Proceeding of ICGPSH 2025 Symposium: The Globalization of Connection: Language, Supply Chain, Tariff, and Trade Wars
DOI: 10.54254/2753-7048/2025.LD24116

Dilemma of Legal Application and Difficulty of Law Enforcement Cooperation in Cross-border Data Flow

Yuying Hou

School of Humanities, Donghua University, Shanghai, China
houyuying@mail.dhu.edu.cn

Abstract: Cross-border data transfers have sparked legal disputes and regulatory difficulties while simultaneously advancing the expansion of the digital economy. This article explores the legal conflicts and law enforcement cooperation dilemmas in cross-border data flows from the perspective of the offense of violating the privacy of citizens in China's Criminal Law. This article uses theoretical analysis and comparative analysis to analyze data sovereignty theory, international flow of production factors theory, privacy rights theory and global governance theory, compares the regulatory rules of the United States, the European Union, Russia and China, and reveals the difficulties China faces in cross-border data flow law enforcement cooperation. This article proposes that China should improve its domestic legal system, add extraterritorial effect clauses, strengthen the research and development of data security technologies, and actively take part in the creation of global regulations to meet the challenges of cross-border data flows. Building an effective regulatory framework and balancing the free flow of data and the protection of personal information is of great significance to achieving sustainable development of the global economy and digital economy.

Keywords: cross-border data flow, legal conflict, personal information protection, law enforcement cooperation, data sovereignty

1. Introduction

As the global informatization process continues to accelerate, data has become a core element of production and trade. The cross-border flow of data not only promotes the prosperity of the global economy and digital economy, but also provides unprecedented opportunities for countries in scientific and technological innovation and security assurance. Against this backdrop, countries are committed to building efficient systems for cross-border data movement, storage and processing in order to fully unleash the potential of data-intensive technologies and cloud computing solutions.

However, while cross-border data flows create huge economic benefits and promote global collaboration, they also raise serious legal and regulatory challenges. First, there is an obvious mismatch between the rapid development of data flow and the existing regulatory system, and countries face fundamental contradictions in balancing the free flow of data with maintaining national security and protecting citizens' privacy. Secondly, the continued widening of the digital divide has created numerous obstacles for the international community in formulating unified regulatory standards. Countries have adopted diverse and even fragmented regulatory measures out of their own

DOI: 10.54254/2753-7048/2025.LD24116

interests. A set of universally binding cross-border data regulatory rules has not yet been formed at the international law level, resulting in a fragmented and lagging global data governance.

In this context, how to build a regulatory framework that can both cope with the rapid development of technology and effectively protect citizens' personal information while ensuring the free flow of data has become a major issue that needs to be addressed urgently. Especially in domestic legal practice, how to effectively connect international regulatory dilemmas with domestic laws and regulations is a major challenge facing legislators and law enforcement agencies. Because of this, the offense of violating the personal information of citizens, as defined by Article 253 of the People's Republic of China's Criminal Code, has emerged as a crucial legal link between the concerns of domestic and foreign data flow oversight.

Therefore, this article will take the crime of infringing on citizens' personal information as the starting point to explore the legal conflicts and law enforcement difficulties that exist in domestic and foreign regulatory systems in the context of the big data era, and try to provide institutional suggestions for resolving this contradiction.

2. Theoretical basis for the regulation of cross-border data flows

With the rapid development of the digital economy, data has transformed from a traditional production product into a core production factor. Its cross-border flow has not only optimized global resource allocation, but also brought unprecedented regulatory challenges. This section will explore the theoretical basis for building a cross-border data regulatory system from the following four theoretical perspectives.

2.1. Data sovereignty theory

The core of data sovereignty theory is national sovereignty in cyberspace [1] or the supreme control of national data within the country [2]. At present, there are significant differences in the understanding of it among countries: the EU takes the protection of basic rights as its basis and regards digital sovereignty as a strategy to deal with competition from transnational digital platforms [3]; China regards data as a strategic asset and emphasizes strengthening control to achieve "strategic autonomy" [4]; some developing countries, on the basis of drawing on the above-mentioned concepts, take into account both technology introduction and information security [5]. Scholars have different interpretations of the connotation of data sovereignty. Some view it as limited to national sovereignty, while others advocate extending it to citizens' right to self-determination of personal data [6]. This article argues that data sovereignty should include the country's comprehensive control over data storage, use and cross-border flow. When formulating data policies, the country must take into account economic benefits, information security and privacy protection to guarantee that the country's and its residents' basic interests are not harmed by the worldwide flow of data.

2.2. Theory of international mobility of production factors

The theory of international flows of production factors originated from classical economics. With the development of globalization and information technology, data as a new type of production factor has become a key driving force for economic development. Theory points out that differences in resource endowments among countries prompt the global flow of production factors to achieve optimal allocation. The cross-border flow of data accelerates technological innovation and industrial upgrading, and changes the economic competition landscape among countries, but it also exposes problems such as lagging supervision and insufficient risk control. Data policy formulation varies significantly across countries, with some pursuing the free flow of information and others emphasizing data security and privacy protection. Therefore, this theory believes that when

DOI: 10.54254/2753-7048/2025.LD24116

explaining the phenomenon of data flow, it is necessary to take into account economic interests, legal and institutional constraints, and provide theoretical support for the establishment of a reasonable data supervision system.

2.3. Privacy theory

The theory of privacy rights originates from modern liberalism and individualism, and aims to protect the peace of citizens' private lives and information security. Under digitalization, the connotation of online privacy rights has expanded to include the right to know, the right to choose, etc. The academic community believes that a balance should be struck between information flow and personal privacy protection in the online environment. Countries have established a legal framework through legislation and judicial practice to ensure information security without hindering data flow. Strengthening personal information protection while promoting the evolution of the digital economy is an important theoretical support for building a cross-border data regulatory system. Privacy rights theory provides a legal basis and value guidance for data governance.

2.4. Global governance theory

Global governance theory aims to address cross-border and cross-sector global issues, with its core being to achieve effective management through multilateral cooperation and pluralistic systems. This theory holds that while maintaining sovereignty, countries should also participate in international cooperation to formulate cross-border data supervision rules. In the early days, it focused on the role of non-state actors, but in recent years, collaborative cooperation between countries has become the mainstream. When exploring data governance models, the international community relies on legal constraints and supplements them with market and social mechanisms, striving to strike a balance between free flow and security supervision. Global governance theory provides a new perspective and method for regulation of cross-border data, and the evolution of its connotation is of great significance to building a global regulatory system that meets the needs of the information age.

In summary, controlling the movement of data between borders involves multiple dimensions such as national sovereignty, economic interests, personal privacy and global governance. These theories not only provide theoretical support for improving the data supervision system, but also lay a solid foundation for the subsequent discussion of specific regulatory rules.

3. Comparison of regulatory rules on cross-border flow of personal data among countries

3.1. US personal data flow regulation oriented towards trade freedom

The cross-border data movement in the United States regulatory rules are mainly aimed at promoting market competition and innovation. They adopt a free market economic model, adopt a relatively loose framework for controlling data flows across borders, and emphasize maintaining global digital market leadership through private market-driven efforts. The United States supports an open, interoperable, and secure Internet environment and promotes the free flow of data [7], striving to further enhance the global competitiveness of its digital economy by expanding market share and collecting more data. Under this framework, although there are no strict criteria for compliance when sending personal data across borders, strict localization requirements are adopted for data closely related to national security. For example, the United States has strengthened controls over sensitive data through the Foreign Investment Risk Review Modernization Act [8]. In particular, restrictions have been imposed on telecommunications companies, applications and cloud services from certain countries in an effort to protect national security [9]. Therefore, although The United States supports

DOI: 10.54254/2753-7048/2025.LD24116

unrestricted data flow., it has imposed strict restrictions on the supervision of national defense and sensitive data [10].

3.2. EU personal data flow regulation rules oriented towards human rights protection

The EU's data flow regulatory rules originated in Europe in the 1970s and still focus on personal data protection. They adopt a location-based regulatory approach and require that before data is transferred to other countries, the receiving country's data protection level must comply with EU standards, especially the "adequacy protection" principle. Based on this principle, the EU has established strict regulatory standards for cross-border data flows to ensure that the rights of data subjects are protected [11]. Although this regulatory model can provide a certain degree of legal foresight, there are several problems in actual operation: first, the procedure for evaluating the "adequate protection level" is cumbersome and time-consuming; second, the judgment of whether it meets the "adequate protection" is often influenced by political factors, resulting in a lack of objectivity in the judgment criteria. The EU has strengthened the enforcement of data protection through GDPR, but this model may also hinder cross-border data flows, especially when data protection standards are not unified, which may trigger more international disputes. Therefore, while the EU's cross-border data flow regulatory model helps protect citizens' privacy, there are still certain challenges in striking a balance between guaranteeing data security and encouraging the unrestricted flow of global data.

3.3. Russia's personal data flow regulation rules oriented towards data localization

Russia has imposed more stringent regulations on cross-border data transfers than the US and EU, which have more lenient or balanced regulatory structures. According to the Russian Federation Personal Data Law, Russia requires domestic companies to localize personal data and limit the movement of data across borders [12]. The latest legal amendments require Russian companies to report to regulators before transferring data across borders, and data can only be moved to particular nations or areas. In addition, Russia also stipulates that regulators can completely ban or restrict the cross-border transfer of certain data for national security, public interest or other special reasons [13]. Such regulations are intended to strengthen the protection of national security and citizens' personal privacy, and to ensure that external data inflows do not pose a threat to domestic interests. Due to Russia's high level of legal and policy control, the free flow of cross-border data is greatly restricted, especially when it comes to sensitive information and national security. Data localization has become an important part of national security policy.

4. Features of China's legislation on cross-border flow of personal data

China is accelerating the development of a cross-border flow management system of personal data. Since the publication of the "Information Security Technology - Guidelines for the Protection of Personal Information in Public and Commercial Service Information Systems" back in 2012, the relevant legal system has been continuously improved and gradually moved towards institutionalization and standardization. The 2017 "Cybersecurity Law" clarified for the first time the security assessment requirements for the outbound flow of critical information infrastructure data, and created a fundamental regulatory framework for the outflow of data; the 2019 "E-Commerce Law" made provisions for the safeguarding of private data and the unhindered and efficient exchange of e-commerce information; the 2020 "Civil Code" further protected the security of personal information from a civil law perspective, emphasizing the rational use of data resources while protecting privacy.

In addition, the successive introduction of the "Data Security Law" and the "Personal Information Protection Law" has made China's legal system for the international transfer of personal information

DOI: 10.54254/2753-7048/2025.LD24116

more mature. To implement the above legal spirit, the national cyberspace administration has successively issued the "Measures for Data Cross-Border Security Assessment", "Personal Information Protection Certification Implementation Rules" and "Standard Contract Measures for Personal Information Cross-Border", forming a relatively complete system and further clarifying operational norms.

In this context, a legislative framework crucial to my nation's cybersecurity, data security, and personal information protection laws has created a fundamental regulatory framework for the cross-border movement of personal data. According to Article 38 of the Personal Information Protection Law, the export of personal data must meet three core elements. First, the export of data must comply with legal procedures, including passing the security assessment of the national cybersecurity and informatization department, passing the certification body certification, or signing a standard contract with the overseas recipient. One of the three is applicable, and there is no requirement to implement them in combination. At the same time, other legal bases such as international treaties or agreements may also be applicable. Second, overseas recipients should ensure that data processing standards are no lower than domestic standards, reflecting my country's dual-dimensional regulatory approach for data outbound transfer: on the one hand, assessments are made based on the receiving nation's degree of protection, and on the other hand, data recipients are ensured to comply with corresponding institutional requirements. Third, cross-border data transmission requires the data subject's individual consent. Article 39 of the Personal Information Protection Law clearly stipulates that data subjects must make separate and clear authorization for the export of their personal information abroad to ensure that their rights to know and choose are protected.

In addition, the crime of violating residents' personal information, as defined by Article 253 of the Criminal Law of the People's Republic of China, is intimately related to the cross-border personal data supervisory system in my nation. This crime not only reflects China's emphasis on protecting personal data of citizens, but also, To a certain degree, reflects the legal consequences that may be faced in cross-border data flows. If data is exported abroad without performing a security assessment in accordance with the law, without ensuring the protection standards of the recipient, or without obtaining the consent of the data subject, it may constitute illegal processing of personal information and may be suspected of violating personal data of citizens.

The crime of violating personal data of citizens includes stealing or unlawfully obtaining citizens' personal information through other means, as well as breaking applicable national regulations by selling or giving away citizens' personal information to third parties or by selling or giving away citizens' personal information acquired while performing duties or rendering services. The legal interest protected by this crime is the citizens' right to personal information, and its purpose is to prevent personal information from being improperly collected, disseminated or abused, thereby protecting the privacy and identity security of citizens.

The crime consists of three types of situations: first, violating state laws by selling or giving away residents' sensitive information; second, illegally providing others with information acquired via the performance of duties; and third, obtaining information by illegal means such as theft. The first two types require “violation of state regulations” as a prerequisite, while the third type emphasizes the attribute of “illegal acquisition”. It is worth noting that if the information is used in legal circumstances such as judicial assistance or with the consent of the parties, it does not constitute a crime. At the same time, the crime must be "serious" and must be intentional, without profit or other specific purposes.

Taking into account the increasingly obvious chain and gang characteristics of information crimes, the determination of "serious circumstances" in judicial practice not only focuses on the amount of information, but also takes into account factors such as illegal gains, usage scenarios, and the identity of the perpetrator. The Interpretation on Handling Information Cases also established a classification

DOI: 10.54254/2753-7048/2025.LD24116

and grading protection mechanism, and strengthened the threshold for conviction of information of different sensitivities. In particular, the review of the use of information further highlights the social harm of information leakage in cyberspace, and provides criminal law protection for the establishment of a sound data outbound supervision system.

Overall, through the coordinated governance of civil and commercial law, administrative law, and criminal law, my country has established a hierarchical and coordinated regulatory method for the international transfer of personal information, taking into account both data circulation and security control, and gradually building a legal system and voice with Chinese characteristics in global data governance.

5. Law enforcement cooperation challenges and strategic responses in the context of China's personal data crime

5.1. Structural and practical barriers to cross-border law enforcement

However, with the increasing cross-border flow of data, China encounters multiple institutional and practical obstacles in promoting international criminal justice cooperation. In particular, cross-border law enforcement cooperation involving the crime of "infringing citizens' personal information" involves both data protection issues and how to effectively pursue criminal liability for cross-border crimes. The "crime of infringing citizens' personal information" in my country's criminal law stipulates acts such as illegal acquisition, sale and provision of personal information, but in cross-border law enforcement, the application and enforcement of these provisions face many challenges.

On the one hand, the extraterritorial effect of domestic laws is still unclear, and the legislative model is defensive. As mentioned above, the current legal framework in China for cross-border personal data flows does not explicitly show how the law has an extraterritorial impact, and is defensive in its legislative model. The law does not directly indicate the extraterritorial effect of the law, but stipulates that legal liability will be pursued for activities that damage national security, public interests, or the legitimate interests of citizens and organizations. Its main purpose is to respond to the challenges of domestic data security and privacy protection, focusing on building a data protection system within the country to protect the country from the adverse effects of foreign infringements on critical infrastructure or data activities, while the active protection and regulation of cross-border data flows are relatively insufficient. This makes it difficult to effectively investigate and sanction foreign entities that infringe on Chinese citizens' personal information in cross-border law enforcement cooperation based on domestic law, making the applicability of criminal law the primary obstacle to cross-border law enforcement cooperation. At the same time, there are significant differences among countries in the identification, punishment standards and sentencing range of data violations under criminal law. Although there are explicit provisions for violating China's penal code's prohibition against "infringing on citizens' personal information", other countries may adopt different legal classifications or handling methods for similar acts, which may make it impossible to make a consistent legal response to the same criminal behavior during cross-border law enforcement. When carrying out such cases, transnational law enforcement agencies often face issues such as whether they can successfully extradite criminal suspects and how to effectively cooperate in combating illegal data transactions.

On the other hand, from the standpoint of international law, China participates only passively and does not contribute to the creation of pertinent international regulations [14]. Regarding global data governance, China adopts a more prudent and conservative stance towards participating in international rules compared with EU countries, the United States, Japan and others. When participating in the formulation of international data governance rules, they tend to consider more about how to adapt to existing international rules and lack the awareness and action to proactively

DOI: 10.54254/2753-7048/2025.LD24116

lead the formulation of rules. Although this consideration is based on China's huge population base and imperfect data legislation, and aims to mitigate potential data breaches and adverse implications, it is indeed legitimate and inevitable. This passivity has resulted in China's relatively weak voice in international data governance, making it difficult to fully integrate its own development needs and interests into international rules. This has caused China to face the dilemma of insufficient legal basis or incompatibility with international rules when dealing with cross-border law enforcement cooperation issues such as transnational data crimes and cross-border data flows. In addition, China maintains a more cautious attitude towards the extraterritorial effect of domestic laws, emphasizing that it should not violate the fundamental ideas of international law. This means that during the legislative process, China often needs to fully consider the restrictions of international law to avoid causing international disputes. Although this cautious attitude helps maintain the international legal order, it also limits China's legislative initiative to a certain extent, making it difficult for China to quickly formulate legal norms with extraterritorial effect when dealing with complex issues such as transnational data crimes. It also affects cross-border law enforcement cooperation's efficacy and efficiency, and makes the prosecution of transnational crimes, especially data crimes, often delayed or impossible to implement.

5.2. Institutional and diplomatic strategies for legal coordination

Based on the above analysis of the dilemma of law enforcement cooperation in China’s crime of infringing citizens’ personal information, this article proposes several solutions from both the domestic law and international law levels.

From a domestic perspective, China should actively change its original governance concepts, proactively leverage its institutional and technological strengths, and actively participate in global data governance.

First, add extraterritorial effect clauses to domestic laws and improve the data governance supervision system. In the Personal Information Protection Law and other relevant laws and regulations, add clear extraterritorial effect clauses to stipulate under what circumstances Chinese law can be applied to the processing and cross-border transmission of domestic citizens' personal information by foreign entities. The protection of Chinese people' rights and interests regarding their personal information will serve as the foundation for the proper expansion of jurisdiction over data infringements committed abroad. At the same time, establish and improve regulatory agencies and mechanisms for data governance, and boost cross-border movement of data management and monitoring. For instance, a special cross-border movement of data regulatory agency should be established to be responsible for the approval, monitoring and enforcing laws pertaining to cross-border data transfers in order to guarantee their security and legality.

Secondly, strengthen the research and development of data security technologies and improve domestic data governance capabilities. For example, by encouraging domestic scientific research institutions and enterprises to use advanced data security technologies, we can provide technical support for cross-border data flows and prevent data from being illegally obtained and abused during cross-border transmission. At the same time, local companies must actively cooperate with and comply with local data legislation and reasonably respond to restrictions on cross-border data flows.

From an international perspective, China should take an active part in international organizations' operations. and put forward Chinese solutions and initiatives. In its international economic activities, China should fully take into account the development of its own digital economy, actively participate in data governance-related activities of international organizations such as the United Nations, the World Trade Organization, and the Organization for Economic Cooperation and Development, and promote the establishment of multilateral and bilateral regulations regarding data movements across borders. For instance, China can advocate the formulation of global data protection and cross-border

DOI: 10.54254/2753-7048/2025.LD24116

flow norms under the framework of the United Nations, integrate China's data governance concepts and practical experience into international rules, and put forward more constructive data governance solutions and initiatives. In terms of security assessment of cross-border data flow and protection of personal information, we propose standards and norms that are in line with China's interests and international development trends, and guide the international community to jointly respond to data governance challenges.

6. Conclusion

In the digital age, one of the main concerns of global governance is the legal disputes and challenges to law enforcement cooperation brought on by cross-border data flows. As a key production factor, data not only promotes global economic development and technological innovation, but also poses severe challenges to national sovereignty, personal privacy protection and international cooperation. Through in-depth analysis of data sovereignty theory, international flow of production factors theory, privacy rights theory and global governance theory, this study reveals the complexity and multidimensionality of movement of data across borders regulation. This paper highlights the shortcomings of the current legal framework in addressing cross-border information crimes and further examines the conundrum of law enforcement cooperation in cross-border data flows from the perspective of the crime of violating citizens' personal information under China's Criminal Law.

To sum up, building a regulatory framework that can both ensure the free flow of data and effectively protect citizens' personal information is the key to achieving sustainable development of the global economy and digital economy. The construction of this framework not only requires countries to seek a balance between data sovereignty and privacy protection, but also requires strengthening cooperation at the international level to jointly formulate unified regulatory rules. In this process, China should actively change its governance concepts, take the initiative to take part in the creation of international regulations, and at the same time improve its domestic legal system and enhance its data governance capabilities to cope with the increasingly complex challenges of cross-border data flows.

In the future, with the continuous advancement of technology and the deepening of international cooperation, the regulatory framework for cross-border data flows will continue to improve. We hope that all countries can work together to jointly respond to this global challenge and contribute to the prosperity of the digital economy and the progress of human society.

References

[1] *Irion, K. 2012. Government cloud computing and national data sovereignty. Policy & Internet (4): 42–43.*
[2] *Sun, N. & Zhang, X. 2015. On data sovereignty: An investigation based on cyberspace games and cooperation. Pacific Journal (2): 3.*
[3] *European Parliament. 2020. Digital sovereignty for Europe. European Parliamentary Research Service Ideas Paper Briefing.*
[4] *Budnitsky, S. & Jia, L. 2018. Branding internet sovereignty: Digital media and the Chinese–Russian cyberalliance. European Journal of Cultural Studies 21(5): 605.*
[5] *Avila Pinto, R. 2018. Digital sovereignty or digital colonialism? Sur International Journal on Human Rights 15(27): 19.*
[6] *Trachtman, J. P. 1998. Cyberspace sovereignty, jurisdiction and modernism. Indiana Journal of Global Legal Studies: 563.*
[7] *CRS. 2020. Internet regimes and WTO e-commerce negotiations. Washington, D.C.: Congressional Research Service.*
[8] *U.S. Congress. 2018. Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA), Pub. L. No. 115-232, 132 Stat. 2173.*
[9] *Executive Office of the President. 2021. Executive Order 14034: Protecting Americans' Sensitive Data From Foreign Adversaries. Federal Register 86(111): 31423–31426.*

DOI: 10.54254/2753-7048/2025.LD24116

[10] UNCTAD. 2021. Digital economy report 2021: Cross-border data flows and development: For whom the data flow. [R/OL]. https://unctad.org/system/files/official-document/der2021_en.pdf (Accessed: 2023-01-12).

[11] Li, Q. 2023. Legal issues of international regulation on cross-border flow of personal data. Liaoning University. DOI:10.27209/d.cnki.glniu.2023.002463.

[12] Russian Federation. 2014. Federal Law No. 152-FZ on Personal Data Article 18(5), as amended by Federal Law No. 242-FZ on Amendments to Certain Legislative Acts.

[13] Russian Federation. 2022. Amendments to the Federal Law on Personal Data (No. 266-FZ), Articles 11 and 12. http://publication.pravo.gov.ru/Document/View/0001202207140080 (Accessed: 2022-12-17).

[14] Lei, M. & Sun, Y. 2021. Legal regulation of cross-border data flow: From the perspective of data rights protection. In: Shanghai Law Research Annual Vol. 6. Beijing University of Technology School of Law and Humanities: 10. DOI:10.26914/c.cnkihy.2021.032929.