Frontiers in Business, Economics and Management
ISSN: 2766-824X | Vol. 19, No. 1, 2025

Research on the Legal Protection of Cross-Border Personal Information Flow under the Holistic View of National Security

Linqi Li, Zhanya Zhao

School of Law, Henan Normal University, Xinxiang 453007, China

Abstract: The cross-border flow and commercial utilization of personal data are central to the globalization of the digital economy. The concept of "cross-border data flow" first appeared in the Organisation for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data in 1980, which initially applied solely to personal data. Since the 21st century, the cross-border flow of data has facilitated global economic integration and innovation, strengthening international collaboration and information sharing. While generating numerous positive effects, cross-border data flow has increasingly complex implications for national security and individual privacy. The need to safeguard national data sovereignty and protect the personal privacy of citizens is paramount, as individuals face heightened risks of personal information leakage and misuse. Furthermore, differing legal and regulatory frameworks concerning personal data across various countries and regions pose legal risks and compliance challenges for cross-border data flows, thereby impacting the protection and security of personal information. In addition, cross-border data flows have given rise to global data security issues that necessitate international cooperation and coordination to address.

Keywords: Personal information; Cross-border data transfer; Rule of law-based regulation.

1. Introduction

The rapid advancement of big data technology has led to a continuous increase in the commercial value and strategic significance of personal information. In daily life, users often must accept the privacy policies set by various application software to use them. However, most users do not carefully review these standardized privacy agreements, which creates opportunities for internet platforms to illegally collect user personal information. Some platforms, after obtaining personal information, engage in unauthorized illegal transactions. Data enterprises, relying on increasingly sophisticated data tracking and analysis technologies, can accurately capture the personal positioning of data subjects. Cross-border data transactions are frequently prohibited, and incidents of personal privacy leakage occur frequently. Ensuring the security of personal information has become an important task in the supervision of cross-border data flow.

Regarding the regulatory issue of cross-border transmission of personal information, China currently adopts a regulatory model centered on "local storage + outbound assessment." However, as a latecomer in data security governance, the construction of China's regulatory system for cross-border flow of personal information is still in its initial stage, lacking theoretical foundation and practical experience. Therefore, a series of risks and challenges are encountered in the process of cross-border transmission of personal information. Specifically, the laws and regulations on the cross-border flow of personal information are relatively fragmented, lacking a unified and coordinated top-level design. The rules for protecting personal information in cross-border data flow are not detailed enough, leading to insufficient support in practical application. At the same time, international regulatory cooperation on the cross-border flow of personal data is disconnected, which can easily put China in an unfavorable position in the globalized data governance system.

2. Refining the Legal Framework for Cross-Border Transfers of Personal Information

A comprehensive, detailed, and logically consistent legal regulatory framework for the cross-border transfer of personal data is of paramount importance for safeguarding national data sovereignty, fostering the development of the data industry, ensuring the security of personal information, and advancing the construction of a rule-of-law-based China. From a legislative perspective, China's regulations concerning the cross-border transfer of personal data were introduced relatively late and lack systematicity. Under the strategic impetus of "Digital China" and "Rule of Law China," China's legislation related to personal information has seen the preliminary formation of a legal framework supporting compliant governance of cross-border data flows, with the successive promulgation of foundational laws such as the Cybersecurity Law, the Data Security Law, and the Personal Information Protection Law [1]. Since 2022, further refinements have been made to the construction of the personal data cross-border flow system through the promulgation of relevant detailed rules, including the Measures for Security Assessment of Data Export, the Measures for Standard Contracts for Personal Information Export, the Implementation Rules for Personal Information Protection Certification, and the Security Certification Specifications for Cross-border Processing Activities of Personal Information. However, as a latecomer in data security governance, there remains room for improvement in China's legal regulation of cross-border data flows [2].

2.1. Enactment of Legislation to Regulate the Cross-Border Movement of Personal Information

Since 2016, China has successively promulgated legal instruments including the Cybersecurity Law, the Civil Code, the Data Security Law, and the Personal Information Protection Law, thereby establishing a preliminary governance framework for the cross-border transfer of personal data. However, these documents primarily consist of principles, and their legal hierarchy remains ambiguous. The specific details and challenges encountered in practice have not been sufficiently elaborated or addressed in these legislative acts, which often leads to difficulties in implementation due to a lack of operational clarity.

The Cybersecurity Law introduced the initial stipulations concerning cross-border data transfer. However, it only mandates data localization and security assessments for the operators of critical information infrastructure, without specifying operational guidelines [3]. In 2017, the Cyberspace Administration of China issued the "Guidelines for Security Assessment of Personal Information and Important Data Outbound," mandating security assessments for all outbound transfers of personal information and important data. Nevertheless, the guidelines lacked explicit standards and procedures for these assessments. Furthermore, the Data Security Law, promulgated by the state, prioritizes the security of important and core data during outbound transfers, yet it does not provide clear definitions for the scope and meaning of "important data." The Personal Information Protection Law dedicates a specific chapter to regulating the cross-border transfer of personal information, but it does not clarify how to address issues such as security assessment standards, information certification standards for professional institutions, and standard contract templates during implementation. The "Measures for Security Assessment of Data Outbound" provides detailed regulations on the evaluation criteria for data export, clearly defining the assessment conditions and procedures. However, further scrutiny is required to ascertain the practical applicability of these provisions. Within the Chinese legislative framework, while the Civil Code and the Cybersecurity Law have established an initial structure for personal information protection, the Personal Information Protection Law (PIPL) has broadened the scope and depth of this protection. To enhance the legal regulation of personal information, consideration should be given to more effective stipulations regarding the legal nature of personal information, such as the establishment of "personal information rights," thereby providing a fundamental basis for the rights of personal information subjects [4]. It is also noteworthy that the infringement of personality rights and property rights during the cross-border flow of personal information should be given sufficient attention. Clear delineation of the remedies available to information subjects for infringements or breaches arising from cross-border personal information processing activities is essential to safeguard their agency in resolving personal information disputes. This approach prevents an over-reliance on public law remedies, which could limit private rights of action and exacerbate the burden on public law redress. In terms of the infringement relief mechanism, incorporating the legal concept of "future harm" could be considered to facilitate the prevention of infringement risks and provide effective compensation for actual losses, thereby achieving the dual functions of prevention and compensation.

Compared to the Civil Code and the Cybersecurity Law, the Personal Information Protection Law expands the scope of protection of personal information, but personal information is still in the legal status of "interests" [5]. In order to strengthen the effect of private law regulation, it is possible to consider making more effective provisions on the legal attributes of personal information, such as the "right to personal information" , which gives the subject of personal information the basis of rights. In addition, the risk of infringement of personal information's personality interests and property rights and interests is involved in personal information exit activities, and it should be made clear that the subject of personal information can initiate infringement or breach of contract remedies for such infringement, so as to prevent the initiative of resolving personal information disputes from being limited due to the too small private rights of action, and to prevent the burden of remedies under public law from being overly burdensome. For tort remedies, the concept of "future damage" can be introduced to achieve the dual purpose of risk prevention and compensation for damages.

2.2. Clarify the Criteria and Methods for the Exit of Personal Information

Against the background of the increasingly frequent and diversified cross-border flow of personal information, a single typology of personal information processors may seem to simplify the supervisory process, but in practice, such simplification often makes it difficult to appropriately reflect the complexity of cross-border flow of personal information and the diversity of practices in concrete operation. In the author's view, the classification of personal information processors can be regulated by law, adopting a more refined and dynamic approach, taking into account the actual type of cross-border personal information processing activities, the nature of the recipient outside the subject as well as the purpose of the transmission and other factors, to form a diversified and three-dimensional regulatory system, and to enhance its relevance and practicality. On this basis, the specific scenarios of exemption from supervision shall be further refined and perfected to make the supervision more flexible and efficient. Meanwhile, for the three existing regulatory mechanisms for cross-border transmission of personal information —security assessment, protection certification and standard contract, it is necessary to clarify their respective positioning and scope of application, and to formulate more detailed regulatory rules from the legislative level in light of their respective characteristics. Among them, protection certification, as a regulatory tool, should continue to be clarified in terms of its scope of application and practical operation, especially regarding the specific handling of the provisions of Article 3(2) of the Personal Information Protection Law, which should be effectively differentiated from the application of the net contract. The standard contract plays an indispensable role in regulating the responsibilities and obligations between the processor of personal information and the overseas recipient, and in controlling the subsequent risks of cross-border information processing. From this, it is clear that unchanging provisions cannot meet the needs of actual practice, and should be refined and adjusted according to the specific conditions of cross-border flow of personal information.

2.3. Strengthening the Extraterritorial Effect of the Rules on the Exit of Personal Information

In order to safeguard the extraterritorial security of personal information interests, China should clarify and refine the extraterritorial effects of legal norms before personal information leaves the country, and provide a legal basis for relevant dispute resolution as early as possible [6]. In accordance with Article 3(2) of the Personal Information Protection Law, China's regulatory management of personal information in the process of cross-border flow significantly reflects the extension of the extraterritorial jurisdiction of domestic law over foreign activities. Therefore, China's legal system should be supplemented with more detailed procedural and substantive provisions on the extraterritorial effect of the management of personal information after its cross-border flow. At the procedural level, the grounds for determining jurisdiction should be specified, and the principles of territoriality, personhood, protectiveness and universal jurisdiction should be fully applied to provide diversified legal protection for the security of personal information. At the same time, the recognised jurisdictional principles of international law should be used as a basis to avoid violating the prohibitions in international law. As well, the provisions of Article 3(2) of the Personal Information Protection Act include indirect obligations on the recipients of personal information outside the country. In addition, in the face of some developed countries abusing their jurisdiction to obtain personal information within our country's borders, we should formulate countermeasures and blocking methods. The blacklisting system in the Personal Information Protection Act is an innovative measure that provides for the establishment of a "restricted or prohibited list of personal information" in response to any country or region that "adopts discriminatory prohibitions, restrictions or other similar measures". This is in response to any country or region that "adopts discriminatory prohibitions, restrictions, or other similar measures" and thus establishes "reciprocal measures" [7]. To this end, it is recommended that, based on the blacklist system, the specific enforcement measures to block the improper acts of other countries be further enriched and improved in conjunction with the Measures for Blocking the Improper Extraterritorial Application of Foreign Laws and Measures and the Anti-Sanctions Law [8].

3. Refining the Rules for the Protection of Personal Information in Cross-Border Data Flows

3.1. Optimising the Security Assessment Rules for Cross-Border Movement of Personal Information

The restrictions on the exit of personal data from China under our legislation are designed to guarantee an equivalent level of protection for our personal data after cross-border transfers and to prevent them from being improperly processed or utilised. At the international regulatory level, the European Union (EU) General Data Protection Regulation (i.e. GDPR) stipulates that the recipient of cross-border personal data must be a third country that has received a "determination of adequacy" from the European Commission, and the criteria for determining the adequacy of the determination are set by the European Commission on its own. It is worth noting that there are not many third countries and regions that can obtain the EU's "adequacy determination", and this restriction can provide support for the EU to be able to obtain the same level of protection for the personal data of its own citizens during cross-border transfers [9]. China has adopted more stringent and detailed requirements in this regard, setting more specialised and specific legislative regulations for the process of cross-border transmission of personal information. In particular, for operators of critical information infrastructures and those who have met the quantitative standards for personal information processors set by the State Internet Information Office, they must undergo and pass a security assessment in China before engaging in the cross-border transmission of personal information. While this security assessment is directly aimed at the processors of personal information within the country, it also indirectly completes the assessment of the recipients of that data outside the country. Like the EU regulations, China also requires recipients of cross-border data to meet the same level of personal information protection as in China [10]. This approach practice has likewise been adopted and implemented by other countries such as Singapore.

In terms of optimising the security assessment rules for the cross-border flow of personal information, it is important to crystallise and strengthen the risk level-oriented framework for the outbound management of personal information. According to the level of risk and potential impact of different types of personal information, we should establish a specific and dynamic personal information risk classification system, considering the nature of various types of information subjects and the specificity of the industry, and formulate corresponding classification and protection standards for sensitive personal information. Through this hierarchical classification, the governance of cross-border flow of data can be effectively guided, and the systematic protection of outbound flow of personal information can be enhanced. For personal information flowing across borders, differentiated regulatory measures must be taken according to its risk level and actual transmission route, such as the imposition of strict outbound restrictions and the strengthening of the registration and filing system. At the same time, risk assessment and early warning mechanisms for dynamic monitoring play a crucial role in identifying, preventing and controlling potential risks in advance. In particular, for sensitive personal information subject to flow restrictions, data receivers should assume the important responsibility of real-time supervision to ensure that the data remains under continuous and effective protection outside the country. On this basis, relevant enterprises or organisations should regularly submit reports on the security status of cross-border flow of personal information to the State Internet Information Office or other competent authorities, and be subject to filing and review. In view of the fact that personal information may be re-transferred after leaving the country, which may result in complex risks such as privacy leakage, it is important to establish strict regulatory requirements for the transfer of personal information received by a data recipient to a third party, including, but not limited to, ensuring that the data recipient provides the third party with a comparable level of personal information protection safeguards. If the rights and interests of personal information are infringed upon, the data recipient and the third party shall assume joint and several legal liability in accordance with relevant laws and

regulations. Through the detailed regulation of the whole process, it provides a full range of legal protection and technical support for the cross-border protection of personal information, ensuring the safety of personal information flow and the inviolability of individual interests.

3.2. Exploring Models of Standard Contractual Terms for Cross-Border Transfers of Personal Information

The model refers to the exit of personal data upon the conclusion of a standard contract (terms) [11]. The standard contractual clause model, as a model with normative nature, may become an important way of cross-border transmission of personal information in China in the future [12]. Considering the continuous improvement of personal information protection laws and regulations both at home and abroad, it is particularly urgent and necessary to establish a set of standard contractual clauses with both practicality and foresight. In the construction of standard contractual clauses in China, we can take the Standard Contractual Clauses (SCC) model of the European Union as a reference, which has rich practical experience and mature legal system support in ensuring the security and legality of cross-border transmission of personal information. The model has rich practical experience and mature legal system support in ensuring the security and legality of cross-border transmission of personal information. The model should be adjusted and optimised locally in accordance with the status of the legislation and practical needs of personal information protection in China, to better adapt to the domestic and international legal environment and market demand.

When choosing the type of contract, we should focus on the type of contract that shows higher risk characteristics, especially for key industry sectors (such as finance, medical care, education, etc.), the standard contract terms in these fields are more stringent and detailed than in ordinary fields, so that the security and privacy of personal information can be adequately safeguarded. The specific content of the standard contract terms should comprehensively cover key elements such as the purpose and destination of the personal information leaving the country, the laws and regulations followed by the recipient, the way the data is stored and processed, as well as the specific rights and obligations of the data provider and the recipient. This not only helps both parties to clarify their respective responsibilities and obligations, but also helps to enhance transparency and credibility in the data transfer process. Further, in order to facilitate the orderly and efficient flow of personal data between the transmitting parties, the standard contract terms should also be designed to provide both mandatory and optional clauses. Such a design not only ensures the basic framework and core principles of the standard contract terms, but also provides different types of data processors with the possibility of flexible choices, assisting them to find the most suitable mode of cooperation in accordance with their own circumstances and needs. In addition, given the complexity and dynamic nature of the personal data protection and cybersecurity fields, the standard contractual terms should also include additional requirements for privacy protection and cybersecurity measures. In this way, the security of data processing activities can be further strengthened and the risk of leakage and misuse of personal information can be effectively prevented and reduced.

3.3. Improvement of Personal Information Protection Certification System

Further improve the certification mechanism and strengthen the foundation of the personal information and data security protection system. China's certification of cross-border flow of personal data is a voluntary certification implemented by the state with the basic orientation of implementing the requirements of the Personal Information Protection Law, which is the fundamental system of the personal information protection system. 2022 In December 2012, the CITIC Standards Committee released the "Cybersecurity Standard Practice Guideline I Security Certification Specification for Cross-border Processing Activities of Personal Information V2.0" (Certification Specification V2.0). Compared with the certification mechanisms for cross-border flow of data in regions or countries such as the EU, Asia-Pacific Economic Cooperation, ASEAN, Singapore, etc., China's certification mechanism for cross-border flow of data has already presented Chinese characteristics in terms of value orientation, regulatory model, etc., but there is still room for further refinement and improvement [13].

At present, although China's cross-border data flow certification mechanism has formed a full-process certification model that includes information review, competence audit and continuous supervision, compared with Europrivacy certification, it is still necessary to explicitly take "compliance support" as the first step in the certification process to meet the needs of the digital economy, and to form a "compliance support + technical validation + on-site audits + post-certification supervision" certification model. Unlike the standard contract (terms and conditions) mechanism, which can directly bind overseas recipients by signing contracts, the current certification mechanism for cross-border flow of data can only bind domestic certified subjects, which also leads to difficulties in controlling data security risks, remedial measures and accountability after cross-border flow of data. Therefore, it is recommended to further expand the certification subject, allow domestic subjects to publicise their level of data protection and compliance through certification, and apply the review standards and processes to foreign subjects, to conduct prior assessment of data recipients and strengthen risk control. As a framework document for the certification mechanism, the Certification Code V2.0 embodies the basic principles and standard functions of industry certification, but there is still a lack of specific provisions on scoring items and process operation. It is recommended to base on the various aspects of the certification procedure and the subjects involved, to refine the details of the certification, and to constitute a full-cycle, full-process, explicit data cross-border certification mechanism. At the same time, the risk management logic of the authentication mechanism should be clarified to improve the multi-risk prevention and supervision system of cross-border data flow [14]. Because China's certification mechanism has yet to be further refined and practically verified, while the certification systems of other countries are diverse and very local in character. For China, on the one hand, we can learn from the advanced foreign certification experience, develop and improve China's third-party certification system, further expand and highlight the important role of third-party certification in the management of cross-border flow of data, and give full play to the international mutual recognition

mechanism of certification as far as possible. On the other hand, we should also actively engage in international exchanges and co-operation, promote the reaching of an international consensus on the governance of cross-border flow of data, establish a regionally integrated system of cross-border flow of data, and actively explore the formulation of the provisions on cross-border flow of data in bilateral free trade agreements, so as to continuously enhance the right of discourse on the governance of cross-border flow of data.

4. Active Participation in Cross-Border Global Governance of Personal Information

In the area of international cooperation, it is necessary to implement the concepts contained in China's overall concept of national security. The overall concept of national security embodies the global security initiative based on the concept of a "community of human destiny" and the value of building a "human security community". Among them, the concept of "international security", as the basis for the "five elements" and "five pairs of relationships" in the overall concept of national security, stresses the core concepts of universality, equality, inclusiveness and cooperation, and advocates the extension and leapfrogging of the space for national security governance from the traditional "national centre" to the future direction of "international integration". While actively safeguarding national security and data sovereignty, China should also proactively seek international cooperation and contribute Chinese wisdom and strength to the improvement of the rules governing the cross-border flow of international personal information and global data security governance.

4.1. Implementation of China's Personal Information Protection Certification "White List" System

At present, China promotes international regulatory cooperation on the cross-border flow of personal data, mainly through the Belt and Road Initiative and bilateral and multilateral free trade agreements. However, in building the Digital Silk Road, China is constrained by the level of digital infrastructure in countries along the route, making it difficult to overcome the data divide and develop regulatory cooperation on cross-border flows of personal data. In addition, among the agreements reached between China and 19 free trade zones, only the RCEP involves regulatory cooperation on cross-border flow of data, while other agreements such as the China-Korea Free Trade Agreement and the China-Australia Free Trade Agreement only provide for personal data protection in principle, which makes it difficult to effectively promote the internationalisation of China's regulatory rules and the normalisation of regulatory cooperation. As mentioned earlier, according to the "adequacy determination" rule, the EU has included 14 countries and regions with equivalent personal data protection standards in the "white list" of cross-border data flows, however, China is not included, which means that the EU occupies a high position in the export of regulatory rules on cross-border personal data flows. However, China is not included, which means that the EU occupies the high ground of exporting regulatory rules on cross-border personal data flows. In this regard, China can learn from the "adequacy determination" rule, extend the scope of application of data security protection certification to international subjects such as countries and international organisations, and based on the principle of reciprocity, include countries and regions with a higher level of data protection in China's "white list" of data protection certification on the basis of scientific assessment. White List" of China's data protection certification.

ASEAN countries play a key role in the Belt and Road Initiative, and in order to promote collaboration, China can prioritise bilateral cooperation with ASEAN countries by signing memorandums of understanding, setting up cross-border certification standards for personal information, and other regulatory measures. China's cooperation with ASEAN countries, with its geographical advantage and cooperation mechanism, provides an opportunity for China to cooperate with the EU on cross-border issues related to personal information in the future. In addition, to address the problems of cross-border data transmission, we can rely on the countries (regions) along the "Belt and Road" to provide targeted solutions to establish a set of unified data transmission formats and standardised "white lists" to ensure the traceability and interoperability of personal information out of the country. Establish a set of unified data transfer formats and standardised "white lists" to ensure the traceability and interoperability of personal information out of China, and strengthen the influence of China's personal information out of China regulatory system. In the pilot project on the safe management of cross-border data transmission, priority can be given to the implementation of the "whitelist" system, and the practical experience of the rule of law in the regulation of personal information exit in Beijing, Shanghai, Hainan and Xiong'an New Area can be summarised, to provide reference for the implementation of the system nationwide. In order to further regulate the cross-border data behaviour of foreign-related enterprises, China can take the lead in formulating templates for personal information protection commitments and encouraging enterprises to consciously accept the regulation in their personal capacity. This initiative will help China reach a bilateral agreement on cross-border data flows with trading partner countries, while also expanding channels for international regulatory cooperation through the establishment of Chinese standards, and facilitating the effective interface between international agreements and domestic rules to safeguard the security of data transfers.

4.2. Building a "China Programme" for the Internal and External Linkage of Cross-Border Transmission of Personal Information

At present, our country has become an important member of the global economic system. We have made great strides in the areas of international trade and investment and are actively participating in the operation of the global digital economy. We understand data is the core of the digital economy, and the cross-border flow of personal information will be an inevitable trend in the development of the digital economy. Therefore, we must strengthen the construction of regulations related to the cross-border flow of personal information in order to protect the security of personal information and privacy of Internet users. Now, China has successfully joined the RCEP, which is an important step for China to participate in the construction of the international data rule system. With the accession of RCEP, the trade, investment and cooperation in the field of digital economy between China and its neighbouring countries will be

developed more deeply and extensively.RCEP is in line with our concept of regulation of cross-border flow of personal information. Therefore, in the future free trade negotiations, we can take the relevant provisions of RCEP as reference to formulate and implement China's concept of regulation of cross-border flow of personal information at the overall and strategic level. By strengthening cooperation and reaching consensus, we can establish an international environment conducive to the prosperous development of the digital economy and create a world where the digital economy thrives. This will not only be conducive to the development of China's digital economy, but will also certainly make positive contributions to the development of the international digital economy.

Making full use of the positive role of free trade zones such as Hainan and Shanghai, and using their early and pilot mechanisms as a leader, we will uphold the principle of free flow of data and ensure the smooth and orderly flow of information in the free trade zones with a huge digital scale. On the premise of public policy and basic national security, we will actively adjust China's regulations on the cross-border flow of personal information, promote the vigorous development of the information technology industry, and create a more favourable environment for cross-border cooperation and development of the digital economy. At the same time, a systematic and complete system of laws and regulations with clear powers and responsibilities will be established in the free trade zone, regulatory mechanisms and risk prevention measures will be strengthened, personal information security and privacy rights will be safeguarded, and a new mechanism for the flow of information will be constructed in line with international standards and China's national conditions, so as to promote the high-quality development of the digital economy and to provide strong support for the promotion of digital transformation.

To improve the regulation of cross-border flow of personal information in China, we should adopt a dual-track domestic and international strategy. At the domestic level, we need to further improve relevant laws and regulations and legislative mechanisms to ensure the compliant flow of personal information. At the international level, we should actively participate in global data governance and strengthen communication and cooperation with other countries and regions. As the world's second-largest economy and a major Internet country with enormous influence and resource advantages, China should actively participate in international data co-operation and promote international data exchange and sharing. We can sign data cooperation agreements with other countries, establish mutually recognised data flow mechanisms, and provide a more convenient data exchange environment for enterprises and individuals. At the same time, we should also actively participate in the construction of an international data governance system, showing Chinese wisdom and providing Chinese solutions to the world.

5. Conclusion

In the context of the globalisation of the digital economy, the cross-border flow of personal information has exacerbated national security risks, personal privacy leakage and legal compliance challenges while promoting international collaboration and innovation. At present, although the rule of law regulatory framework for the cross-border flow of personal information in China has been initially constructed, it still faces problems such as a fragmented legal system, insufficient operationalisation of the rules, and a weak international cooperation mechanism. These shortcomings not only weaken the effectiveness of the maintenance of data sovereignty, but also make it difficult for China to grasp the right to speak on rule-making in global data governance. To this end, it is necessary to take a two-pronged approach from the legislative and practical levels: on the one hand, by clarifying the legal attributes of the "right to personal information" , refining the security assessment and standard contracts and other supporting rules to enhance the operability of the law; on the other hand, it is necessary to introduce a dynamic regulatory mechanism of risk classification and classification to strengthen the extraterritorial effect of the law, and to enhance the effectiveness of the law with the help of the "blacklisting" mechanism. On the other hand, it is necessary to introduce a dynamic regulatory mechanism for risk classification, strengthen the extraterritorial effect of the law, and effectively deal with the improper jurisdiction of other countries by means of the "blacklist" system and the tool of blocking law.

In the future, the governance of cross-border flow of personal information should consider both domestic improvement and international synergy. At the domestic level, we should accelerate the integration of fragmented legal norms, promote the pilot experience of FTZs to the whole country, and build a regulatory system that takes into account both safety and efficiency; at the international level, we need to proactively participate in multilateral negotiations, deepen the cooperation with ASEAN and RCEP member countries, and explore the mutual recognition mechanism for the certification of the "whitelist" , so as to promote the integrated construction of regional rules on the flow of data. China, as an important participant in the global digital economy, is a major player in the global digital economy. As an important participant in the global digital economy, China should promote the orderly and open flow of data across borders on the basis of safeguarding data security and privacy rights, and contribute Chinese wisdom to global data governance by exporting governance solutions that are both inclusive and effective, so as to achieve a multi-dimensional balance between national interests, corporate innovation and individual rights.

References

[1] Zhu Lin, Research on Cross-border Data Flow Governance in the Era of Big Data, Soochow University Press, 2022 edition, p. 2.

[2] Xu Yongjun and Wang Xingguang, "Research on security Governance of Cross-border Data Flow under the Overall National Security Concept", in Library and Information Knowledge, No. 6, 2023, pp. 20-30.

[3] Zhang Yixin, "See China's Countermeasures from the External Regulation of Cross-border Data Flow", in Journal of Chongqing University of Posts and Telecommunications (Social Science Edition), No. 2, 2022, pp. 51-62.

[4] Zhao Jun and Yao Ruonan, "The Domestic Regulatory Path and System Improvement of Personal Information Exit", in Governance Research, No. 2, 2024, pp. 123-140 + 159-160.

[5] Zhang Xinbao and Ge Xin, "Measuring the Interests and Constructing the System of Legal Regulation of Face Recognition", in Huxiang Law Review, No. 1, 2021, pp. 36-51.

[6] Song Dingbo Nan and Wu Dezheng, "Study on Optimisation of the Regulatory System for Cross-border Flow of Personal

Data under the New Security Landscape", in Intelligence Theory and Practice, No. 3, 2024, pp. 54-61.

[7] Peng Yue, "The Trade Law Dimension of Cross-Border Data Privacy Protection", in Law Application, No. 6, 2022, pp. 16-28.

[8] Ding Hantao, "On the Enforcement Mechanism of the Blocking Law and Its Practice in China", in Global Law Review, No. 2, 2022, pp. 176-192.

[9] Yao Xu, The Governance of Cross-Border Data Flows in the EU, Shanghai People's Publishing House, 2019 edition, p. 12.

[10] Qiao Yide, "Study on Building a New Development Pattern of Double Cycle in Shanghai", in Science Development, No. 12, 2020, pp. 34-43.

[11] Jin Jing, "EU Standards for Cross-Border Transfers of Personal Data - Rule Construction, Judicial Promotion and Paradigm Expansion", in European Studies, No. 4, 2021, pp. 89-109+7.

[12] Chen Sheng and Wang Kexin, "Research on the Regulatory Issues of Cross-border Flow of Personal Information in the Age of Digital Economy", in China Business Journal, No. 24, 2023, pp. 44-47.

[13] Xing Huiqiang and Li Zehui, "China's Personal Data Cross-Border Flow Authentication System and Its Improvement", in Journal of Zhengzhou University (Philosophy and Social Science Edition), No. 6, 2023, pp. 54-60.

[14] Zhang Xiaojun and Liu Zeyang, "RCEP Basic Security Exception Provisions for Cross-Border Flow of Data and China's Programme", in Journal of Zhengzhou University (Philosophy and Social Science Edition), No. 4, 2023, pp. 36-42+127.