# Current Situation and Prospects for Governance of Cross Border Data Flow

Yu Wang[a], Yingyi Yao[b], Haijun Wang[*], Zongshuang Jiao[c], Yufei Wu[d], Linlin Zhou[e]

CATARC Intelligent and connected technology Co., LTd. No.68, East Xianfeng Road, Dongli District, Tianjin, China

[a]wangyu2023@catarc.ac.cn, [b]yaoyingyi@catarc.ac.cn,
[*]wanghaijun2019@catarc.ac.cn, [c]jiaozongshuang@catarc.ac.cn,
[d]wuyufei@catarc.ac.cn, [e]zhoulinlin@catarc.ac.cn

**Abstract.** With the booming development of digital trade, cross-border data flow has become a key factor driving economic development. Various countries have introduced regulatory rules for cross-border data flow to promote the safe, orderly, free and convenient flow of cross-border data. This article analyzes the current situation of cross-border data flow governance both internationally and domestically. Based on this, it summarizes the problems faced by China's cross-border data flow governance and proposes improvement suggestions, in order to enhance China's international competitiveness in data cross-border flow governance and promote the development of the digital economy.

**Keywords:** Cross border data flow, Data supervision, Data compliance, Data governance

## 1 Introduction

With the rapid development of information technology, digital trade has gradually become a new trend in international trade development and a new engine for trade growth. The prosperity of digital trade cannot be separated from the cross-border flow of data[1-2]. According to data from the World Trade Organization, in 2022, the scale of global cross-border data circulation increased by 120.6%, and the scale of digital service trade increased by 36.9%, both higher than the growth rate of global service trade and goods trade during the same period. Developing governance rules for cross-border data flow, ensuring the safe, orderly, free and convenient flow of cross-border data, has become the key to maintaining the sustained prosperity of digital trade.

This article focuses on the governance of cross-border data flow, analyzes the current situation of international and domestic data cross-border flow governance, and on this basis, summarizes the problems existing in China's data cross-border flow governance, and puts forward suggestions for improvement, in order to enhance China's

ICPDI 2024, September 06-08, Jinan, People's Republic of China

DOI 10.4108/eai.6-9-2024.2353626

international competitiveness in data cross-border flow governance and promote the development of the digital economy.

## 2 International Governance Status of Cross Border Data Flow

In response to the cross-border flow of data, various countries have introduced regulatory rules to promote the safe, orderly, free and convenient flow of cross-border data.

The General Data Protection Regulation (GDPR) issued by the European Commission in 2016 stipulates three ways for the cross-border flow of personal data[3]. The first is based on the sufficiency recognition mechanism (i.e. the "whitelist" mechanism), the second is based on binding company rules, standard contract terms, codes of conduct, certification mechanisms and other safeguard measures, and the third is based on legal exceptions such as data subject consent, fulfillment of contractual obligations, and protection of important public interests.

The United States has established a decentralized but rigorous regulatory system for the export of data in key areas. For example, in the field of foreign investment, the Foreign Investment Risk Review Modernization Act (FIRRMA) stipulates that foreign investments by US companies that maintain or collect sensitive personal data should be included in the security review scope of the Committee on Foreign Investment in the United States (CFIUS) if the US company meets the corresponding conditions and may grant specific rights to foreign investors[4]. On the other hand, the United States expands its overseas data retrieval rights through "long arm jurisdiction"[5]. The Clarifying Overseas Use of Data Act stipulates that the United States can access data stored overseas based on national security needs. Foreign companies may be required to provide data as long as they provide business in the United States and have sufficient contact with the United States[6].

On a global scale, there is no unified rule system for cross-border data governance, and different countries and regions mainly coordinate and manage cross-border data flows through bilateral or multilateral regional cooperation. The Regional Comprehensive Economic Partnership (RCEP) takes "free flow of data" as the fundamental principle and "secure flow of data" as the exception principle, balancing the free flow of data and full protection[7-8]. The Comprehensive and Progressive Agreement for Trans Pacific Partnership (CPTPP) regulates data issues from three aspects: personal information protection, cross-border transmission of information through electronic means, and the location of computing facilities[9]. The Data Privacy Pathfinder Agreement proposes for the first time the establishment of the APEC Cross Border Privacy Protection Rule System (CBPRs)[10].

# 3 Current Status for Governance of Cross Border Data Flow in China

## 3.1 The Institutional System of Cross Border Data Flow in China

Since 2016, China has gradually formed a data cross-border flow governance system with the Cybersecurity Law of the People's Republic of China, the Data Security Law of the People's Republic of China, and the Personal Information Protection Law of the People's Republic of China as the core, supported by regulations and guidelines such as the Data Export Security Assessment Measures, the Implementation Rules for Personal Information Protection Certification, the Standard Contract Measures for Personal Information Export, and the Rules for Promoting and Regulating Cross border Data Flow, as shown in Figure 1.

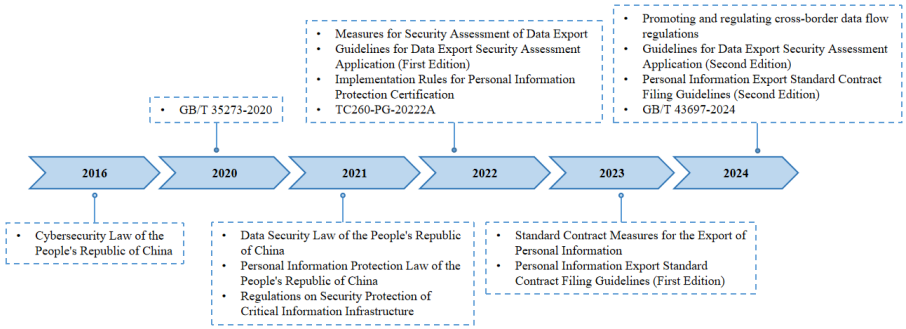


**Fig. 1.** The development history of China's cross border data flow supervision policies.

## 3.2 The Main Ways of Cross-border Data Flow in China

Based on the above laws and regulations, China has formed four cross-border data flow methods, including exemption methods, data export security assessments, personal information export standard contract filing, and personal information protection certification. Among them, the data export security assessment method is the strictest and most complex. Under the security assessment method, enterprises need to first conduct a self-assessment of data export risks on their own, and then apply for a national security assessment. In the self-assessment process of data export risk, the first step is to conduct a compliance assessment of the purpose of data export, and then evaluate the level of data export security risk.

The compliance assessment of data export purposes mainly considers three aspects: legality, legitimacy, and necessity, as shown in Table 1.

**Table 1.** Compliance Assessment Considerations.

| Evaluation aspects | Evaluation basis |
|---|---|
| A. legitimacy | $A_1$. Not explicitly prohibited by laws and regulations<br>$A_2$. Those who are not recognized as ineligible to leave the country by relevant |

| | |
|---|---|
| | departments such as the national cyberspace administration, public security, and security departments |
| B. rightness | $B_1$. The personal information subject has separately agreed. Although it is an emergency situation that endangers the safety of citizens' lives and property without the individual consent of the personal information subject.<br>$B_2$. Not violating the regulations of relevant regulatory authorities |
| C. necessity | $C_1$. Necessary for fulfilling contractual obligations<br>$C_2$. Necessary for conducting business within the company<br>$C_3$. Necessary for fulfilling relevant requirements proposed by government departments in our country |

The calculation method for the legitimacy evaluation value L is shown in equation (1).

$$L = (A_1 \& A_2) \& (B_1 \& B_2) \& (C_1 | C_2 | C_3) \quad (1)$$

Among them, the values of $A_i$, $B_i$, and $C_i$ are 0 or 1

If the compliance evaluation value L is set to 1, the data export security risk level assessment steps can continue; If the value is 0, the enterprise is not allowed to carry out this data export activity.

The risk level assessment of data export security mainly considers two aspects: the possibility of security incidents occurring and the degree of impact on rights and interests. Based on factors such as the security capabilities of data processors, data recipients, legal environment and contractual agreements, and data security control measures, the likelihood of data security incidents occurring can be evaluated. The probability analysis of data security incidents can be conducted based on a percentage system, and the risk occurrence probability score value can be given according to the score interval, as shown in Table 2.

**Table 2.** Probability Levels of Data Security Incidents.

| Level | Score |
|---|---|
| High | [75%,100%] |
| Medium | [30%,75%） |
| Low | [0%,30%） |

Based on factors such as data sensitivity, data magnitude, data range, and data processing techniques, the degree of impact on equity can be evaluated. Quantitative analysis of the degree of equity impact can be conducted based on a percentage system, and the score value of equity impact can be given according to the score interval, as shown in Table 3.

**Table 3.** Equity affected level.

| Level | Score |
|---|---|
| Very high | [80%,100%] |
| High | [60%,80%） |
| Medium | [40%,60%） |
| Low | [20%,40%） |
| Very low | [0%,20%） |

Taking into account both the possibility of data security incidents and the degree of impact on rights and interests, the level of data export security risk can be evaluated. The calculation formula is shown in equation (2).

$$R = P \times M \tag{2}$$

Among them, P is the score value of the likelihood of data security incidents occurring, M is the score value of the degree of equity impact, and R is the score value of data security risk assessment.

According to the R value, the level of data security risk can be determined, as shown in Table 4.

**Table 4.** Data security risk level.

| The value of R | Data security risk level |
|---|---|
| [60%,100%] | Very high |
| [50%,60%) | High |
| [40%,50%) | Medium |
| [20%,40%) | Low |
| [0,20%) | Very low |

If the data security risk level is moderate or below, the enterprise can apply for a national security assessment; If the data security risk level is above medium, the enterprise needs to carry out rectification, and after the rectification is completed, a risk self-assessment needs to be conducted again.

# 4 The Problems and Challenges Faced by the Governance of Cross Border Data Flow in China

## 4.1 The Cooperation Network for Cross-border Data Flow Needs to be Expanded

In order to reduce obstacles to cross-border data flow, countries such as the United States and Europe have been trying to establish cross-border data flow rules that are in line with their own interests and establish a data cross-border flow cooperation network in the Western world. In contrast, the connection between China's cross-border data flow rules and international high standard rules and data cross-border governance rules of other economies is still insufficient, and a broad network of data cross-border flow cooperation has not yet been formed. Therefore, there is a lack of leadership and discourse power in the formulation of global data cross-border flow rules. This situation to some extent restricts the operation and development of China's digital trade enterprises in the international market.

### 4.2 The Innovation of Regulatory Policies for Cross-border Data Flow in Special Regions is Slightly Insufficient

With the rapid growth of digital trade, the demand for offshore data centers is becoming increasingly significant. Although China has established a negative list system for cross-border data flow in free trade pilot zones, the pilot supervision of cross-border data free flow in special areas such as free trade zones and Hainan Free Trade Port still needs to be deepened, especially for low latency and high-frequency data flow scenarios required for cross-border business. Relevant special regulatory measures still need to be further optimized and improved. Regarding the establishment of an offshore data supervision policy similar to a "data embassy", which is a data management area that enjoys special status both domestically and internationally and is exempt from conventional domestic supervision, the specific policy framework and implementation details still need further research and exploration.

### 4.3 The Increasing Demand for Cross-border Data Flow Exacerbates the Risk of Data Leakage

With the deployment and implementation of strategies such as "the Belt and Road" and "going global", business activities such as overseas listing of domestic enterprises, establishment of overseas branches, overseas mergers and acquisitions, and cooperation with overseas enterprises have become increasingly frequent, and the demand for cross-border data flow has significantly increased. Cross border data flow has the characteristics of long transmission chains, and with the increasing frequency of cross-border data transmission, data is more prone to leakage, posing security risks to countries and enterprises. Although most enterprises have taken technical measures to protect data security, cross-border data attack technologies have also been upgraded, significantly increasing the cost of enterprise data security protection.

## 5 Reflection and Outlook

### 5.1 Exploring the Establishment of a Whitelist Mechanism for Cross-border Data Flow

The whitelist mechanism is an important means to facilitate cross-border data flow channels. Countries and regions such as the European Union and Russia have all used whitelist supervision mechanisms in cross-border data flows. China can learn from the experiences of these countries and regions, establish a whitelist system that is in line with China's national conditions, facilitate cross-border data flow channels, and appropriately relax restrictions on cross-border data flow. For example, countries and regions along the "the Belt and Road" can take the lead in signing special bilateral agreements on cross-border data flow to promote the free cross-border flow of data with countries along the "the Belt and Road".

### 5.2 Actively Promote Bilateral and Multilateral Negotiations on Cross-border Data Flows

At present, a unified system of cross-border data rules has not been formed globally. Western countries such as the United States and Europe are actively collaborating with partners to build a cross-border data flow circle. In order to grasp the discourse power of international rule making, China should increase the negotiation content of cross-border data flow in various bilateral and multilateral trade negotiations. While respecting the legal systems of various countries, based on the unified principle of cross-border data flow, we should promote the formation of jointly recognized mechanisms such as data protection certification and standard contract terms, and achieve free cross-border data flow within the region.

### 5.3 Strengthen the Innovation of Regulatory Policies for Cross-border Data Flow in Special Regions

For the Shanghai Free Trade Zone Lingang New Area, Hainan Free Trade Port, Beijing Digital Trade Demonstration Zone, Guangdong Hong Kong Macao Greater Bay Area and other areas, we should fully leverage the policy innovation advantages of these regions, establish offshore data centers similar to domestic and international customs for data in cross-border trade, e-commerce, finance, pharmaceutical research and development, and achieve free and convenient flow with foreign countries, exempt from existing domestic legal supervision, and establish special offshore data supervision systems for special regions to better serve cross-border economic and trade cooperation.

### 5.4 Improve the Security Guarantee Capability of Cross-border Data Flow

Security is a prerequisite for cross-border data flow. The transmission of data overseas may bring various uncontrollable risks, such as data leakage, data abuse, etc., posing a threat to national security. Therefore, while promoting cross-border data flow, it is necessary to enhance the security guarantee capability of cross-border data flow. Government departments, cross-border enterprises, security institutions, and other entities can collaborate to build a data cross-border flow security threat perception and monitoring early warning infrastructure, coordinate the acquisition, analysis, analysis, judgment, and early warning of data security threat information, strengthen the sharing of data security threat information, and form technical capabilities such as rapid response to data security events, tracking and tracing malicious behavior.

## 6 Conclusion

As a product driven by the digital economy, cross-border data flow inevitably brings national security risks while promoting global economic development. In order to balance development and security, various countries and regions have formulated

unique cross-border data flow supervision models based on their local conditions. This article analyzes the current situation of cross-border data flow governance both internationally and domestically. Based on this, it summarizes the problems faced by China's data cross-border flow governance and proposes suggestions for exploring the establishment of a data cross-border flow whitelist mechanism, actively promoting bilateral and multilateral negotiations on data cross-border flow, strengthening innovation in data cross-border flow supervision policies in special regions, and improving the security guarantee capacity of data cross-border flow. The aim is to enhance China's international competitiveness in data cross-border flow governance and promote the development of the digital economy.

## References


1. Gewin, V. (2016) Data sharing: An open mind on open data. Nature, 529: 117-119.
2. Wugmeister, M., Retzer, K., Rich, C. (2007) Global Solution for Cross-Border Data Transfers: Making the Case for Corporate Privacy Rules. Georgetown Journal of International Law, 38(3):449-498.
3. Hong, Y. Q. (2024) The "Rebalance" of China's Data Export Security Management System: From the Perspective of National Data Competition Strategy. China Law Review, 03: 201-212.
4. Li, J., Zhao, R. J., Fan, Y. Q. (2023) Effectiveness, Problems and Improvement Suggestions of Cross-border Data Flow Governance in China. International Business Research, 06: 84-95.
5. Mei, A., Pan, Z. J. (2024) Governance Models, Challenges and Compliance Approaches for Cross Border Data Compliance of Enterprises. Information Studies: Theory & Application, 1-9.
6. Liang, Y. N. (2023) Corporate Data Compliance Governance: From Personal Data Protection to Cross border Data Flow. Social Scientist, 12: 81-85.
7. Hong, Z. G., Huo, J. X. (2022) RCEP's regulation on cross-border data flow and its important impact. Southwest Fin, 4: 83–94.
8. Ma, H. T. (2024) Review of Rules for Cross border Data Flow in RCEP and China's Response. Foreign Economic Relations & Trade, 06: 30-33.
9. Xie, Z. J., Yang, S. D. (2021) Regulation of Cross border Data Flow in Global Governance and China's Participation: A Comparative Analysis Based on WTO, CPTPP, and RCEP. International Review, 5: 98-126.
10. Ma, G. (2024) Research on the Coordination of Cross border Data Transmission Rules and International Rules in China. Journal of CUPL, 02: 227-239.