Analysis of the Legal Regulation of Cross-border Flow of Financial Data in China

[1]Peng Qi, [2]Yuanqi Sun

[1]15339228678@163.com, [2]sunyuanqi66@163.com

Xi'an Jiaotong University, No. 28, Xianning West Road, Xi'an,Shaanxi 710049, People's Republic of China

Abstract. In the digital economy environment, the cross-border flow of financial data has become increasingly important, but a unified regulatory mechanism has not been formed in the world, which brings obstacles to the flow of transnational financial data. Differentiated free trade agreements (FTA) can have different effects on the transnational flows of financial data. China has a huge demand for the cross-border flow of financial data, but the potential risks can not be ignored. This paper aims to establish an effective regulatory regime to ensure data security and maximize its economic value. Considering that China's construction and participation in the supervision of cross-border financial data flow is still in its infancy, it is necessary to improve the supply level of the rules of the free trade zone, so as to promote the healthy development of China's financial service trade. Through the method of literature review and case analysis, the regulatory system of financial data flow is deeply studied. On the one hand, the existing literature is reviewed and analyzed to understand the current situation, problems and solutions of the cross-border flow of financial data; on the other hand, to explore the practice and experience of different countries in the cross-border flow of financial data. Overall, establishing an effective regulatory system is the key to ensuring the security of financial data and maximizing its economic value. In terms of cross-border flow of financial data, it is necessary to start from the two aspects of cross-border flow of financial data and data security to improve the supply level of free trade zone rules, so as to promote the healthy development of China's financial service trade.

Keywords: international economic and trade rules · trade in financial services · cross-border data flow

1 Introduction

As the core of contemporary economy, finance plays a pivotal role in the process of global economic integration. The rapid development of modern information technology, network technology and cloud computing technology has made a new pattern in the production, exchange and consumption of financial data in cross-border financial transactions. With the continuous development of data mining and cloud computing and other technologies, the processing and computing power of financial data has been greatly improved.However, because technology is continuously in flux, it is impossible to accurately assess the impact of cross-border data flows on trade without knowing the future developments in technology and because of the "pre-internet" trade agreements in place. [1]The cross-border flow of financial data brings huge economic benefits in the process of promoting the globalization and regionalization of

MSIEID 2023, December 08-10, Guangzhou, People's Republic of China

DOI 10.4108/eai.8-12-2023.2344822

financial data, but also has structural risks, so it is necessary to prevent and supervise. Based on this, this paper intends to start with the analysis of the causes and risks of cross-border flow of Chinese financial data, study the legal norms and regulatory purposes of cross-border flow of international and regional financial data, and try to establish a set of legal supervision system of cross-border flow of financial data suitable for China's national conditions.

2 The Necessity of Cross-border Flow of Financial Data

2.1 Cross-border Data Flow is the Internal Demand of the Development of Financial Service Trade itself

Firstly, cross-border financial data flows generate huge economic benefits, which is the internal power of cross-border data flows. At the same time, the relevant financial institutions have also established a relatively perfect database and calculation system, through the different types of user behavior, consumption habits, transaction records, biological characteristics of analysis and processing, build user portrait, achieve accurate marketing, risk control, differentiation decision, etc., creating huge economic benefits.

Secondly, it is an important trend of the current development of financial market to integrate and transmit financial information, especially to domestic and foreign institutions within the prescribed time limit to realize financial transactions. On the one hand, with the rapid development of cross-border payment industry, the fintech represented by blockchain has helped cross-border payment to achieve a disruptive leap; on the other hand, the overseas listing of the company will involve a large amount of investment amount and customer scale, including customer assets, annual income and other very sensitive financial data. This may lead to a cross-country flow of financial information after public offerings or issuance.

2.2 Cross-border Flow of Data is the Inevitable Result of Fintech Progress

Firstly, with the development of digitalization and networking, the localized storage of financial data has been realized. This allows domestic financial institutions to set up dedicated data centers abroad, or rent the cloud servers of IT enterprises, or sign hosting agreements to store the data abroad for a long time. Secondly, the data-sharing methods brought about by technological development, such as open banks, provide the impetus for the flow of financial data across borders. Under the open banking model, commercial banks open their financial data to their partners through API (Application Programming Interface), SDK (Software Developmentkit), etc. Users can easily implement account inquiry, loan application, mobile payment and other services in different application scenarios. Third, in the open banking system, a large number of transactions and information recipients are involved, and the outflow of financial information is inevitable. For example, a multinational company that needs to do business in China could allow its wholly owned subsidiaries in China to do business with other companies in China. In this context, the wholly-owned subsidiaries of multinational corporations often outsource the data processing work, and massive financial data will be generated in the transaction process, thus constituting the cross-border flow of financial data.

2.3 Cross-border Data is a Necessary Cooperation for Overseas Supervision and Judicial Behavior

In the fields of finance, healthcare and education, for example, the cross-border circulation of data often involves complex business practices and legal relationships. Without an effective and cross-border data cooperation mechanism, overseas regulators and judicial authorities will be difficult to obtain key evidence, which will undoubtedly greatly weaken their law enforcement effect. In addition, the cross-border flow of data may also cause serious problems such as transnational fraud and cyber crime, which may be impunity without timely data sharing.

3 Status and Problems of Cross-border Flow of Financial Data in China

3.1 The Development Status of Legal Regulation on Cross-border Flow of Financial Data in China

Cross-border financial activities will inevitably generate cross-border financial data flows, which will not only promote economic exchanges among different countries, but also cause data security issues such as individual and enterprise data security, and national data security. At present, there is no special legislation for the cross-border flow of financial data in China, and only the three laws of Network Security Law, Data Security Law and Personal Information Protection Law are [2]. Accordingly, the analogy can be applied to China's supervision of cross-border financial data. Therefore, the transmission of cross-border financial data in China must comply with the relevant provisions of these three laws.

Article 37 of the Cyber Security Law states that units engaged in telecommunications services in China must undergo a security evaluation if they need to transmit abroad. Article 66 of this law stipulates, to the unit or unit, impose 500,000 yuan above 500,000 yuan, can revoke business license, and can impose 100,000 to 100,000 yuan to concerned personnel."Data safety law" article 2 has been clear about the data management in domestic harm to national interests behavior, and clear the relevant state authorities in accordance with their own laws to review the requirements of foreign agencies for domestic data, and not approved by the competent department of any organization and individual cannot pass to foreign storage data in our country. Article 48 of the law provides corresponding penalties for the violation of Article 36 of the Data Safety Law. Article 36 of the Personal Information Protection Law stipulates that the personal information collected by state institutions must be kept in China, and when necessary, it must pass the safety evaluation of the relevant departments.

According to the above data security status quo and the basic spirit of the three laws, China's Data Exit Security Assessment Measures was issued and implemented on July 7 this year, which aims to promote data security and free cross-border flow. The measures stipulate that the cybersecurity committee must conduct security evaluations of data involving cross-border transmission in accordance with the requirements of the Regulations. The Measures specify four situations, so that the cross-border flow of ordinary data can be protected by law, but they do not specify the cross-border flow of financial data. China's financial system has corresponding regulations and measures in anti-money laundering, online payment, credit rating and personal financial information protection, which protect different levels of financial information, so as to

clarify the bottom line of data governance and realize governance under the protection of the whole data chain.[3].In addition, China has also participated in many international organizations, including the China-Europe Free Trade Agreement and the Southeast Asia Free Trade Agreement, which in principle require keeping its financial data in its territory to ensure its financial security.

3.2 Supervision of Cross-border Flows of Financial Data

China's cross-border financial data flow is increasingly large, if improperly regulated, will have a negative impact on national economic security. Therefore, the regulation of cross-border financial data is a manifestation of the implementation of national data sovereignty. However, if financial data is improperly regulated, it may destroy the global economic cycle, thus having a negative impact on China's economic interests.

Firstly, the data sovereignty risk brought about by the cross-border financial data flow. In terms of data exit, it mainly involves the problem of cross-border transmission of data when processing data by private rights subjects; in the data exit situation handled by private entities, the exit control measures formulated according to different places form various complex and diverse control modes, which risk the data to be reused.

In terms of data retrieval, it mainly focuses on the access and use of data by the public power subject. In the data transfer scenario of the public power subject, if the relevant important financial data is involved, China has always adhered to the principle of free flow in the attitude of overseas data transfer, and tries to avoid unilateral exercise of power. However, by virtue of its legislative advantages, the EU maintains data sovereignty in the world, and successfully promoted the "EU standards" as "international standards" through legislative measures to expand its jurisdiction, so as to realize the remote jurisdiction of overseas data. The United States, with its technological advantages, further implements "Electric Curtain Action" and uses the "honeycomb" platform and quantum attack system through the "Anger Project" and "Star Wind Project" for large-scale access to global data. Such behavior leads to a disorderly flow of data across the world, posing a serious threat to national security. Without the protection of national data sovereignty, it is difficult for personal financial data rights to get effective relief.

Secondly, the regulation of cross-border flows of financial data that exceed security needs can hinder economic development. Whether from the legal norms of cross-border flow of financial data in China, or from the various international trade agreements signed by China, there is no perfect governance system for cross-border flow of financial data. In 1980, the OECD issued the Guide on Privacy Protection and Cross-border Flow of Personal Data, which proposed minimum restrictions on personal information collection [4]; European and American countries used the advantages of global information technology to promote the free circulation of financial data; after the financial crisis in 2008, the international community paid attention to the transnational leakage of financial data and further strengthened the control of financial information. At the G20 Summit in Osaka in 2019, a preliminary framework was established to promote the cross-border flow of financial information, which is undoubtedly a victory for trade protectionism in Europe and the US.

Financial data as globally recognized important data, therefore, its control, processing and use is to consolidate strategic measures data sovereignty, but different big data financial development level, advantage countries supported by digital technology, and with its own build

the domestic regulation framework for long arm jurisdiction of other countries, in the long run, financial data will present to the developed countries disorder into the sample of state. Only by strengthening the safety supervision of financial data and promoting the efficient cross-border circulation can we promote the development of the domestic great circulation.

4 Evaluation and Analysis of the Regulation Mode of Cross-border Flow of External Financial Data

The regulation of cross-border flow of financial data follows the overall regulation of cross-border data flow. In fact, developed countries represented by Europe and the United States embody different protection requirements and standards in the regulation of cross-border flow of personal financial data, which provides diversified reference ideas for improving the legal regulation of cross-border flow of personal financial data in China [5].

4.1 The EU Model

As one of the earliest regional organizations in the world to regulate cross-border data flow, the EU has established a relatively perfect regulation on cross-border data flow. Early before the establishment of the European Union, the OECD on privacy protection and personal information transmission guide cross-border data flow declaration and in 1981 by the European Council through the personal data automation processing personal protection convention [6], the European countries agree on personal cross-border data flow problem provides a favorable legal environment. Since then, in response to the increasing security threats and challenges in the digital economy environment, the EU issued GDPR in 2016 to regulate the cross-border flow of personal data and ensure its comprehensive protection in all aspects through legislation in specialized fields.

In general, the EU's cross-border data flow governance is mainly based on the GDPR, which provides detailed provisions on the cross-border flow of data. The EU emphasizes the adequacy transfer of data and distinguishes between "transfer based on adequacy" and "transfer without adequacy". By dividing different cross-border flow scenarios of personal financial data, more conditions or situations that can realize the cross-border transfer of personal data can be added, so as to give more flexibility and convenience to the cross-border flow of personal financial data. At the same time, in order to ensure the safety and efficiency of personal financial data, the EU has also established a mutual incentive mechanism between the corresponding regulatory agencies and administrative agencies.

4.2 The American Model

Relying on its own data resources advantages, the United States has taken the lead in enjoying the dividends of digital finance, and sought greater benefits in the digital economy, and vigorously advocated the free circulation of data across borders, which is also a policy of the United States.In the United States, the early Internet gained substantially-both financially and in terms of its regulatory framework-from the U.S.[7]The United States has adopted a "zoning legislation" approach. This has led to differences in the regulation of different industries, and strict regulation of data in certain important industries or fields. In terms of the financial industry, the United States enacted the Privacy Law of Financial Consumers in 1978, which is the legal

responsibility of financial institutions and takes protecting the privacy of financial consumers as the main content. The Financial Services Modernization Act promulgated by the United States in 1999 focused on the protection of personal privacy and established five basic principles, while the Consumer Financial Information Privacy Act promulgated in 2000 reaffirmed and highlighted the relevant provisions of the Financial Services Modernization Act.23NYCRR500 is the first cyber security regulation enacted specifically formulated for financial institutions in the United States. The California Consumer Privacy Act (CCPA) of 2018 is to make up for the comprehensive protection of personal information privacy in the United States. CCPA is known as the "strictest privacy protection". Many multinational technology companies (such as Microsoft, Amazon, Apple, etc.) have added CCPA to their privacy protection system. Although CCPA is A state-level law, its legal impact is no less than GDPR.

The United States has adopted a "double-faced" stance on the cross-border flow of personal financial data: first, for political and economic considerations, and second, for national security and personal privacy considerations. From the perspective of the internal legal system of the United States, it guarantees the national security on the premise of promoting the openness and circulation of information. For example, the Clarification of the Legal Use of Overseas Data Act (also known as the Cloud Act) adds protection to its domestic cloud data. For another example, the US listed China as "a threat to the National Security and Personal Data Protection Act 2019" The 2021 Executive Order even urged the US Department of Commerce to take steps to [8] to ensure foreign access to private information from American citizens. From the perspective of external law, the United States, based on its strong comprehensive strength and financial hegemony, advocates expanding the scope of transnational data law enforcement through "long-arm jurisdiction". In recent years, America's "long-arm jurisdiction" has expanded into new areas, such as data sovereignty and cyber security. For example, the US Cloud Act replaces the "server Code". Under the Act, whether the data is stored at home or abroad, the executive agency of the United States has the right to "control" the domestic and foreign data.

5 Suggestions on Improving the Cross-border Flow of Financial Data in China

With the deepening development of global economic integration, the cross-border flow of financial data has become an inevitable trend in the financial industry and related fields. However, there are also many risks and challenges in this process, and we need to strengthen supervision and management to ensure the stability and security of the financial market. In this context, this paper will discuss the suggestions to improve the cross-border flow of financial data in China to promote the healthy development of China's financial industry.

5.1 Strengthen the Legislative Expression of China's Data Sovereignty

"The international community has not yet formed a common rule in the field of data protection law. Opening an external application path for the application of local data protection rules will help China accumulate domestic experience in data legislation, establish an internal and external linkage mode with global data governance, and promote the formation of international rules for data protection."In the face of the extraterritorial application of China's current regulations, the

first suggestion is to innovate the jurisdiction model at the legislative level and clearly stipulate the extraterritorial effect provisions.

First of all, the scope of applicable objects should be expanded in legislation, and the applicable objects in China's current exit rules should not be limited to "the data generated within China and transferred from China to overseas", but to "the data generated within China transferred to overseas and other subsequent flow of the data abroad". In addition, we can refer to the legislative experience of international powerful countries. The United States establishes jurisdiction through the CLOUD Act under the "data controller standard", while the European Union establishes the "institutional establishment standard" and the "target intention standard" through the GDPR. In general, these countries are trying to actively adopt unilateral legislation on the premise of not violating international rules, so as to establish the "sovereign expansion" mode of "long-arm jurisdiction" and the expansion of the effect outside the national law.

Secondly, we can make laws to strengthen the supervision of cross-border digital transactions in China. By establishing a sound cross-border digital trading regulatory system, clarifying the regulatory scope, regulatory mode, regulatory standards and other ways, the corresponding regulatory system will be improved: By strengthening the information disclosure requirements of cross-border digital trading platforms and merchants, to ensure that consumers can fully understand the transaction information and risks. Establish a professional regulatory agency responsible for the supervision and enforcement of cross-border digital transactions. Therefore, when other countries threaten our national security, our sovereignty can transcend the tangible territorial boundaries by mastering the actual control force, and realize more flexible and efficient power allocation.

Thirdly, according to article 38 of the current Personal Information Protection Law, in order to ensure the adequate protection of personal information, we should timely introduce an adequate assessment mechanism or a similar mechanism. The European Union plays a major role in the data security evaluation mechanism. The core of this mechanism is to evaluate other countries or regions, which is essentially the embodiment of a supranational organization participating in the game. The United States has always regarded multinational enterprises as an important participant in the global data interest game, relying on the support of national legislation and international multilateral cooperation to expand their overseas jurisdiction through the continuous practice of enterprises, so as to realize the so-called "long arm" effect. In the big game, there is no doubt that the power of multinational enterprises as the main body of private rights is limited, therefore, under the specific national conditions, our country can learn from the experience of the European Union, with the identity of a sovereign state and other countries and regions, which for Chinese multinational enterprises to provide national data support.

5.2 Build an Efficient Cross-border Regulatory System for Financial Data

So far, China's regulatory system for transnational data flow has been modified and improved. In recent years, the government has taken some legal measures to prohibit the core data from leaving the country, classify and store the data, and establish industry self-discipline and other supervision mechanisms. However, there are still some shortcomings in the current international system of evaluating cross-border financial data. For example, the data safety law, the network security law and other laws and regulations for the financial data outbound regulators for the national information security authority, but the specific implementation rules of overseas

supervision mechanism, such as which cross-border financial data should be checked, what method, what standard, etc., there are still ambiguity.

First of all, the legislative orientation of China's banking industry should be open and inclusive, aiming to promote the benign development of the financial industry, and send a more positive and free message. For example, in the transnational circulation of personal data involving customers, extensive consent and free withdrawal mechanisms should be adopted, rather than strict informed consent. We can learn from the experience of the EU. In the case of enhanced regulation, it ensures the effective distribution of the market, the vitality of the data and the real interests of the data industry.

Secondly, in the future legislative stage, the "one-size-fits-all" approach should be gradually changed to the dynamic monitoring of the circulation of financial data. From the division and governance of industry autonomy and legal control to the dual integration, it is necessary to promote the division of labor and cooperation of industry autonomy rules and legal norms and the coordination and cooperation of multiple subjects. Specifically, to clarify the responsibilities of regulatory authorities, for regulated enterprise compliance work to provide guidance and support, focus on cross-border financial data flow prior supervision and path supervision, ensure the security of financial data through regulation, promote the development of financial services, as far as possible mining, keep the value of the financial data production factors of [9].

5.3 Establish a reasonable hierarchical management system of financial data

Through regular grading evaluation of financial data, the efficiency of financial data security audit can be improved, and the audit system can be optimized. Combined with article 5 of the Draft for Network Data Security Management, the importance of data can be divided into core data, important data and general data.

First of all, our country should refer to the type of important data to establish a core financial data list, gradually increase the number of important evaluation project, the severity of the review, clear data sender and receiver should take responsibility, and implement the responsibility of technical measures, comprehensive decision whether to allow specific financial data exit.

Secondly, formulate the corresponding security assessment policies for the important data and even the core data in the financial data. In this way, a dynamic and accurate exit security assessment system of financial data should be gradually established. In the cross-border supervision of financial data, the free flow of financial data should also be guaranteed to promote the development of financial service trade. From 2017 the network security law data classification way presents the characteristics of "bottom-up", to 2021 in the data safety law in the country as the main body of "top-down" data classification protection mechanism, to 2022 in the security assessment method of data exit of personal information classification clear, but the important data classification mainly evaluated by source subject. This shows that important data is closely related to national security interests and evolves dynamically, so its classification criteria should be more flexible. Under the unified leadership of the network information department, China can set up a unified financial data protection agency, be in charge of data grading security evaluation, and implement the whole process supervision. The financial industry organization shall formulate the self-discipline norms in this field, which shall take effect in the industry after being reviewed by the data protection agency and approved by the

network information department, so as to realize the self-management and self-supervision of enterprises. In the process of data collection, transmission and exchange, financial data controllers should assume the responsibility of self-examination to ensure the legality of data collection, the security of data transmission and the compliance of data exchange. For the recipients of financial data, a safety evaluation system can also be designed, adopt a way similar to the white list, and adopt the corresponding supervision mode according to the results of the evaluation level, from the preliminary evaluation to the whole-process supervision. Such financial data protection network architecture is not only with the second chapter of the data security standard system, industry collaboration, establish data transaction management system such as planning, and make the complex regulatory responsibilities rights, review division of rationalization, make our regulatory system and internal review from other countries, better docking international economic and trade rules.

In addition, in accordance with the "data security law" proposed "important data directory" system, can be crucial to national security and social public interests into financial data, through the localization of data storage and exit security assessment, further enhance the financial data flow rules of operability and transparency, and the "important data directory" regularly update maintenance, to adapt to the needs of financial services trade development of cross-border financial data flow.

5.4 Develop Regional Cooperation Channels for Financial Data Exit

In the context of the growing regional trade negotiations, the strong economic strength of the United States and Europe enables them to promote the realization of their economic goals through trade means. China should also learn from such strategies and actively promote trade dialogue with other countries, so as to enhance our competitiveness while ensuring data sovereignty.

Although China's financial service trade started late, it has developed rapidly. Therefore, while emphasizing data sovereignty, China cannot simply imitate the United States and Europe. In the negotiation process of regional economic cooperation, we can first implement the financial data export security assessment policy in the free trade zone on the premise of clear protection of digital sovereignty. Such as priority in the free trade zone to set up financial data exit security evaluation system, through the exploration of financial data classification standard, combined with regional financial data cross-border transmission, and financial data receiving and financial data using specific factors such as purpose, build a logic of rigorous, fair and transparent and easy to operate evaluation system, improve the strength of free trade zone information technology security evaluation system is scientific and accurate. Finally, on the basis of Beijing Digital Trade Pilot Zone, Shanghai and Zhejiang Free Trade Zone and Hainan Free Trade Port, the scope of the pilot cross-border data flow rules in the free trade zone will be further expanded, and the reform experiment of cross-border financial data flow will be carried out to effectively realize the overall plan.

In order to increase the influence in the multilateral trade agreement, our country can start from the regional financial trade in services, in view of the financial data flow and regulatory measures, the interests of the developed countries and developing countries, become the active rule makers, rather than passive participants, improve the digital economy operability.[10] As for the current situation that China's current legal data exit channels are sufficient safeguard

measures, we can try to establish a white list mechanism for cross-border flow of regional financial data. By evaluating the business environment of the financial data inflow, if the financial data protection level can meet the minimum requirements of the financial data outflow, and there is no negative report about the cross-border flow of financial data, the white list can be included in the free flow of financial data. Due to the significant differences in data security protection level between countries, our country can negotiate with the developed countries financial data cross-border flow, on the basis of financial data cross-border international trade regulation development mode, seeking common ground while reserving differences, weigh the national data security protection level, establish the minimum standard of financial data protection, so as to build up the regional financial data cross-border flow whitelist mechanism, promote the regional financial data cross-border free and safe flow, strengthen the financial data cross-border international trade regulations of international cooperation.

6 Conclusion

With the rapid development of the digital economy, the cross-border flow of financial data has become an important driving force for financial services trade. However, this process also comes with challenges of data security and privacy protection. This paper makes a series of pertinent suggestions by deeply analyzing the regulatory necessity of cross-border financial data flow, as well as the current situation and problems in this field in China.

First of all, the cross-border flow of financial data is an inherent demand for the development of financial services trade. As financial markets become globalized and digitalized, financial institutions need to capture and share customer data across borders to provide more accurate services. However, this flow also brings with it the challenges of data security and privacy protection.

China has made some progress in regulating the cross-border flow of financial data, but there are still some problems. On the one hand, China has not yet formed a perfect legal system to regulate the cross-border flow of financial data. On the other hand, the existing provisions are too general and lack specific implementation rules and operational guidelines. In addition, China's international cooperation in cross-border data flow is also relatively small, which limits the competitiveness of China's financial institutions in the international market.

To address these issues, the following recommendations are proposed. First, top-level design should be strengthened to improve the legal system for cross-border flow of financial data. Specifically, special laws and regulations should be formulated to clarify the scope, conditions and procedures for cross-border data flows, and at the same time strengthen the supervision of data security and privacy protection. Second, the formulation of implementation rules and operational guidelines should be strengthened to improve the operability of laws and regulations. This includes clarifying the specific responsibilities of regulatory authorities, formulating a data classification and hierarchical management system, and establishing a risk assessment mechanism for cross-border data flows. In addition, international cooperation should be strengthened, and actively participate in the formulation and negotiation of international data governance rules, so as to enhance China's voice and competitiveness in the international market.

In conclusion, China should strengthen the regulation of cross-border financial data flow to protect data security and privacy rights, and promote the healthy and orderly development of financial services trade. By improving the legal system, strengthening the formulation of implementation rules and operational guidelines, and strengthening international cooperation, we can effectively improve China's regulatory capacity and level in cross-border financial data flow, and provide a strong guarantee for the global development of China's financial market.

Foundation Project: Supported by project of China Postdoctoral Foundation (Project number: 2023M732765).

References

[1] Czar Matthew Gerard T. Dayday, Cross-Border Data Flows and Data Regulation under International Trade Law [J]. Philippine Law Journal,2023,96(01):33-81.
[2] Zhong Hong, Yang Xinyu. Research on the Security and Regulation of Cross-border Financial Data Flow [J]. New Finance, 2022 (09): 38-44.
[3] Guo Li. The "delicate" approach of personal financial data governance in the digital age [J]. Journal of Shanghai Jiao Tong University (Philosophy and Social Sciences Edition), 2022,30 (05): 15-27.
[4] Zhang rudder. On the legal standards for the cross-border flow of personal data [J]. Journal of China University of Political Science and Law, 2018, (03): 98-109 + 207-208.
[5] Wang Yuanzhi. Legal regulation on the cross-border flow of bank financial data in China [J]. Research on Financial Regulation, 2020 (01): 51-65
[6] Liu Jinrui. Global regulation towards cross-border flows of data: Fundamental concerns and the China Programme [J]. Research in Administrative Law, 2022, (04): 73-88.
[7] Voss, W. Gregory. Cross-Border Data Flows, the GDPR, and Data Governance [J]. Washington International Law Journal,2020,29(03): 485-532.
[8] Zhao Haile. International Legal Conflicts and countermeasures of personal Information protection from the perspective of data sovereignty [J]. Contemporary Jurisprudence, 2022,36 (04): 82-91.
[9] Liu Yan, Ran Congjing. The International strategy of cross-border supervision of financial data and China's approach [J]. Financial Review, 2023,15 (04): 109-123 + 126.
[10] Qi Peng. Construction of cross-border transmission and sharing governance scenarios of "Belt and Road" digital economic data [J]. Journal of Beijing University of Technology (Social Science Edition), 2022,22 (02): 118-130.