DOI: 10.18254/S278229070031783-7 Original paper

Regulation and Dilemma of Cross-border Transmission of Financial Information

©2024 Armstrong Sheng Chen[a]

[a] Northwest University of Political Science and Law,
Dentons Shanghai, China
armstrong.chen@dentons.cn

Abstract. It is important to ensure the order and security of the cross-border transmission of financial information, so it is self-evident that it is necessary to regulate and continuously improve this process. Compared with developed countries, China still lacks regulations on the cross-border transmission of financial information. There are difficulties and obstacles in the cross-border transmission of financial information, and suggestions are made to improve the status quo.

Keywords: financial information, cross-border transmission, legal regulation

For citation: Chen A.S. 2024. Regulation and Dilemma of Cross-border Transmission of Financial Information. *Law & Digital Technologies 4(1): 15—24.*

INTRODUCTION

Cross-border transmission of financial information in the global financial market has gradually attracted the attention of many countries. Governments in these countries are aware of the need for regulation of this process. In recent years, various laws and policies have been introduced to regulate these transmissions. However, in practice, there are dilemmas and obstacles in the cross-border transmission of financial information, such as conflicts between financial information confidentiality obligations and cross-border transmission, information sharing, and whether the provisions of "domestic storage and operation" should apply to financial information. In addition to continuously improving their own laws and regulations in order to promote the synergy of self-regulation of the financial industry and government regulation, they should also coordinate the international development of cross-border financial information transmission while improving legal regulations in this area.

1. THE INTRODUCTION OF FINANCIAL INFORMATION IN CHINA

On February 13, 2020, the People's Bank of China issued the Personal Financial Information Protection Technical Specification (hereinafter referred to as the Specification)[2]. The Specification defines personal financial information as personal information obtained, processed and preserved by financial institutions through the provision of financial products and services or other channels, including account information, authentication information, financial transaction information, personal identification information, property information, and loans Information and additional information reflecting certain circumstances of a particular individual. The time for feedback issued by the People's Bank of China on the Implementation Measures for the Protection of Financial Consumers' Rights and Interests (Draft for Comment) (hereinafter referred to as the 2019 Implementation Measures) ends on January 25, 2020[3]. Article 27 of the 2019 Implementation Measures first amends the Personal Financial Information of the Implementation Measures for the Protection of Financial Consumer Rights and Interests of the People's Bank of China (hereinafter referred to as the Implementation Measures for 2016) implemented on December 14, 2016[4]. It is "consumer financial information", which defines financial information as "buy, use" related information of financial products or services, including personal identification information, property information, account information, credit information, financial transaction information and other related information.

2 http://www.cfstc.org.cn/bzgk/gk/view/bzxq.jsp?i_id=1856
3 http://www.pbc.gov.cn/en/36882 53/3689009/3788480/41 21916/2020110615170136365.pdf
4 http://www.pbc.gov.cn/english/ 130733/3881691/index.html

In the era of data informatisation, the free flow of various types of data has promoted the development of cross-border services and cross-border trade. The cross-border transmission of financial information not only promotes the internationalisation of enterprises but also facilitates the rapid development of the global financial industry. If the cross-border transmission of financial information lacks unified legal supervision but is allowed to expand freely and disorderly, then financial transactions are bound to become chaotic. For individual users in financial transactions, if personal financial information is leaked by financial institutions or used in an improper way, the owner of the information is likely to suffer property losses. At the same time, financial institutions will also be subject to administrative and other legal sanctions.

2. ANALYSIS OF STATUS QUO OF THE REGULATION OF CROSS-BODER TRANSMISSION OF FINANCIAL INFORMATION

On April 8, 2018, the China Banking and Insurance Regulatory Commission was officially established on Beijing Financial Street. Considering the historical process of China's financial reform, the merger of banking and insurance regulatory agencies can be described as a landmark event, which marks that the modern financial regulatory framework is further reshaped. The banking industry emphasizes serving entities, addressing the risks of shadow banking in an orderly manner, and promoting the establishment of a long-term mechanism for risk management and control, while the insurance industry pays more attention to the introduction of new policies in equity, products, channels and promotes the return to a focus on high quality through detailed and strict regulatory standards (Meng et al. 2019). From laws to departmental regulations, China's regulations on the cross-border transmission of financial information are gradually becoming more complete and detailed. However, compared with other countries and regions like the EU, there are still some deficiencies.

2.1. Regulation of cross-border transmission of financial information in China

On January 21, 2011, the People's Bank of China issued the Notice on Banking Financial Institutions Doing a Good Job in Protecting Personal Financial Information (hereinafter referred to as the 2011 Notice)[5]. Article 6 stipulates that personal finance collected in China shall be stored, processed, and analyzed within China. Except as otherwise stipulated by laws, regulations, or the People's Bank of China, banking financial institutions shall not provide domestic personal financial information overseas.

On June 11, 2014, the General Office of the People's Bank of China issued the Notice on the Special Inspection of Personal Financial Information Protection in 2013. The main problems found include the improvement of the internal control system of foreign banks and stricter safety precautions. Information security management standards have been implemented, and customer information is managed in a hierarchical manner. However, some foreign banks set up data centers overseas and submit data across borders in accordance with the regulatory compliance requirements of the home country or the head office, which does not comply with the relevant regulations of the regulatory authorities.

The Cyber Security Law of the People's Republic of China came into effect on June 1, 2017[6]. Article 31 of the Cyber Security Law proposes that the state should deal with important industries and fields such as public communications and information services, energy, transportation, water conservancy, finance, public services, and e-government, as well as other breaches, loss of functions, or data leakage. Key information infrastructure that may seriously endanger national security, national economy, people's livelihood, and public interests, should implement key protection based on the network security level protection system. Article 37 of the Cyber Security Law stipulates that operators of critical information infrastructure should store important personal data, such as citizens' personal information collected and generated during operations within the territory of the People's Republic of China. For the provision to overseas organizations or individuals, the safety assessment shall be carried out in accordance with the methods formulated by the State Network Information Department in conjunction with relevant departments of the State Council.

Article 33 of the Implementation Measures 2016 stipulates that the storage, processing and analysis of personal financial information collected within China shall be conducted domestically. Except as otherwise stipulated by laws, regulations, and the People's Bank of China, financial institutions cannot provide domestic personal financial information overseas. To handle cross-border business, the domestic financial

5 https://www.gov.cn/gongbao/ content/2011/content_1918924.htm

6 http://www.cac.gov.cn/2016-11/07/c_1119867116.htm

institution, authorised by the parties, may transmit relevant personal financial information collected domestically to overseas institutions (including the head office, parent company, branch, subsidiary, and other related institutions necessary to complete the business). This must comply with laws, administrative regulations, and relevant regulatory authorities. Furthermore, through agreements, on-site verification, and other effective measures, they must require foreign institutions to keep the personal financial information confidential.

On June 27, 2018, the Ministry of Public Security announced the Network Security Registration Protection Regulations (Draft for Comment)" (hereinafter referred to as the Protection Regulations)[7]. Article 15 of the Protection Regulations is based on the importance of the network in national security, economic construction, and social life, as well as its damage to national security, economic security, and social security. Factors such as order, public interest, and the degree of harm to the legitimate rights and interests of relevant citizens, legal persons, and other organizations divide the network into five levels of security protection. Accordingly, the Protection Regulations stipulates that network operators should perform different levels of security protection obligations according to different levels of security protection to ensure network and information security. For example, Article 21 requires network operators above the third level to perform general network security protection obligations as stipulated in Article 20, and also fulfill special network security protection obligations, such as establishing a level-by-level approval system. In addition, the Protection Regulations requires network operators to conduct online testing, rating evaluation, security rectification, and security self-examination. In terms of data and information security protection, Article 31 of the Protection Regulations require network operators to establish and implement important data and personal information security protection systems; take protective measures to to ensure that data and information are collected, stored, transmitted, and used securely, and provide security during the destruction process; establish technical measures such as off-site backup and recovery to ensure the integrity, confidentiality, and availability of important data. Without permission or authorisation, network operators shall not collect data and personal information unrelated to the services they provide. They must not violate laws, administrative regulations and the agreement between the parties to collect, use and process data and personal information. Unauthorized access, use, and provision of data and personal information are not allowed.

On July 11, 2018, the People's Bank of China issued the Notice on Strengthening the Management of Cross-Border Financial Networks and Information Services (hereinafter referred to as the 2018 Notice)[8]. The 2018 Notice requires foreign providers to provide cross-border financial networks and information services to domestic users and shall perform performance reports in written form (including electronic documents) to the People's Bank of China within 30 working days before the formal provision of services. The overseas provider shall report to the People's Bank of China in writing on the services carried out in the first half of the year by July 20 and for the previous year by January 20 of the following year. If an overseas provider provides services to a domestic user, and there are major changes in its service content, business rules, or technical means, it shall report to the People's Bank of China in writing within 30 working days before the change. Overseas providers are not allowed to build a dedicated financial network within the country to provide services such as financial information transmission, but they can authorize their institutions established in China to perform relevant reporting obligations. In addition, the 2018 Notice requires domestic users intending to use the services of overseas providers to complete the reporting procedures in advance with the provincial branch of the People's Bank of China where the legal entity of the domestic user is located. Overseas providers and domestic users should join the China Payment and Clearing Association and accept industry self-regulation management. In accordance with the needs of macro-prudential management, the People's Bank of China conducts assessments on the performance of reports by overseas providers and the reports of domestic users, strengthens cross-border financial networks and information security protection, information sharing and supervision, and will register with overseas providers. The local supervisory authority establishes a supervisory cooperation framework and strengthens coordination, communication, and information sharing. This is the specific practice of the Chinese version of the ‘long arm jurisdiction’ principle in the field of financial supervision.

7 http://www.bnia.cn/hyzx/zcfg/xzfg/2022-03-30/190.html

8 http://www.pbc.gov.cn/tiaofasi/144941/ 3581332/3730200/2018122910433634323.pdf

The E-Commerce Law was promulgated and implemented on January 1, 2019[9]. Article 25 of the E-Commerce Law stipulates that relevant authorities should take necessary measures to protect the security of data information provided by e-commerce operators, and personal information, privacy and business secrets are kept strictly confidential and may not be disclosed, sold or illegally provided to others. Article 30 requires e-commerce platform operators to ensure the security of e-commerce transactions. It stipulates that they should ensure network security and stable operation, prevent illegal and criminal activities, and formulate emergency plans to effectively respond to network security incidents. Article 31 requires operators of e-commerce platforms to record and store information on goods and services, as well as information on transactions, for at least three years from the completion of the transaction. In addition, the E-Commerce Law embodies China's support and intention to promote the development of cross-border e-commerce, establishing customs, taxation, entry and exit inspection and quarantine, payment settlement and other management system regulations that meet the characteristics of cross-border e-commerce. The export management department shall promote the construction of comprehensive services and supervision systems for cross-border e-commerce customs declaration, tax payment, inspection and quarantine in accordance with the law, optimize the supervision process, promote the realization of information sharing, mutual recognition of supervision, mutual assistance in law enforcement, and improve cross-border e-commerce services and regulatory efficiency. In addition, in terms of cross-border e-commerce cooperation, the E-commerce Law in Article 73 proposes that the country promote the establishment of cross-border e-commerce exchanges and cooperation with different countries and regions, participate in the formulation of international e-commerce rules, and promote electronic The development of international mutual recognition systems such as signatures and electronic identities and the promotion of the establishment of a cross-border e-commerce dispute resolution mechanism. Regarding punishment, the E-Commerce Law works with the provisions of the Cyber Security Law, and the relevant competent departments are responsible for taking punitive measures within a time limit for violations of the above-mentioned provisions, including ordering business rectification and imposing administrative fines.

On June 13, 2019, the National Internet Information Office (hereinafter referred to as the Internet Information Office) released the Measures on Security Assessment of Cross-Border Transfer of Personal Information (Consultation Draft) (hereinafter referred to as the Evaluation Measures) to solicit opinions from the public. In order to ensure the security of personal information in the cross-border flow of data. Article 3 of the Evaluation Measures stipulates that before the personal information leaves the country, the network operator shall declare the personal information outbound security assessment to the local and provincial network information department. Additionally, the 'Evaluation Measures' list the materials that the network operator should provide for the outbound security assessment declaration. Article 5 of the Evaluation Measures stipulates that the provincial cyber-information department should organize experts or technical forces to conduct security assessments after receiving the personal information exit security assessment application materials and verifying their completeness. The safety assessment should be completed within 15 working days. If the situation is complex, the assessment period can be appropriately extended. In addition, Article 10 of the Evaluation Measures also stipulates that the provincial network information department should regularly organize the inspection of the personal information exit records of the operator's personal information exit records, focusing on checking the travel conditions of the contract's obligations and whether there are any violations of the state. Regulations or actions that damage the legitimate rights and interests of the personal information subject. The Evaluation Measures also stipulate the respective responsibilities and obligations of the contract or other legally valid documents signed between the network operator and the recipient of personal information on both sides.

Article 34 of the People's Bank of China Financial Consumer Rights Protection Implementation Measures (Draft for Comment) (hereinafter referred to as the 2019 Central Bank Implementation Measures) was issued by the Central Bank on December 27, 2019[10]. The storage, processing and analysis of information shall be carried out in China. If providing consumer financial information overseas is necessary for business needs, it should meet the following conditions: 1) necessary for processing cross-border business; 2) written authorization from financial consumers; 3) information recipient for completion Related institutions necessary for the business (including the head office, parent company or branch, subsidiary, etc.); 4) by signing agreements, on-site verification and other effective measures, overseas institutions are required to

9 https://www.gov.cn/xinwen/2018-08/31/content_5318220.htm

10 https://zqyj.chinalaw. gov.cn/readmore?listType=2&id=3606

information. Article 45 of GDPR stipulates in detail the "appropriateness assessment, qualification review and safeguard measures for the cross-border transmission of information data" (Wu and Huo 2018): 1) the third country should have the protection level stipulated by GDPR before cross-border transmission of information and data; 2) when evaluating the protection level, it is necessary to consider factors such as relevant regulations, respect for human rights, supervisory agencies, and international commitments; 3) after the European Commission 's assessment, it can decide whether to achieve the level of protection through a bill, and the implementation of the bill should provide for a periodic review mechanism at least every four years; 4) the European Commission should continuously monitor whether third countries or international organizations comply with the Committee 's compliance Evaluation decision and whether to protect data in accordance with Article 25 (6) of Directive 95/46; 5) when the evaluation object no longer meets a sufficient level of protection, the European Commission will revoke, amend or terminate the aforementioned decision; 6) the European Commission should publish a list of specific regions and specific departments in third countries and international organizations on the "European Union Bulletin" and its website.

Article 45 of GDPR actually embodies the sufficiency determination mechanism. When the data protection level of the third country meets the requirement of sufficiency, it provides the necessary guarantee for the data provider country. However, although the sufficiency determination mechanism is important, it is not the only consideration. According to the provisions of Article 46 of GDPR on "Safety Measures for the Transfer of Subjects", if there is no sufficiency determination, the third country shall provide certain safeguards for data transferred across borders, such as binding company rules, contract terms, third-party certification. However, the above measures must be approved by the European Commission or the National Data Protection Agency. Secondly, if the third country cannot provide the corresponding safeguards, it can take the means of enumerating only a limited data transmission impairment list, such as the transfer agreed by the data subject, the necessary transfer for the benefit of the data subject, and the public benefit transfer and other situations.

However, it should be pointed out that, for the purpose of preventing financial crimes such as money laundering and preventing financial risks, many EU financial supervision laws have set clear requirements for the processing and control of customer data by financial institutions (Wang 2018a). For example, the "European Financial Instruments Market Directive II"[15] (MiFID II) and "IFRS 9"[16] have emphasized the obligations of banks and other financial institutions for customer data collection, processing and reporting. This may conflict with GDPR, so the financial industry may face a dilemma in compliance.

3. DIFFICULTIES AND OBSTACLES IN THE CROSS-BODER TRANSMISSION OF FINANCIAL INFORMATION

According to China's legal regulations on the cross-border transmission of financial information and its comparison with related systems outside the country, the state pays more and more attention to the cross-border transmission of financial information, but the difficulties and obstacles still cannot be underestimated.

3.1 Conflict between the obligation of confidentiality of financial information and cross-border transmission and information sharing

In the financial industry, the obligation to keep financial information confidential is a tradition. Prior to the digital era, banks were required to assume confidentiality obligations with respect to customer identity information, account information, and transaction information, and were not allowed to provide or allow others to inquire. Nowadays, with the Internet as the main information transmission channel, cyberspace is full of financial information. If the confidentiality of the above financial information cannot be guaranteed, the security of the entire financial market will be affected. Therefore, when regulating the cross-border transmission of financial information, it is necessary to consider the confidentiality obligations of various financial information subjects. For example, Articles 10, 36, 40, 45 of the Cyber Security Law stipulate the confidentiality obligations of network operators.

Of course, there are exceptions to confidentiality obligations. For example, Article 31 of the E-commerce Law stipulates the confidentiality obligations of operators of e-commerce platforms and then adds: "If laws and administrative regulations provide otherwise, follow their provisions". Article 37 of the Cyber Security

15 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0065

16 https://www.ifrs.org/issued-standards/list-of-standards/ifrs-9-financial-instruments/

Law stipulates that personal information and important data collected and generated by the key information infrastructure should be stored in the territory, but if due to business needs, a security assessment should be conducted in accordance with national regulations, and it also remains the provision "legal, administrative regulations stipulate otherwise". Article 2 of the Measures for Security Assessment for Cross-border Transfer of Personal Information (Draft for Comment) also stipulates that if the State has other regulations regarding the exit of personal information, the regulations shall prevail. It should be pointed out that in cases where the executive and judicial organs exercise public power, they do not consider the current large-scale and high-frequency flow of data between different legal entities. If the obligation of confidentiality is strictly explained, it may also restrict the flow of financial data between domestic and foreign affiliated financial institutions. This issue needs to be resolved by the regulatory authorities through appropriate interpretation or modification of relevant regulations to avoid hindering the sharing and flow of financial data.

3.2. Discussion of whether the provision of "Domestic Storage and Operation" applied to financial information is reasonable

The Notice on Banking Financial Institutions Doing a Good Job in Protecting Personal Financial Information was the first to limit the storage, processing and analysis of "personal financial information" within the territory. Subsequently, the promulgation of China's Cyber Security Law in 2016 caused widespread concern in all walks of life. On September 25, 2017, the United States submitted a defense document to the Council for Trade in Services of the WTO in response to China's Cyber Security Law and related supporting measures. In the defense document, the United States believes that the concept of "Critical Information Infrastructure (hereinafter referred to as CII) proposed by China is too broad and vague, and network operators of cross-border transmission of data will be subject to review by Chinese authorities. These review procedures will inevitably hinder the cross-border transmission of information and disrupt normal business operations.

After the Cyber Security Law, the Cyberspace Administration of China issued the "Regulations on the Protection of Critical Information Infrastructure Security (Draft for Comments)" (hereinafter referred to as the Protection Regulations) on July 10, 2017[17]. The definition and scope of protection are defined as satisfying the conditions of "in case of damage, loss of function, or data leakage, which may seriously endanger national security, national economy, people 's livelihood, and public interest". Such cases shall be regarded as CII. Government agencies and industries such as energy and finance are included as typical CII sectors. It can be seen that according to the provisions of the Cyber Security Law and its supporting measures, personal information and important data generated and collected by the financial industry should be included in the protection scope of CII.

In addition, Article 29 of the Protection Regulations reiterates the CII information domestic storage regulations, and Article 34 sets forth requirements for "domestic operations": CII operation and maintenance should be implemented within the territory. The Regulations on the Protection of Personal Information and Important Data Collected and Generated by CII Operators are stricter than the Cybersecurity Law, expanding from "domestic storage" to the double limitation of "domestic storage + operation". After the implementation of the Protection Regulations, the operation, maintenance and technical support of the financial data collected and generated by CII operators should be implemented within the territory. If it is indeed necessary for business requirements to conduct remote access, maintenance, and debugging operations overseas, the CII operator should report to the competent department in advance.

Once the information collection and producer fall into the category of "CII operators", they must be restricted by the "domestic storage + operation" of financial data. Under the current environment that encourages the further opening of the financial industry, domestic and foreign markets are gradually tending to converge. Domestic financial institutions may expect to cooperate with large overseas multinational companies and promote their brands to the international community, while foreign-funded companies also covet China's huge commercial market, so it is a common choice to penetrate its products into the Chinese domestic market. From this point of view, in future business activities, the cross-border transmission of financial information may be the normal state of corporate cross-border business activities. Therefore, "domestic storage + operation" has brought great obstacles to the cross-border transmission of financial information and may have a fundamental impact and substantial obstacles on the business of some enterprises or even the normal development of enterprises.

17 http://www.cac.gov.cn/2017-07/11/c_1121294220.htm

4. THE IMPROVEMENT OF REGULATIONS FOR CROSS-BORDER TRANSMISSION OF FINANCIAL INFORMATION

In the globalized environment, world security and prosperity are dependent on the connectivity of data and information (Borchert 2015). Maintaining good connectivity of financial information is an indispensable factor for the healthy development of global financial markets.

4.1 Improvement of China's legal regulations on the cross-border transmission of financial information.

Article 2 of China's Cyber Security Law stipulates that its geographical applicable scope is within China's territory, that is, as long as the network is built, operated, maintained, and used within China's territory, regardless of whether the specific attribute is domestic or foreign capital, it shall obey the relevant provisions of the Cyber Security Law. The GDPR 's scope is more extensive: 1) GDPR applies to the processing of personal data by all data controllers or processors established within the EU, regardless of whether the actual processing is performed within the EU; 2) even if the data controller or processor is not established in the EU, as long as it provides goods or services for the data subject in the EU, or monitors the activities of the data subject occurring in the EU, the processing of personal data will fall within the jurisdiction of GDPR; 3) GDPR also applies to personal data processing activities performed by data controllers established outside the EU, but applying the laws of member countries in accordance with the provisions of public international law. It can be seen that the determination of jurisdiction in China's Cyber Security Law is far less detailed and specific than GDPR which means the China’s regulation on information transfer needs to widen its scope.

Although Articles 22, 41, 42, 43 of China's Cyber Security Law mention the rights of users to know, decide and control, compared with GDPR, it is still too broad and general. The 42 articles of the third chapter of GDPR provide detailed regulations on the right to know, access, correct, and deletion of data subjects.

According to Article 24 of China’s “Network Security Law”, network operators handle network access, and domain name registration services for users, handle network access procedures for fixed phones and mobile phones or provide users with information publishing and instant messaging services. When signing an agreement with a user or confirming the provision of services, the user should be required to provide true identity information. If the user does not provide true identity information, the network operator shall not provide related services to them. GDPR makes detailed provisions on the legal rights and obligations of the data controller, such as the data controller's interest boundary, evaluation procedures, the data processing purpose, data processing notification obligation, and data transfer notification obligation. At the legislative level, compared to GDPR, China pays greater attention to the control of cross-border data transmission at the national macro level and the obligations and responsibilities of network operators, but does not sufficiently address the legitimate rights and interests of network operators.

As it has been discussed above, in the amendment of relevant legislation and the formulation of supporting measures in the future, China should further improve the above aspects.

4.2. Promoting the synergy between the self-regulation of the financial industry and government regulations

In western developed countries, for the protection system of data, most countries adopt two types of opposing regulatory methods: general information and key information, and China's data cross-border regulation can be regarded as “local supervision” and “global supervision” (Fu 2017).

For the financial information collected and generated by both sectors, the public sector network information system is more important than the general private sector. It should maintain a higher level than the private sector in terms of regulatory standards. This requires the financial industry’s self-regulation and government regulation to be different on a separate basis and ultimately go hand in hand (Liang and Wu 2018). For strengthening the legal regulation of cross-border transmission of financial information, a pragmatic public-private partnership is particularly important. The so-called public-private partnership refers to the sharing of resources and information between the public and private sectors, similar to the operation of a partnership to maintain financial information.

Nowadays, most countries have established a security assessment mechanism for the cross-border transmission of data. Therefore, for the legal regulation of cross-border transmission of financial information, countries should encourage financial industry associations and other self-regulatory organizations to

participate in security assessment on this basis. As a supplement to the market mechanism, the voluntary participation of members of the financial industry in security assessments can establish a dynamic data management order. In addition, governments of various countries should respect the rules of industry and the development of their financial markets to improve their respective laws and regulations.

4.3. Coordinated development at the international level for cross-border transmission of financial information.

For the regulation of the cross-border transmission of financial information, it is an issuecountries need to consider at the international level for future coordination. Although governments globally have gradually established different frameworks for the legal regulation of the cross-border transmission of financial information, issues such as conflicts of application of laws will still be difficult. For companies that provide services to the world, the safer option in the conflict of law application is to store the personal data of citizens of different countries served in the corresponding country (or other regions approved by the country's policies), of course, this has undoubtedly produced. In view of the huge new costs and the complex issues of jurisdictional competition and co-operation, there is an urgent need for a co-ordination mechanism at the international level (Wang 2018b).

Some domestic scholars believe that in the cross-border data flow regulation, there are conflicts of interest between the "good data protection", "cross-border data free flow", and the "data protection autonomy" of governments (Huang and Li 2017). "Good data protection" represents the security of data of the country, individuals and social groups. Unlike traditional service trade, in cross-border services and trade under the new situation, cyberspace is flooded with various relevant data. In the process of global informatization, the "free flow of cross-border data" is the cornerstone of cross-border services and cross-border trade in various countries. Sound cross-border services and cross-border trade should be accompanied by good cross-border data flow. If the flow of cross-border data is restricted, multinational companies that rely on the analysis of cross-border data cannot make correct and targeted business judgments, resulting in a decline in the quality of cross-border services and trade. The "data protection autonomy" of governments of various countries shows that the sovereignty of countries in cyberspace is not interfered with by other countries or institutions. When cross-border data flows weaken data subjects' control of their own data, the loss of key national data resources and their data protection autonomy. The resulting effect may be that a country's economic and cultural conditions are easily controlled by developed countries. This influences the country's right to speak in economic, trade, and international exchanges, as well as its autonomy in cultural development.

Choosing between different interests to achieve a more appropriate fit is important. Throughout the history of the international community, various cooperation methods, including bilateral and multilateral agreements, have existed for cross-border data transmission. For example, the Asia-Pacific Economic Cooperation (APEC) proposed a cross-border privacy rule system (CBPR) in 2012 to regulate the cross-border transmission activities of APEC member companies to protect data related to personal privacy. For the cross-border transmission of financial information, the above method may be a desirable measure.

In addition, countries can submit laws and regulations on the cross-border transmission of financial information to the WTO. As an organization that promotes global cross-border trade and services, the WTO offers the fairest way to reach unity among all parties. Under the legal framework of the WTO, members' interests can be assimilated, promoting the liberalization of global trade. However, it also requires members to strive to maintain the WTO's existing systems and rules to avoid a shutdown state.

CONCLUSION

China has enhanced cross-border information protection through continuous legislation. However, there is still a gap compared to more mature regulatory systems like that of the European Union. Therefore, China's current regulation should increase in depth and breadth, promote cooperation between self-regulation and government regulation, and strengthen coordination at international levels in cross-border information transmission. In this way, a more effective and sound regulatory system for cross-border information transmission can be established.

REFERENCES

1. Borchert, H. 2015. It Takes Two to Tango: Public-Private Information Management to Advance Critical Infrastructure Protection. European Journal of Risk Regulation 6 (2): 208–218. https://doi.org/10.1017/s1867299x00004517.
2. Fu, P. 2017. “A brief introduction to the regulatory framework of data cross-border transmission under the system of "Computer Network Security Law.” April 12, 2017. https://mp.weixin.qq.com/s/M90N82DqwjYs_Btn-CzSyw
3. Huang, N., and Y. Li. 2017. The Evolutionary Trend of Trans-border Data Flows Regulation and Its Cause Analysis. Journal of Tsinghua University (Philosophy and Social Sciences Edition) 5: 172–82. https://doi.org/10.13613/j.cnki.qhdz.002634
4. Liang, Y., and D. Wu. 2018. Enlightenment of EU GDPR strong regulation model on data governance of China's financial industry. Financial Technology Age 9: 27–29. https://doi.org/10.3969/j.issn.2095-0799.2018.09.005
5. Meng, F., Y. Song, and H. Li. 2019. “China's Banking and Insurance Regulatory Commission opens to the outside world” Beijing Business Today, April 15, 2019.
6. Wang, R. 2018a. Analysis on the main content and influence of EU general data protection regulation. Financial Accounting 8: 17–26.
7. Wang, R. 2018b. Cognition and suggestion of data cross-border flow policy: from the perspective of comparison and reflection of American and European policies. Security and Confidentiality of Information and Communications 3: 41–53.
8. Wu, S., and W. Huo. 2018. EU GDPR and analysis of data cross-border issues. China Information Security 7: 17–33, 37.
9. Zheng J., and D. Gao. 2018. The EU GDPR and its Impact on the Financial Industry. China Finance 14: 80–82.