THE SIGNIFICANCE AND CHALLENGES OF LEGAL REGULATION OF CROSS-BORDER FLOW OF PERSONAL INFORMATION FROM THE PERSPECTIVE OF NATIONAL SECURITY

Wang Cong
Doctoral Student at the University of World Economy and Diplomacy, Tashkent 100174, Uzbekistan, Suqian University, Suqian 223800, China

Abstract:
As the wave of digitalization sweeps the world, the cross-border flow of personal information has become an important link supporting global economic activities. However, the national security risks associated with this process are increasingly valued by countries. How to effectively maintain national security while promoting the free flow of data has become a core issue in legislation and policy making in the current international community. This article explores the significance of legal regulation of cross-border flow of personal information and the practical challenges it faces from multiple dimensions, including data sovereignty, geopolitical game, systemic risk prevention, international rules game, and balance between security and development, and proposes strategies and suggestions for defending data sovereignty in the future.

Keywords: National security Personal information Cross-border flow Data sovereignty.

INTRODUCTION

The cross-border flow of personal information has become a core carrier of global economic connectivity, but the national security risks it has caused are also becoming increasingly prominent. Personal information is not only a manifestation of personal personality rights. Through technical analysis, the freely flowing personal information can also about a country's social conditions and economic level, causing national information security risks. The analyses of personal information are 9 entirely possible to infringe on the country's traditional sovereignty. From Russia's "data localization" legislation to the EU's GDPR adequacy recognition mechanism, [1] from the United States' "Cloud Act" to China's "Data Security Law", countries are building a "digital sovereignty moat" through legal regulations. This legal action is not only a response to individual privacy rights, but also an inevitable choice to maintain national security and resist systemic risks. Personal information security is highly related to national security, and data information security has been integrated into the national security system. [2]

ANALYSIS AND RESULTS

1. Data sovereignty is the legal foundation of national security

As the legal foundation of national security, data sovereignty has become a core issue in global digital governance. In the context of globalization and digitalization, cross-border data flows not only promote economic development, but also trigger sovereignty games. The theory of data sovereignty refers to the fact that a country or region has legal jurisdiction and control over data generated, stored and circulated within its territory, ensuring data security, privacy protection and national security from external interference. [3] This theory originates from the extension of the traditional concept of national sovereignty in the digital age. It emphasizes the political, economic and security attributes of data as a strategic resource and is the key to maintaining a country's strategic autonomy in cyberspace. The European Union established the principle of "data localization" through the General Data Protection Regulation (GDPR), while the United States advocated jurisdiction over overseas data through the CLOUD Act, reflecting the sovereignty claims under different governance models. The United Nations Roadmap for Digital Cooperation emphasizes that countries have the right to autonomously manage data within their territory, but they need to balance the relationship between security and development, openness and autonomy. [4] Developing countries are particularly exposed to the risk of data colonialism and need to pass legislation to prevent key data from being monopolized or abused. The international community is competing for rules around data sovereignty, which is essentially an extension of the principle of equality of state sovereignty in the digital age. In the future, building a global data governance framework that balances security and cooperation will be a key challenge to maintaining the stability of the international order.

2. Challenges to national security posed by cross-border flow of personal information

Regulation of cross-border flow of personal information is increasingly becoming a strategic tool for geopolitical games between major powers. The technological competition between China and the United States is particularly prominent in this area. The U.S. Cloud Act authorizes law enforcement agencies to retrieve server data stored abroad across borders, while Article 36 of China's Data Security Law clearly stipulates that "without the approval of the competent authorities of the People's Republic of China, data stored in the territory of the People's Republic of China shall not be provided to foreign judicial or law enforcement agencies" [5]. This direct confrontation in legislation actually reflects the deep intention of both sides to compete for the dominance of digital governance rules.

Rule output and countermeasures constitute the other side of the game. The EU implements the export of its data protection standards through the "adequacy recognition" system. Currently, 15 countries/regions have obtained data transfer whitelist qualifications. If countries that fail to obtain recognition want to obtain EU data, they must accept data

protection standards equivalent to GDPR. In response, Article 42 of China's Personal Information Protection Law establishes the "principle of reciprocity", which stipulates that if other countries adopt discriminatory prohibition or restriction measures against China, China has the right to take reciprocal measures to suspend the provision of data to them. [6]

The global data governance landscape is showing a trend of camp formation. The US-led Cross-Border Privacy Rules (CBPR) system and the EU-Japan data flow circle have formed a competing regional framework. It is worth noting that the Indo-Pacific Economic Framework launched in 2024 bundles the free flow of data clauses with military cooperation, attempting to build an exclusive digital alliance. This trend of differentiation forces countries to clarify the scope of their "data allies" through legislation to prevent strategic opponents from infiltrating their key areas through data links.

Data leaks in key industries may also have a serious impact on the lifeline of the country's economy. The hacker attack on Statoil is an example. The cause was that its contractor processed the data of North Sea oil field employees through an overseas cloud platform, resulting in the exploitation of a vulnerability in the drilling platform control system. This incident directly prompted Norway to revise the National Security Law and raise the security assessment level of energy industry data outbound to the highest level. [7]

The compliance of cross-border data service providers is directly related to national security. During the Ukrainian war in 2022, Russia passed legislation to force payment institutions such as Visa and Mastercard to store user data within the country, successfully resisting the potential risk of financial data supply interruption under Western sanctions. Such "data chain disconnection" plans are increasingly becoming an indispensable part of the modern national security system.

In summary, the current global data flow regulation faces three core paradoxes:

First, there is a tension between the economic benefits of free flow of data and the need for sovereign security. For example, although India's decision to ban TikTok was based on security considerations, it caused local companies to lose about $2 billion in market opportunities.

Second, the deterrent effect of long-arm jurisdiction has exacerbated the fragmentation of global rules. The conflict in jurisdiction between the EU GDPR and the US Cloud Act has significantly increased the compliance costs of multinational companies.

Finally, the open demand for technological innovation often conflicts with the conservative tendency of risk prevention and control, which is particularly evident in the cross-border scientific research sharing and privacy leakage risks of biometric data.

3. Find response strategies in the balance between security and development

Countries actively use flexible mechanisms to safeguard security interests under the framework of international rules. For example, in the negotiations to join the Comprehensive

and Progressive Agreement for Trans-Pacific Partnership (CPTPP), China cited the national security exception clause in Article 14 of the World Trade Organization's General Agreement on Trade in Services (GATS) to implement local storage requirements for sensitive data such as population health and geographic information, while following international rules and maintaining the bottom line of security.

Cross-border law enforcement cooperation models are also constantly innovating. In 2023, the Data Access Agreement signed by the United States and the United Kingdom pioneered the permission for law enforcement agencies of the two countries to directly access the data of cloud service providers in each other's territory, bypassing the lengthy procedural restrictions of traditional mutual legal assistance treaties. This mechanism, known as the "digital extradition treaty", is reshaping the pattern of international law enforcement power.

Regional cooperation mechanisms show great potential. The Digital Economy Framework Agreement (DEFA) launched by ASEAN in 2024 created a "joint risk assessment pool" to promote member countries to share data outbound risk intelligence and implement mutual recognition of certification bodies. This regional security community model has significantly enhanced the overall defense capabilities of member countries.

To solve these difficulties, countries are actively exploring innovative governance tools. The "data sandbox" mechanism launched by Singapore allows cross-border data flows in specific scenarios to be tested in the regulatory sandbox, providing space for financial technology companies to avoid policy uncertainties. Brazil's General Data Protection Law innovatively introduces a "dynamic adequacy assessment" mechanism, requiring a review of the data protection level of other countries every two years to adapt to the rapidly changing technological environment. These practices show that national security should not be an excuse for digital protectionism, but a dynamic rebalance between security and development should be achieved through precise and flexible regulatory paths.

Conclusion

The legal regulation of cross-border flow of personal information is essentially a strategic move to reconstruct the depth of national security defense in the digital era. The construction of the future national security system will show two major development trends:

First, dynamic defense enabled by technology will become the key. For example, the "Privacy Enhancement Technology Compliance Certification" (PET) being tested by the European Union aims to achieve "available but invisible" data through the application of technologies such as homomorphic encryption, thereby reducing the risk of leakage from a technical level. [8]

Second, the elastic boundaries of rule interoperability will become increasingly important. Similar to the expansion of the Asia-Pacific Economic Cooperation (APEC) Cross-Border

Privacy Rules (CBPR) system, by establishing a mutual recognition mechanism under a common security framework, it will help significantly reduce compliance frictions in cross-border data flows.

Only by firmly defending the core security interests of the country while maintaining the openness and inclusiveness of the rules can we build a sustainable national security ecology in the surging wave of digital globalization.

REFERENCES

1. Russia's 2015 "Personal Data Law" requires that citizens' data must be stored on domestic servers, successfully preventing American technology companies from unlimited access to Russian social network data. This regulation prevents data resources from becoming "digital colonies" and prevents key information from being used by external forces to manipulate public opinion.

2. Xiong Guangqing, Zhang Sumin. "Improvement of my country's Data Outbound Security Management System from the Perspective of the Overall National Security Concept"[J], Journal of Harbin Institute of Technology (Social Sciences Edition), 2023, No. 5, p. 32.

3. Lessig, L. (2006). Code: And Other Laws of Cyberspace, Version 2.0. Basic Books.

4. "Digital Cooperation Roadmap of the Secretary-General of the United Nations", https://www.un.org/zh/content/digital-cooperation-roadmap/, June 10, 2025.

5. Article 36 of China's "Data Security Law".

6. Article 42 of China's "Personal Information Protection Law".

7.Combatting Cyber-Attacks In The Oil And Gas Industry, https://www.foxbusiness.com/markets/combatting-cyber-attacks-in-the-oil-and-gas-industry, June 15, 2025.

8. Ethereum privacy proposal proposes GDPR-compliant modular architecture, https://news.qq.com/rain/a/20250609A090ZQ00, June 12, 2025.