cross-border data flows, making countries pay more attention to the contradiction between data security and free flow. How to resolve this contradiction to promote global governance and cooperation has become a research hotspot. Foreign scholars focus on analyzing the value and risk of cross-border data flows and their impact on international trade. Some people believe that cross-border data flows can provide more economic development opportunities for countries, so they call for attention to the formulation of relevant rules. Other studies have pointed out that with the advancement of technology, data localization may have adverse effects, especially in the relationship between data sovereignty and cross-border flows. In addition, after reflecting on the data flow measures of the United States and the BRIC countries, it is found that the United States tends to oppose data localization and advocate free data flow because of its advantages in data processing capabilities and intelligence monitoring. These studies not only reveal the complexity of

cross-border data flow, but also provide ideas for solving the contradiction between data security and free flow and promote global cooperation and governance in the field of cross-border data flow.

This paper believes that in the context of the "Belt and Road," China can build a TDF (Trade in Digital Financial services) along the route to regulate international cooperation organizations, establish a multi-coordinated law enforcement mechanism, and set operational rules based on flexible governance and soft law cooperation to build a legal regulation path for cross-border data flows in line with the actual situation of countries along the route. First, select countries with similar legislation to reach a bilateral cooperation mechanism first, form a normative experience and then gradually extend it to other countries to build common standards. Secondly, establish regulatory agencies and organizational arrangements, including forming a universal TDF regulatory framework, uniting members with similar willingness to create a China-led digital economic and trade organization, and selecting cities with active digital economic development as a contact point to drive countries along the line to participate in data governance. [5]

## **6. The Governance of Cross-Border Data Flow under the Overall National Security Concept is 'China's Blueprint'**

### **6.1. Top-Level Design of Cross-Border Data Flow Governance**

Scholars have extensively discussed the legal norms and improvement measures of cross-border data flow and emphasized the importance of governance issues. Some studies have pointed out that special legislation on data should be accelerated, and equal attention should be paid to data localization protection and cross-border data flow, to ensure the establishment of order and maintain free market transactions. China is actively building a cross-border data flow system that is linked to international high-standard economic and trade rules through the construction of laws and regulations and institutional innovation. There is no completely unified governance model in the world. There are many governance models, including the EU model oriented by human rights perspective and the American model oriented by market perspective. Each of them has its own emphasis on protecting personal data and promoting the free flow of data. It is argued that the risk of cross-border data flows has led to thinking about security governance, and the two main legislative models exist between the EU and APEC. The legal coordination and convergence of cross-border data flows can be achieved through the promotion or transplantation of legal principles of different countries by international organizations.

### **6.2. Cross-border Data Flow Governance Practice Plan**

At present, it is very important to strengthen the pilot promotion, explore the leading scheme of security governance in key areas, and further analyze the technology to improve the ability of security risk prevention. In the pilot of cross-border data flow governance in China's special regions, there is a view that it needs to be further strengthened. In order to improve the data compliance and governance capabilities of digital trade enterprises, promote high-level

international cooperation, and jointly formulate cross-border data flow governance rules, it is suggested that China should not only cooperate within RCEP members, but also consider joining agreements such as CPTPP to improve the data legislative framework and improve international voice. There are different characteristics and models in the governance of cross-border data flow at home and abroad. Through the construction of laws and regulations and institutional innovation, China is actively building a cross-border data flow system that is compatible with international high-standard economic and trade rules. There is no completely unified governance model in the world. There are mainly human rights-oriented EU model and market-oriented US model. These models have different emphases on protecting personal data and promoting the free flow of data.

The development of cross-border data flow governance pilot work aims to summarize a management model that is in line with national conditions and can be linked to international rules through practical exploration in specific industries or regions. At present, intelligent connected vehicles, biomedicine, public funds and other fields have become the focus of the pilot. These fields not only have urgent needs for cross-border data flow, but also have obvious industry characteristics. The pilot experience has replicability and promotion value. For example, the data list released by Shanghai Lingang New Area clarifies the data categories and fields, providing clear guidance for cross-border data flow. Through continuous optimization and improvement of relevant policies and regulations, combined with technological innovation and personnel training, China is striving to depict a 'Chinese blueprint' for cross-border data flow governance that meets the requirements of the times, not only to protect national security and development interests, but also to promote the prosperity and development of the digital economy.

## 7. Future Research Prospects

Looking forward to the future, with the continuous advancement of globalization and digitization, cross-border data flows will play an increasingly important role in international economic cooperation and national security.

China needs to further deepen and improve the governance mechanism of cross-border data flow under the guidance of the overall national security concept, to ensure that it cannot only meet the needs of national security, but also promote the effective use of data resources. To this end, China will continue to optimize the legal and regulatory systems related to cross-border data flows, accelerate the formulation and revision of special regulations, refine operational guidelines, enhance the enforceability and transparency of legal norms, and strengthen research on emerging technologies and application scenarios. Layout in advance to prevent potential risks. At the same time, China will further deepen international cooperation and exchanges, actively participate in discussions on international organizations and multilateral platforms, promote the formation of unified and coordinated global data governance standards, enhance mutual trust by signing bilateral or multilateral agreements, and establish stable cooperative relations, especially explore more flexible and effective cross-border data transmission models within the framework of the Belt and Road Initiative. Finally, based on the successful practice of the existing pilot areas, China will gradually expand the scope of the pilot and select more representative industries and regions to carry out the pilot work.

## References

- [1] Richard D. Taylor, Data localization: The internet in the balance. *Telecommunications Policy*, 2020(8), p44.
- [2] John Selby, Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both?. *International Journal of Law and Information Technology*, 2017(3), p213-232.
- [3] W. Gregory Voss. Cross-Border Data Flows, the GDPR, and Data Governance. *INTERNATIONAL ORGANISATI ONS RESEARCH JOURNAL*, 2022,5(17).
- [4] Aaronson, S.A. and Leblond, P: Another Digital Divide: The Rise of Data Realms and Its Implications for the WTO. *Journal of International Economic Law*, No.21, 2022.
- [5] Bergen K J, Johnson P A, de Hoop M V, et al: Machine learning for data-driven discovery in solid Earth geoscience. *Science*, No.3, 2019.