Analysis of the Fragmentation and Coordination Path of International Rules for the Protection of Personal Data Rights and Interests in the Era of Big Data

Xinyu Niu *

Faculty of Commerce, Hong Kong Shue Yan University, Hong Kong, China

* Corresponding Author Email: 237013@hksyu.edu.hk

Abstract. As the era of big data progresses in depth, while cross-border data flow has become a new engine for global economic growth, it also poses severe challenges to personal data rights. The data governance rules adopted by various countries to address this issue exhibit a distinct "fragmentation" feature, posing significant resistance to international cooperation and corporate compliance. This article focuses on this topic. By using the comparative research method, case study method and legal text analysis method, the core differences in regulatory systems and cross-border rules among the three major data governance models of the European Union, the United States and China were systematically analyzed. By analyzing typical cases such as the "Schrems II" case and the Didi incident, this paper proposes a multi-level coordination path centered on building "interoperability", aiming to provide theoretical references and practical suggestions for constructing a fairer, more efficient and safer global digital governance model.

Keywords: Era of big data, the rules for personal data rights, fragmented interests.

1. Introduction

With the in-depth evolution of the era of big data, the scale of cross-border data circulation is expanding, and data elements are flowing globally. Data privacy has become a double-edged sword. On the one hand, cross-border data flow promotes trade development, cross-border data chain integrates global supply chain, and many small and medium-sized enterprises can participate in data division through cloud services. According to the McKinsey Global Institute (MGI), since 2008, the contribution of data flows to global economic growth has exceeded that of traditional cross-border trade and cross-border investment [1]. On the other hand, it also infringes on personal data rights and interests. For example, after people around the world browse social media, radio and television, online shopping and other big data platforms, personal information such as preference trajectory and geographical location is retained by databases. Many websites require users to agree to privacy agreements before they can use basic services. The only entry for lengthy and obscure terms is the "consent" option, which is full of forced consent [2]. Based on the current problem of personal data rights protection in the era of big data, countries have taken measures to deal with it. For example, the European Union's General Data Protection Regulation, (GDPR), California's Consumer Privacy Act (CCPA) of the United States, and China's Personal Information Protection Law protect personal data rights and interests from different dimensions, but there is no unified regulatory system for cross-border data flow [3]. Therefore, under the fragmented international rules, it is necessary to work out a coordination path that not only protects the privacy of personal data but also gives full play to the globalization of data elements. For example, in 2020, the Court of Justice of the European Union determined that the Privacy Shield agreement between the European Union (EU) and the United States was invalid in the "Schrems II" case. It was precisely due to the fundamental disagreement between the EU and the United States on data protection standards that thousands of enterprises faced the crisis of legality of cross-border data transmission. The urgent shift to more costly Standard Contractual Clauses and Binding Corporate Rules fully exposed the huge compliance costs and legal uncertainty caused by the fragmentation of international rules. In addition, Didi has been subject to scrutiny and heavy penalties from Chinese regulators for violating relevant laws and regulations. The incident highlights China's strict stance on data compliance regulation and has clear cautionary

implications for multinationals operating in the country. If enterprises fail to comply with the requirements of data localization storage and outbound security assessment and transfer domestic data to overseas processing without authorization, they will face significant compliance risks, which fully reflect the compliance conflicts and jurisdiction overlap caused by the fragmentation of international data rules. Based on this, this paper adopts the comparative research method, case study method and legal text analysis method to analyze the causes and impacts of the fragmentation of international rules by comparing the three data governance models of the EU, the United States and China, and then explores the coordination path to balance the cross-border data flow and rights and interests protection in the era of big data, providing theoretical basis for the construction of international rules that give consideration to security and development. The government will promote a fairer, more efficient and more secure global digital governance model.

2. Literature Review

The arrival of the era of big data has made cross-border data flow a new engine of global economic growth and also pushed the protection of personal data rights and interests to the forefront of international governance. The academic circle has carried out multi-dimensional discussions on this issue, and the existing research mainly focuses on the following three aspects:

First of all, the dual understanding of data value and risk in the era of big data has become an academic consensus. As some studies show, the contribution rate of data flow to global economic growth has exceeded that of traditional transnational trade and transnational investment [4]. However, behind the value creation, personal data rights and interests face serious threats. Some scholars have revealed the common phenomenon that platform enterprises violate users' right to know an autonomy by means of "forced consent" to obscure privacy agreements, highlighting the urgency of privacy protection [5].

Secondly, relevant scholars analyze the causes, manifestations and impacts of the fragmentation of international rules. Some scholars believe that GDRP sets high standards for privacy protection in the era of artificial intelligence through strict "informed consent" and responsibility of data controllers [6]. The coexistence of the "market dominance and industry self-discipline" model in the United States at the federal and state levels, and the concept of "paying equal attention to security and development" reflected in China's Personal Information Protection Law, these studies clearly depict the current situation of the "fragmentation" of the global data governance landscape. Some scholars further pointed out that such differences in rules derived from different legal traditions, economic demands and sovereignty concepts lead to the lack of a unified regulatory system for cross-border data flow, which brings great challenges to the compliance and international cooperation of multinational enterprises [7]. However, the existing research mostly stays on the description and comparison of national models or generally puts forward the necessity of "strengthening coordination." It lacks the analysis of the deep contradictions between rules and fails to fully propose the specific conflicts brought by the fragmentation of international rules in judicial practice and corporate compliance.

Finally, discussion on the path of international coordination is becoming an emerging hotspot. Some scholars have analyzed that the current international data governance presents a pattern of four modes, namely, the United States, Europe, Russia and China, standing side by side. Rule conflicts, regional fragmentation and the formation of exclusive data circles have intensified the fragmentation of the international rule system. It also proposes to build a "hierarchical and collaborative" governance framework to promote the integration of rules. Promote "interoperability" between major data governance modes to coordinate data sovereignty and security and efficiency of cross-border flows [8]. Although the current research has analyzed the key issues such as the specific implementation mechanism of "interoperability" and the driving force of regulatory cooperation among different sovereign states, it still lacks in-depth and operational scheme design, which is the direction that this study attempts to break through and deepen.

3. Comparison of Core Differences in Personal Data Rights and Interests Protection Rules between the US and Europe

3.1. United States

The American model embraces a decentralized regulatory approach that lacks a unified privacy regulator at the federal level. Its regulatory system consists mainly of state legislation, industry-specific regulations (such as the Health Insurance Portability and Accountability Act for medical data and the Children's Online Privacy Protection Act for minors), and the Federal Trade Commission's enforcement of "unfair or deceptive practices" [9]. In terms of regulatory scope, the United States emphasizes the constraints on "domestic enterprises," but lacks the long-arm jurisdiction provisions similar to those of the European Union. For example, European businesses are subject to the GDPR's cross-border rules even if they collect EU residents' data outside the U.S.; The United States, on the other hand, mainly relies on industry self-discipline and contractual arrangements, and does not establish universal obligations to overseas enterprises [10].

In terms of cross-border data flow, the United States has long pursued a model with industry dominance and self-regulation as the core. A typical example is the US-EU Privacy Shield framework, which allows companies registered in the US to legally receive EU personal data through self-certification and commitment to comply with EU standards [11]. However, this mechanism was ruled invalid by the European Court of Justice (Schrems II) in 2020 due to the lack of effective restrictions on mass surveillance by US intelligence services, which could not meet the EU's requirement of "equivalent protection". Since then, although the US and EU launched the "Transatlantic Data Privacy Framework" in 2023, its stability and legal sustainability are still controversial [12].

3.2. The EU

The EU model builds a unified and highly independent regulatory system with no geographical restrictions. Through the principle of "long-arm jurisdiction", their data processing activities will be monitored as long as they involve the provision of goods or services to data subjects in the EU. No matter where the processor is located, it is governed by the EU model. The extra-territorial effects of such laws also have a direct and far-reaching impact on Mauritius, which is pushing ahead with data privacy reform.

In terms of cross-border data flow, some scholars have analyzed that the core financing of the "adequacy determination" of the EU model is the main reason for its extra-territorial effectiveness, that is, the European Commission will approve the free flow of data into a third country only when it determines that it can provide a level of protection "substantially equivalent to that of the EU". For countries such as Mauritius, obtaining "adequacy recognition" is a key part of their digital economy development, so when they revise their data protection laws, they are largely in line with the standards of the EU model [13].

3.3. China

The Chinese model is a "multi-coordinated" regulatory framework; Each department shall be responsible for the division of labor within the scope of its own responsibilities to form a joint regulatory force. Its jurisdiction covers domestic personal information processing activities and also has regulatory effect on overseas recipients. In terms of jurisdiction and measures, China has established the regulatory scope of "whole process + hierarchical classification", taking into account both "security and efficiency". It not only regulates the whole process of personal information processing activities but also carries out hierarchical and classified management according to the importance and sensitivity of data, and adopts various means such as security assessment, compliance audit and certification. It aims to achieve a balance between protecting individual rights and interests and safeguarding national security and public interests.

In terms of cross-border data flow, the Chinese model takes' security assessment 'as the core and adheres to the premise that security and development attach equal importance to data exit: "national

security and public interests are not harmed, and the legitimate rights and interests of individuals are not harmed". The provisions of Article 3 of the Personal Information Protection Law mean that even foreign companies, if they process the information of Chinese citizens, and in one of the three circumstances stipulated, it should also comply with the legal provisions of China [14].

4. Coordination and Optimization Path of Fragmented International Rules on the Protection of Personal Data Rights and Interests

4.1. Regional Coordination Level

First of all, people should promote "differentiated mutual recognition". On the basis of recognizing the same basic protection objectives, according to the core differences between the rules of the two sides, people should define the compliance elements and exceptions that can be recognized by each other through rule mapping or mutual recognition catalogue, so as to reduce the comprehensive negative barriers caused by different legal texts. This idea can draw on the OECD's common framework on cross-border data flows and privacy principles to provide value orientation and technical evaluation criteria for mutual recognition [15].

Second, pilot cross-border data flow can be carried out. For example, a number of China-EU/China-Us digital enterprises and industries (such as Huawei and Siemens) are selected to implement dual-track compliance pilots, allowing enterprises to independently choose EU model or Chinese model compliance paths under the "Core Principles Framework", and at the same time, peer regulators will conduct supervision through regulatory dialogue, mutual recognition of data protection impact assessment, joint audit and other means.

4.2. Adaptation Level of Domestic Rules

In the United States, it is suggested to give priority to promoting the overall framework legislation at the federal level, integrating the fragmented rules at the state level, and setting a unified baseline for cross-border transfer, federal law enforcement and private rights relief, so as to reduce the uncertainty in international negotiation [16].

In the EU, a risk-based interpretation of flexibility is recommended while upholding the high standards of EU regulations: Incorporate "developing country capacity and compliance reality" into the assessment dimension, simplify the SCCs application process for low-risk, desensitized or de-labeled data transmission [and provide a regulatory fault tolerance mechanism for technology protection measures adopted by enterprises in specific cross-border scenarios. The importance of complementary technical measures has also been emphasized in the relevant recommendations of the European Data Protection Board [17,18].

In China, cross-border compliance categories and channels should continue to be refined: expand the exit white list of "low-risk data/desensitizing data", improve the transparent guidelines of standard contracts and security assessment, and set up a fast channel to encourage compliance enterprises to give priority to pilot, so as to release an open signal to the international community with predictable compliance costs [19].

4.3. Technology Empowerment Level

Promote privacy enhancement technologies (PETs), encourage the use of federate learning, differential privacy, homomorphic encryption and other technologies in cross-border cooperation, achieve the goal of "data available and invisible", and fundamentally reduce the dependence on physical data migration. Studies have shown that these methods can reduce the risk of privacy disclosure while maintaining the effectiveness of analysis [20].

Build a cross-border data compliance technology platform, led by international organizations or industry alliances, and establish a technology platform of "compliance requirement database + rule mapping tool + real-time compliance monitoring" to automatically compare enterprises' cross-border

processing behaviors with compliance points in the United States, Europe and China and issue compliance suggestions or early warnings.

5. Conclusion

This study systematically analyzes the dilemma of international rule fragmentation in cross-border data flow and personal data rights protection in the era of big data by comparing the three major data governance models of the EU, the United States and China. The three modes have significant differences in legislative purpose, regulatory system and cross-border rules, which are rooted in the legal tradition, economic structure and sovereignty concept of each country. It has brought certain resistance to enterprise compliance and international cooperation. In order to cope with this resistance, this study actively explores a coordination path with "interoperability" as the core. This approach can promote the construction of a collaborative governance framework and promote the global and efficient flow of data under the premise of ensuring data security by enhancing the interoperability of rules and regional cooperation. However, there is still a lack of practical verification, and the comparison is only made in terms of macro rules, without specific analysis of enterprises and international cooperation at the micro level. Future research needs to combine empirical investigation and case analysis, and further focus on operational solutions to enhance the practical research of theory construction.

References

[1] Liu R., Zhou J. Y. Policy issues and countermeasures of cross-border data flow in China's digital economy. Keji Zhongguo Science & Technology China, 2021, (4): 53 – 56.

[2] Long J. T. Protection path of antitrust law for personal privacy rights in the big data era. Renmin Luntan People's Tribune, 2022, (24): 112 – 115.

[3] Jiang H., Chang P. Y. The Normative Construction of Cross-border Data Flow from the Perspective of the Basic Categories of Law. Journal of Yantai University (Philosophy and Social Sciences Edition). 2025.

[4] Liu R., Zhou J. Y. Policy issues and countermeasures of cross-border data flow in China's digital economy. Keji Zhongguo Science & Technology China, 2021, (4): 53 – 56.

[5] Long J. T. Protection path of antitrust law for personal privacy rights in the big data era. Renmin Luntan People's Tribune, 2022, (24): 112 – 115.

[6] Hua J. Privacy protection in the era of artificial intelligence: Analysis of provisions in EU General Data Protection Regulation and related proposals for new regulations. Lanzhou Academic Journal, 2023, (6): 97 – 108.

[7] Jiang H., Chang P. Y. The Normative Construction of Cross-border Data Flow from the Perspective of the Basic Categories of Law. Journal of Yantai University (Philosophy and Social Sciences Edition), 2025.

[8] Tang Z. Fragmentation of international rules on cross-border data flow and coordination paths. Jiangxi Social Sciences, 2025, 45 (6): 120 - 130.

[9] Cate F. H., Mayer-Schönberger V. Notice and consent in a world of Big Data. International Data Privacy Law, 2013, 3 (2): 67 – 73.

[10] Schwartz P. M., Peifer K. N. Transatlantic data privacy law. Georgetown Law Journal, 2017, 106 (1): 115 – 179.

[11] Kuner C. Transborder data flows and data privacy law. Oxford: Oxford University Press, 2021.

[12] European Commission. EU–U.S. Data Privacy Framework: Adequacy decision. Brussels: European Commission, 2023.

[13] Makulilo A. B. The long arm of GDPR in Africa: Reflection on data privacy law reform and practice in Mauritius. In The Right to Privacy Revisited (pp. 121 - 150). Routledge, 2021.

[14] Xiong G., Zhang S. The extraterritorial application of China's personal information protection norms: An examination from an international comparative perspective. Ji Bijí, 2025. Advance online publication.

[15] Organisation for Economic Co-operation and Development (OECD). OECD guidelines on the protection of privacy and transborder flows of personal data. Paris: OECD Publishing, 2013.

[16] European Commission. Standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679. Official Journal of the European Union, 2021.

[17] European Data Protection Board (EDPB). Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. 2021.

[18] Cate F. H., Mayer-Schönberger V. Notice and consent in a world of Big Data. International Data Privacy Law, 2013, 3 (2): 67 – 73.

[19] Shokri R., Shmatikov V. Privacy-preserving deep learning. Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, 2015: 1310 – 1321.

[20] Cheng L., Liu F., Yao D. Enterprise data breach: Causes, challenges, prevention, and future directions. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 2017, 7 (5): e1211.