DOI: 10.54254/2753-7048/2025.BR26817

Research on Enterprise Cross-border Data Compliance

Yuexuan He

Department of Mathematics and Statistics, Villanova University, Villanova, USA
yhe@villanova.edu

Abstract. With the continuous development of the global digital economy, cross-border data flows have become a critical component of businesses' international operations. At the same time, cross-border data compliance has become a major challenge facing businesses. The development of China's cross-border data compliance policy can be divided into three stages: initial exploration, system development, and refinement. These three stages highlight China's policy approach to cross-border data regulation, evolving from principled guidance to systematic governance. At the same time, it is clear that existing cross-border data compliance practices are plagued by several issues: fragmented legal regulations cause inconsistent application; vague compliance standards result in inconsistent implementation; and insufficient integration with international rules leads to high compliance costs. Comparative analysis of international systems such as the United States' fragmented regulatory framework, the EU's internal market harmonization with extraterritorial data transfer restrictions, and ASEAN's openness and security exceptions demonstrates the need for further research and governance in policy, implementation, and corporate compliance capacity building. In the future, China needs to establish a cross-border data management framework that prioritizes both security and efficiency, exploring a governance path for achieving a dynamic balance between data security and the digital economy.

Keywords: Cross-border Data Compliance, Fragmented Regulations, International Harmonization, Dynamic Balance

1. Introduction

As the global digital economy expands rapidly, data has emerged as a crucial factor of production alongside land, labor, capital, and technology. As businesses continue to internationalize, cross-border data flows have become a crucial component of the digital economy, and their importance is growing. According to McKinsey research, by 2025, cross-border data flows will have an estimated impact of $11 trillion on the global economy. During this period, countries are rapidly developing diverse cross-border data management mechanisms to address challenges such as national security, personal privacy protection, and industry competition.

For example, since the promulgation and implementation of the Cybersecurity Law, China has gradually established a multi-level regulatory framework, led by the Data Security Law and the Personal Information Protection Law. This framework has also improved the data export compliance system, encompassing security assessments, standard contracts, and privacy certification. In March

2024, the Cyberspace Administration of China issued the "The “Regulations on Promoting and Regulating Cross-Border Data Flows”, specifying clear exemptions and prohibitions on data exports to strike a dynamic balance between protecting data security and ensuring efficient cross-border data movement. However, under the existing regulatory framework, enterprises still face numerous compliance challenges in practice. For example, current laws and regulations are fragmented, and the Cybersecurity Law and the Data Security Law lack a coordinated mechanism for defining regulatory targets and implementing enforcement measures, leading to a continuous increase in compliance costs for enterprises. Furthermore, international regulations vary significantly, and enterprises expanding into overseas markets face complex challenges such as the EU GDPR's "adequacy decision" requirements and the "long-arm jurisdiction" issues raised by the US Cloud Act. Most theoretical research on cross-border data compliance focuses on a single country or region, lacking a systematic discussion of the full-chain operational mechanisms and multifaceted governance issues involved in the multi-faceted process.

Based on this, this article focuses on cross-border data compliance for enterprises. It first reviews China's data-related policies and regulations, and then examines the main challenges facing cross-border data compliance in practice. It then deeply examines the policies and systems of developed countries and regions such as the US and Europe, offering valuable insights into internal corporate governance, policy improvement, and international cooperation mechanisms. This article provides an institutional basis for enterprises to establish a cross-border data management framework that balances security and convenience.

2. Overview of enterprise cross-border data compliance issues

2.1. Definition of relevant concepts of enterprise cross-border data compliance

Cross-border data compliance management involves systematic control over the entire data lifecycle, encompassing data collection, storage, transmission, and processing. Enterprises are required to strictly adhere to the laws, regulations, industry norms, and international standards of both the importing and exporting countries. Furthermore, a dynamic management mechanism centered on risk prevention must be established. Its core elements include: First, the scope of compliance encompasses various types of data, including personal information, important data, and trade secrets. The Data Security Law defines “important data” as critical information assets that, if altered, destroyed, or illegally used, could endanger national security, economic stability, social order, or public health and safety [1]. Second, compliance scenarios encompass both active cross-border transmission and passive cross-border flow. Third, compliance responsibilities embody a dual "legal-technical" system, requiring compliance with the "notice and consent" principle of the Personal Information Protection Law while leveraging technical means such as encryption algorithms and anonymization to ensure data security [2].

2.2. The development of enterprise cross-border data compliance policies and systems in China

From 2012 to 2016, China underwent an initial exploratory stage of cross-border data regulation, during which the Standing Committee of the National People’s Congress issued the “Decision on Strengthening Online Information Protection”(hereinafter the “Decision”). This marks a critical development phase for China's cross-border data management. With the continued deepening of global digital transformation and the rapid expansion of the domestic internet industry, the demand for cross-border flow of personal information continues to grow, and the accompanying security risks are gradually emerging. This decision, for the first time, proposed that cross-border transfers of personal information must adhere to the principles of "lawfulness, fairness, and necessity," providing core value guidance for subsequent legislation and clearly defining the basic ethical standards that businesses and participants in cross-border data activities should adhere to. Due to the early stages of development of the digital economy and the objective limitations of data understanding, early policy documents tended to focus on macro-level guidance, lacking specific operational paths and supporting safeguards. Against this backdrop, businesses faced numerous uncertainties and risks in their operations. The legal boundaries of cross-border data flows remained unclear, relying primarily on the constraints of market entities and internal industry self-regulatory mechanisms. These factors, to a certain extent, restricted the effective circulation and rational allocation of data elements.

The period from 2017 to 2021 marked the establishment of a cross-border data regulatory system in China. The promulgation and implementation of the Cybersecurity Law in 2017 was a landmark event. It established for the first time a security assessment mechanism for data localization requirements and cross-border transfer, and specifically stipulated the responsibilities of critical information infrastructure operators for domestic data storage, thus providing institutional guarantees for data security from a legal perspective. This institutional arrangement reflects a deep concern for the security of core national information, aiming to prevent potential risks associated with cross-border data flows and safeguard national security and public interests. Since 2021, the Data Security Law and the Personal Information Protection Law have been successively promulgated, gradually establishing an institutional framework based on "categorized and hierarchical protection" as a key principle. These two laws implement strict control measures for the cross-border transmission of important and core data, classifying data into three levels: general, important, and core, and adopting differentiated regulatory strategies. Their legislative framework has gradually expanded from regulating a single link to encompassing the entire process, establishing a comprehensive governance mechanism for every stage of the data lifecycle and providing a systematic legal basis for cross-border data flows [3].

The period from 2022 to the present has been a period of optimization and improvement for China’s cross-border data regulation. The booming global digital economy has led to a growing demand for cross-border data flows, but this has also faced the dual pressures of data security and economic interests. Consequently, China's relevant policies have gradually shifted towards a more intensive approach, striving to establish a dynamic balance. To address data security and circulation issues, the 2022 "Measures for the Security Assessment of Cross-border Data Transfer" detailed the reporting process, conducting quantitative assessments based on indicators such as data size and sensitivity. This significantly enhanced regulatory effectiveness and provided businesses with more specific compliance guidance. The 2023 "Measures for Standard Contracts for Cross-border Transfer of Personal Information" also introduced corresponding contract templates to reduce institutional costs and alleviate the pressure on small and medium-sized enterprises caused by regulations. The 2024 "Provisions on Facilitating and Regulating Cross-border Data Flows (draft for comment)" introduced a negative list model for management in free trade pilot zones, and implemented exemptions for specific situations such as scientific research and academic settings and anonymization processing scenarios. This reflects a governance approach characterized by "safe and sustainable development." This will further promote the unleashing of the value potential of data elements and enhance the initiative and level of Chinese companies' participation in market competition at the international level [4].

In summary, the policy evolution of cross-border data compliance in China reflects the deepening development of data governance concepts and the continuous enrichment of implementation steps. Starting from principled exploration, a complete set of institutional frameworks has gradually been formed, and then improved and upgraded towards a more detailed operating model. This progress clearly shows the trend of regulatory thinking constantly moving forward [5].

2.3. Problems facing cross-border data compliance in Chinese enterprises

2.3.1. Fragmentation of legal regulations and conflicting applications

Currently, China's cross-border data compliance system is markedly fragmented, with relevant regulations scattered across numerous laws, regulations, and departmental rules. While this legislative approach demonstrates a systematic approach to data governance, it also creates numerous difficulties in legal application. For example, the definition of "important data" in the Cybersecurity Law and the Data Security Law differs significantly. The former focuses on national security, while the latter extends to a wide range of areas, including economic operations and public health. Due to the differing regulatory emphases between the two regulations, it is challenging for enterprises to establish a unified cross-regional data compliance system. Furthermore, regulatory conflicts are evident in the financial sector. For example, the Technical Specifications for the Protection of Personal Financial Information (JR/T 0171-2020) focus on technical security requirements for cross-border transmission, while the Measures for the Security Assessment of Data Export emphasize a multi-dimensional assessment framework for data size and sensitivity. While there is some overlap in regulatory objectives between the two, financial institutions still face duplication in compliance audits and rectification tasks [6]. Consequently, financial institutions incur substantial annual data compliance expenditures to meet the demands of these numerous regulations.

2.3.2. Ambiguous compliance standards and uncertain implementation

Key concepts such as "important data" and "sensitive personal information" are legally undefined and have become a major obstacle to corporate compliance. For example, while the "Data Security Technical Data Classification and Grading Rules" provide some guidance to companies, they fail to establish industry-specific quantification criteria. For example, in the healthcare sector, there's no clear basis for determining the ownership of patient genetic information and electronic medical records, and in the energy industry, there's no unified standard for classifying the security levels of power grid operation data. Currently, most companies face significant obstacles in independently determining data classifications and must rely on regulatory authorities for case-by-case decisions [7]. This over-reliance on ex post regulatory determinations not only prolongs corporate compliance time but also sparks debate about fairness due to varying regulatory standards. For example, when technology companies applied for data export security assessments, inaccuracies in data classifications led to repeated revisions to their application materials, resulting in project delays and significant losses [8].

2.3.3. Inadequate alignment with international rules and high compliance costs

Amidst deepening economic globalization, there are significant deficiencies in the alignment of China's cross-border data compliance system with international regulations. On the one hand, China has not joined the APEC Cross-Border Privacy Rules (CBPR) System proposed by APEC; on the other hand, there has been no substantial progress in the mutual recognition process between the "adequacy decision" mechanism and the GDPR. This has led to numerous compliance risks for companies expanding into overseas markets. For example, Chinese companies targeting the EU market must not only comply with the domestic "Measures for Data Transfer Security Assessments Abroad" but also conduct Data Protection Impact Assessments (DPIAs) based on the EU standard contractual clauses, which undoubtedly increases operational complexity and costs. Research data shows that this dual compliance requirement increases the average compliance cost for companies by approximately 30% [9]. Some small and medium-sized enterprises, unable to afford these high costs, have withdrawn from the EU market. Furthermore, the potential conflicts arising from foreign laws such as the "Clarifying Lawful Overseas Use of Data Act" also increase the compliance burden and operational risks for companies [10].

3. Lessons from overseas enterprises' cross-border data compliance systems

3.1. The United States: a compliance mechanism with sectoral federal laws with state-level supplementation

Currently, the United States has established a system of decentralized legislation and multi-level supervision for cross-border data compliance. At the federal level, the Federal Trade Commission Act grants the FTC broad enforcement powers, enabling it to investigate and impose penalties for data breaches and unfair business practices. The Health Insurance Portability and Accountability Act and the Children's Online Privacy Protection Act provide specific protections for health data. At the state level, the California Consumer Privacy Act establishes consumer rights to know and delete data. The California Privacy Rights Act, which came into effect in 2023, adds a new privacy protection agency, significantly raising data compliance standards.

With regard to cross-border data transfers, the European Court of Justice invalidated the Safe Harbor Agreement due to the Prism scandal. Subsequently, the EU-U.S. Data Privacy Framework reestablished a transatlantic data flow mechanism, introducing redress channels for data subjects and government oversight mechanisms [11]. Furthermore, the United States, through the Clarifying Lawful Overseas Use of Data Act, grants law enforcement agencies the right to access overseas data and requires companies to cooperate with cross-border data enforcement requests, demonstrating its commitment to expanding data sovereignty. For overseas companies, the US data compliance system offers a dual "incentive and penalty" approach. The Google Android user data abuse case demonstrates regulatory characteristics characterized by institutional restructuring, expanded sovereignty, and a balanced approach of firmness and flexibility [12]. Some technology companies can meet compliance requirements by establishing local data centers and implementing data classification and tiered management. However, violations of relevant regulations, such as the $5 billion fine imposed on a social media platform by the FTC for a user data breach, can serve as a significant deterrent. Faced with a complex data compliance environment, companies must establish a dynamic compliance system, closely monitor changes in federal and state legislation, and increase investment in data security technologies to mitigate potential legal risks [13].

3.2. EU: "loose inside, tight outside" privacy protection and regional barriers

The EU has established a "loose inside, tight outside" compliance system centered around GDPR, with personal data protection as a core principle for cross-border data flows. The GDPR adopts a "territorial + personal" jurisdictional principle, regulating not only data processors within the EU but also businesses processing EU citizens' personal data abroad. Violators face substantial fines of up to 4% of their annual turnover. Meta, for example, was fined €1.2 billion for cross-border data transfer violations.

For cross-border data transfers, the EU has established a two-tiered mechanism of "adequacy determination + alternative measures." Data from countries with a data protection adequacy determination (such as Japan and South Korea) can flow freely, while data from countries without such determinations must adopt measures such as Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs), and the data subject must provide explicit consent. This strict regulation creates a "single domain" within the region where data can flow freely, but imposes higher compliance thresholds for entities outside the domain. The EU promotes the flow of non-personal data within the EU through the Regulation on the Free Flow of Non-Personal Data, establishing a governance framework of "internal freedom and external control" based on the GDPR. Moreover, cross-border data cooperation between the EU and the US, through the Safe Harbor Agreement, the Privacy Shield Agreement, and the Data Privacy Framework (DPF), has revolved around the struggle between "government data access restrictions" and "company compliance obligations," reflecting the EU's dynamic balance between protecting privacy and promoting trade [14].

3.3. ASEAN: flexible openness and security exception mechanisms led by regional agreements

ASEAN countries' cross-border data compliance rules are primarily reflected in regional trade agreements, exemplified by the RCEP and DEPA, which feature a "presumptive free flow with security exceptions" approach. RCEP promotes the free flow of cross-border data and prohibits data localization as a prerequisite for commercial activities. However, it provides two exceptions, namely "legitimate public policy objectives" and "essential security interests," allowing member states to restrict data flows for reasons such as national security and personal information protection, such as Indonesia's requirement for local storage of social media data. DEPA, on the one hand, promotes the free flow of cross-border data, relaxes location restrictions on computing facilities, and simplifies digital trade processes; on the other hand, it ensures security through rules such as personal information protection and online trust mechanisms, while retaining regulatory space for data related to national security. DEPA is the first dedicated digital economy agreement with more flexible rules. It requires parties to allow cross-border data flows and restrict data localization, but allows them to take necessary measures based on "legitimate public policy objectives." It also encourages open data sharing and supports innovative mechanisms such as regulatory sandboxes and trusted data frameworks. Compared to the CPTPP, the ASEAN agreement better balances the regulatory needs of developing countries with the freedom of data flows. For example, the RCEP's personal information protection provisions focus on preventing unsolicited commercial information. DEPA emphasizes the compatibility and mutual recognition of legal mechanisms between parties, creating a more compliance-friendly environment for small and medium-sized enterprises. This "principles plus exceptions" approach aligns with the development trend of the digital economy while also leaving policy space for member states.

4. Optimizing the path to cross-border data compliance for Chinese enterprises

4.1. China should further improve cross-border data compliance policies and regulations and build a unified and coordinated rules system

China should adhere to the principle of "giving equal importance to security and development," refine the top-level design of policies and regulations for cross-border data flows, and clarify data classification and grading standards. The current definitions of "important data" in the Data Security Law and the Measures for Security Assessment of Cross-border Data Transfer are rather vague. Reference can be made to the EU GDPR's "Sensitive Personal Data" list and the US EAR's "Controlled Data" catalog. Industry-specific, actionable guidelines for identifying important data can be developed, for example, with special protection requirements for financial and medical data, to reduce uncertainty for enterprises in meeting these requirements.

Improve regulatory coordination mechanisms. Addressing the current overlapping responsibilities among the Cyberspace Administration of China, the Public Security Bureau, and the Ministry of Industry and Information Technology, an inter-agency coordination mechanism for data compliance supervision can be established, modeled on the coordination structure of the European Data Protection Board (EDPB). This system will unify enforcement standards and eliminate the compliance costs associated with multiple regulators. Strengthen international alignment, deepen governance coordination with ASEAN under the RCEP, actively promote accession to DEPA, gradually relax local data restrictions using a "negative list" model, and develop higher-level cross-border data flow regulations within free trade zones, such as by promising qualified companies simplified security assessment procedures through a "white list." Improve cross-border data law enforcement coordination mechanisms, sign data mutual legal assistance treaties with major trading partners, clarify the procedures and scope for data retrieval, and avoid legal disputes caused by long-arm jurisdiction [15].

4.2. China should focus on the enforcement of policies and systems, shifting from an emphasis on policy design to a focus on precise policy implementation

The effectiveness of policies lies in the precision of their implementation. On the one hand, the implementation of the data export security assessment system should be strengthened. The current "Measures for Security Assessment of Cross-border Data Transfer" lists four categories requiring reporting, but companies' self-assessment standards vary and their risk prediction capabilities are insufficient [16]. A "state-led assessment framework with accredited third-party validations" model could be established, with the national cyberspace administration issuing assessment guidance templates to encourage companies to engage professional institutions to conduct risk assessments, focusing on the protection level of the data recipient and the security of the transmission path. Reference can be made to the EU SCC clause structure to develop a standard contract template tailored to China's national conditions.

On the other hand, efforts should be made to promote the implementation of a standard contract system for the export of personal information. The "Measures for Standard Contract for Cross-border Transfer of Personal Information" provide a convenient path for small and medium-sized enterprises, but supervision of contract performance during and after the implementation must be strengthened, requiring enterprises to submit compliance reports promptly to prevent situations where contracts are formally compliant but actual practices are not.

Pilot "regulatory sandboxes" should be implemented in pilot free trade zones to allow enterprises to test new cross-border data services, such as cross-border medical data sharing and industrial internet data transmission, in a controlled environment, and to improve relevant rules based on this experience. Supervision of the entire data lifecycle should be strengthened, creating a closed loop from "informed consent" during collection, "classification and grading" during storage, "security assessment" during transmission, to "irrecoverable destruction." For example, enterprises should be required to utilize de-identification and encryption technologies to reduce the risk of leakage.

4.3. Enterprises should proactively build full-chain compliance capabilities and collaborative mechanisms

As the main actors in cross-border data flows, enterprises should move from "passive compliance" to "proactive governance." Internally, dedicated data compliance departments or data protection officers (DPOs) should be established. Referencing GDPR requirements, these roles should oversee data processing activities, respond to regulatory inquiries, and develop internal rules and regulations covering the entire process of data collection, transmission, storage, use, and destruction. For example, consider the approval process for cross-border data transfers and the frequency of risk assessments.

For technical support, adopt technologies such as privacy-preserving computation and federated learning to ensure "data is available but not visible." In particular, when financial companies share cross-border credit data, they should use encryption algorithms to protect personal privacy, improve data security standards, and enhance the trust of overseas partners through international certification.

For external collaboration, small and medium-sized enterprises can leverage the power of industry associations to establish cross-border data compliance alliances, share information on target countries' regulations, compliance cases, and other information, and reduce individual compliance costs. The Internet Society of China can organize the development of the "Guidelines for Cross-Border Data Compliance in Key Countries". Furthermore, strengthen third-party supplier management. When selecting cloud service and data processing providers, consider data protection capabilities as a supplier entry criterion. Contracts should clearly define the compliance responsibilities of both parties to prevent potential consequences from third-party violations.

Regarding emergency response, enterprises should develop contingency plans for cross-border data security incidents and conduct regular simulation drills. In the event of a data breach, they should promptly report it to domestic and international regulators and inform the data subject, similar to the GDPR's 72-hour reporting deadline, to establish a rapid response system. Enterprises should integrate compliance concepts into their business models and consider data compliance a core competitive advantage, such as relying on compliance certification to gain international market access. This can foster trust in cross-border e-commerce, cross-border finance, and other sectors, achieving a virtuous cycle of security and development [17].

5. Conclusion

Corporate cross-border data compliance is a core issue balancing security and development in the digital economy. Its complexity lies in the systematic nature of domestic regulations, the divergent nature of international regulations, and the diversity of corporate practices. After more than a decade of exploration, China has established a compliance system centered around the Cybersecurity Law, the Data Security Law, and the Personal Information Protection Law. However, fragmented legal regulations, unclear definitions of key concepts, and inadequate alignment with international regulations have not been completely addressed. This has led to rising compliance costs for businesses and increased enforcement difficulties. Practices in developed countries such as the United States, Europe, and the ASEAN region demonstrate that cross-border data compliance requires a dynamic balance between openness and security. Regarding cross-border data compliance, the United States relies on the Clarifying Lawful Overseas Use of Data Act (the "CLOUD Act") to exercise "long-arm jurisdiction." The CLOUD Act, formulated based on a "data controller standard," requires that data be submitted to the United States, regardless of where the data is physically stored, as long as the data controller is headquartered in the United States or registered as a company in the United States. The CLOUD Act overcomes existing barriers to local data storage, granting the US government the right to bypass the principle of reciprocity and directly access overseas data, demonstrating its unilateralist approach. The United States is leveraging "long-arm jurisdiction" to expand data sovereignty, encouraging companies to cooperate with cross-border data law enforcement requests. Regarding cross-border data transfer, while reshaping transatlantic data flow mechanisms through instruments such as the Transatlantic Data Privacy Framework, the United States has similarly used "long-arm jurisdiction" to safeguard U.S. data interests, imposing significant constraints on overseas companies. The United States' fragmented regulatory framework and "long-arm jurisdiction," the EU's "adequacy determination" centered around the GDPR, and ASEAN's flexible frameworks through the RCEP and DEPA offer governance strategies for countries at different stages of development. China should improve relevant policies and regulations, clarify data classification and grading standards, establish interdepartmental coordination mechanisms, and align with international rules. At the implementation level, China should emulate the U.S. strategy of combining firmness with flexibility. Companies should meet compliance requirements by building local data centers and implementing categorized and graded management, while regulators should impose severe penalties such as high fines for violations to create a deterrent. The United States' review, notification, and transparency reporting mechanisms for responding to law enforcement requests can also be used as a reference. Companies must build a comprehensive compliance system, enhance their technical support capabilities, and strengthen their international collaboration capabilities to unlock the value of data while ensuring data security, enhance the competitiveness of Chinese companies in the global digital economy, and provide a "Chinese solution" for global data governance.

References

[1] Lai, X. and Ma, S. (2024) Problems and Improvement of Compliance Governance for Cross-border Commercial Data Flow. Administrative Reform, (4), 43-53.

[2] Wu, X., Chu, J. and Fu, J. (2024) Research on Risk Prevention and Control of Cross-border Flow of Enterprise Data. Credit Information, 42, 41-49.

[3] Yang, Y. (2024) Research on compliance of cross-border flow of enterprise data. Master's Thesis, Lanzhou University.

[4] Chen, S. (2024) Research on the legal regulation of cross-border data flow in our country. Master's Thesis, Chinese People's Public Security University.

[5] Hu, H. and Geng, Q. (2023) Research on the governance of cross-border data flows: Traceability, context and trends. Intelligence Theory and Practice, 46, 178-186.

[6] Mei, A. and Pan, Z. (2024) Governance model, problem review and compliance approach of enterprise cross-border data compliance. Intelligence Theory and Practice, 47, 60-67.

[7] Li, J., Zhao, R. and Fan, Y. (2023) Our Country Governance Effectiveness, Problems and Suggestions for Improvement of Cross-border Data Flow. International Business Research, 44, 84-95.

[8] China Research Institute Puhua Industry Research Institute (2025) 2025-2030 China Fintech Industry Dynamic Research and Market Profit Forecast Report. Retrieved from https: //m.chinairn.com/hyzx/20250304/180037223.shtml.

[9] Liu, Y. and Song, G. (2024) DPF US and European Cross-border Data Flow Rules Game and Its Mirror. World Economic Research, (7), 29-42.

[10] Zang, Y., Mei, Q., Zhang, J., et al. (2025) The Generation Mechanism of Safety Production Governance Efficiency from the Perspective of Supply Chain Network: A Multiple Case Study Based on Resource Dependence and Resource Management Theory. Science and Science and Technology Management, 46, 87-106.

[11] Zhang, X. and Zhu, Y. (2024) The Evolution and Enlightenment of the Legal System of Personal Data Protection in the United States. Journal of Wuhan University of Science and Technology (Social Sciences), 26, 60-76.

[12] Global Network (2025) California Jury Finds Google $315 Million in Damages for Abuse of Android User Data. Retrieved from https: //www.toutiao.com/article/7522356400656335423/?upstream_biz=doubao& source=m_redirect.

[13] Liu, J. (2022) Towards Global Regulation of Cross-Border Data Flows: Fundamental Concerns and China's Plan. Administrative Law Research, (4), 73-88.

[14] Li, M. (2021) China-EU Cross-border Data Flows Cooperation in the Context of China-US-EU Triangle Game. European Studies, (6), 1-24.

[15] Yan, X. (2021) Data Compliance from the Perspective of Cybersecurity: Basic Theories, Problem Examination and China's Plans. Shanghai Law Research, (8), 33-40.

[16] Cyberspace Administration of China (2022) Measures for the Security Assessment of Cross-border Data Transfer. Retrieved from https: //www.gov.cn/gongbao/content/2022/content_5707283.htm.

[17] Zhang, X. (2020) Models and References for the Construction of Data Sovereignty Rules: On the Rule Construction of Data Sovereignty in China. Modern Law, (6), 136-149.