International Journal of Social Sciences and Public Administration
ISSN: 3005-9836 (Print), ISSN: 3005-9585 (Online) | Volume 2, Number 3, Year 2024
DOI: https://doi.org/10.62051/ijsspa.v2n3.22
Journal homepage: https://wepub.org/index.php/IJSSPA/index

Legal Regulation Risks and Insights Related to Cross-Border Flow of Data

-- Analysis based on the Measures for Standard Contracts for the Exit of Personal Information

Zixuan Tian[1, a], Chenhao Wen[2, b, *], Jinfeng Fan[3, c]

[1]Qingdao City University College of Foreign Languages, Qingdao, China
[2]Shaanxi Normal University College of Arts, Xi'an, China
[3]Beijing City University College of Public Administration, Beijing, China
[a]tianzixuannn@outlook.com, [b, *]nijintianchifanlema0v0@outlook.com, [c]fanjinfengggg@outbook.com

ABSTRACT

The primary objective of this research is to ensure the secure and compliant transmission of personal information from China. To this end, the Chinese government has implemented the "Standard Contract Measures for the Export of Personal Information." This study employs both literature review and factor analysis methods to meticulously examine the potential risks in the practical implementation of these measures, and further suggests strategies to address the current challenges. Additionally, the study introduces foreign systems for reference, aiming to guide Chinese enterprises in circumventing legal risks associated with cross-border data flows and ensuring the security and compliance of personal information departing from the country. The findings of this research reveal that the existing legal framework for cross-border data flows in China has certain shortcomings, providing valuable insights for the improvement of China's legal framework and related regulatory systems. Furthermore, it offers practical cautionary value for Chinese enterprises in their operations.

KEYWORDS

Cross-border Data Flow; Personal Information Protection; Cross-border Commerce.

1. INTRODUCTION

1.1. Research Background

With the rapid development of Internet technology, the cross-border flow of data across the globe has become more and more frequent. This makes the protection of personal information an urgent problem. Previously, the laws and regulations on cross-border flow of data promulgated in China, such as the Network Security Law of the People's Republic of China, the Data Security Law and the Personal Information Protection Law, mainly stipulate the basic legal principles and framework of data security and personal information protection from the national level, which lacks operability, and it can be seen that the specific specific norms for personal information out of the country are relatively blank.

1.2. Problem Statement and Objectives

Against this background, China has promulgated the Measures for Standard Contracts for the Exit of Personal Information, which stipulates in detail the specific operational procedures for personal information processors and overseas recipients in the exit of personal information, with the aim of ensuring that the activities of overseas recipients in the handling of personal information meet the standards for the protection of personal information stipulated in the relevant laws and regulations of China, and clarifying the rights and obligations of personal information processors and overseas recipients in the protection of personal information. However, in actual operation, the Measures may have some legal regulation risks. If this problem is not solved, then the role of the legislation will not be effectively realized. This paper will explore its shortcomings from different aspects and provide some measures to solve them.

2. RISKS IN THE CONCRETE OPERATION OF THE MEASURES

2.1. Risk of Impact Assessment of Personal Information Protection

According to the Measures for Standard Contracts for the Exit of Personal Information, enterprises are required to carry out personal information protection impact assessment when exporting personal information. When conducting personal information protection impact assessment, enterprises may have inaccurate assessment results due to the ambiguity of the assessment method and assessment standards, which may affect the enterprises' legal compliance in conducting personal information outbound. As well as the lack of assessment criteria may cause leakage of personal information in the process of cross-border data exchange.

In the scale, scope, type, sensitivity, and risk of outbound personal information, which is one of the contents of the assessment criteria, for outbound personal information, enterprises may fail to clearly define the classification and scope of the data, which makes it difficult to accurately assess the actual amount of data and risk involved in the assessment process. Moreover, enterprises may fail to comprehensively identify potential risks during the assessment process, or may not analyse the risks in sufficient depth, resulting in the accuracy of the assessment results being affected.

In the second part of the question of whether the channels for safeguarding the rights and interests of personal information are smooth, the Measures do not provide a specific explanation of the word "smooth". An enterprise's assessment of the channels it has established to safeguard the rights and interests of information may deviate from the actual situation. In the process of assessment, enterprises may have ambiguous judgement on the publicity, convenience and effectiveness of the channels. For example, as the business develops and the number of users increases, the enterprise may fail to adequately predict the growth rate of the scale of personal information, resulting in the rights and interests of the channel not being able to carry the risks associated with the volume of data.

2.2. Supervision and Management Risks

Enterprises need to regularly supervise the contractual performance of offshore data receivers to ensure that they use and protect personal information in a lawful and compliant manner. However, in practice, it may be difficult for enterprises to grasp the specific situation of overseas data receivers in real time, which leads to the risk of inadequate supervision. And enterprises need to ensure that offshore data receivers take adequate data security protection measures. In practice, it may be difficult to fully understand and supervise the implementation of data security measures by overseas data receivers, leading to security risks. In addition, the complaint handling mechanism agreed in the contract between the processor of personal information and the offshore recipient may be unfair and opaque, resulting in complaints of damage to personal information rights and interests not being handled effectively.

When transmitting personal information across borders, it is necessary to establish effective co-operation and co-ordination mechanisms with overseas data receivers. However, in practice, enterprises may face problems such as poor co-operation and difficulties in co-ordination, thus affecting the protection of personal information.

2.3. Scope of Application

2.3.1. Definition, Scope and Importance of Cross-border Data Flow

Cross-border data flow refers to the process of data transmission from one country or region to another. The cross-border flow of data includes the transmission of personal data and non-personal data. Personal data refers to any information related to an identified or identifiable natural person, and non-personal data refers to any information that is not related to a natural person.

2.3.2. Scope of Application of Standard Contract

The scope of application of the " Standard Contract Measures for the Export of Personal Information " (hereinafter referred to as the " Measures ") is that " data processors provide personal information to other organizations or individuals outside the territory of the People 's Republic of China through contractual agreements. " It does not involve the relationship between data processors and overseas recipients, nor does it involve cross-border data transmission of domestic enterprises.

For the scope of application of the standard contract method for the exit of personal information, there is no clear provision in the current laws, regulations and departmental regulations. According to the provisions of laws and regulations such as the ' Measures ' and the ' Network Security Law ', the scope of application of the standard contract method can include the following two situations : First, the overseas receiver is the person who processes personal information (that is, the ' overseas institution ' referred to in the above ' Measures ') ; second, the overseas receiver is a domestic enterprise. The former refers to the domestic enterprise directly controlled by the foreign personal information processor, and the latter refers to the domestic enterprise that controls the personal information processor abroad.

For the first case, because the standard contract method is a departmental regulation formulated by the national network information department, the regulation belongs to the normative document at the level of laws and regulations, and the ' method ' is a departmental regulation formulated on the basis of it, which belongs to the normative document with lower effectiveness level. According to Article 4 of the ' Measures ', under normal circumstances, a personal information processor may only provide personal information overseas by entering into a standard contract if:

1) Non-critical information infrastructure operators;

2) processing personal information less than 1 million people;

3) Since January 1 of the previous year, the cumulative number of people who have provided personal information to overseas is less than 100,000;

4) Since January 1 last year, less than 10,000 people have provided sensitive personal information overseas.

Combined with the application of the " data exit security assessment method, " the two distinguish which personal information exit mechanism is applicable to the handlers with specific identities and a specific number of personal information. For personal information processors who fall into the scope of application of the " data exit safety assessment method, " they should declare the data exit safety assessment according to law;

for the second case, since the standard contract method clarifies the concept of "network operator," its scope of application should be consistent with laws and regulations such as "network security law."

2.3.3. Analysis of Key Issues

The standard contract is applicable to a variety of personal information outbound scenarios, such as human resource management and business needs within multinational groups, Chinese companies purchasing overseas services or products, and providing services to domestic customers. Enterprises need to judge whether they can provide personal information overseas by signing standard contracts according to their own conditions. In practice, enterprises often face difficulties due to the complexity of business scenarios and data flows. In view of the difficult problems, it is necessary to make prudent judgments based on regulatory consultation, industry practice and specific scenarios. Although Article 4 of the " Measures " clearly stipulates that personal information processors may not use quantitative splitting and other means to avoid exit safety assessment, the specific explanation still needs to be further explained by the regulatory authorities.

2.4. Limited Contractual Binding Force

Annexed to the Scheme is a model standard contract, The main content of the standard contract is to include the definition and basic elements of the contract, the contractual obligations of the personal information processors and the overseas recipients, the impact of the foreign recipients' national or regional policies and regulations for the protection of personal information on the performance of the contract, the rights of the subjects of personal information and related remedies, and termination of contracts, liability for breach of contract, dispute resolution, etc., It also designed two appendices on the exit of personal information, other terms agreed between the two parties, etc. Although the Approach provides for standard contracts, in practice the signing and performance of contracts depends primarily on the conscious nature of each enterprise. In the absence of effective regulation and strict legal liability, some companies may be at risk of non-signing or breach of contract.

2.5. Differences in Data Protection Levels

In the United States, for example, as an advanced information technology country, The United States has the world's leading cloud computing services industry, and the United States promotes the free flow of data across borders in TPP. Opposing the imposition by other Governments of restrictions on the cross-border movement of Internet data, Opposition to other countries' local storage requirements is intended to clear the way for U.S. companies to open up international markets. Due to different levels of data protection in different countries and regions, the personal information of our citizens may not be protected to the same degree after leaving the country. In the event of data breach or misuse, this will cause great damage to the legitimate rights and interests of our citizens.

2.6. Cross-border Cooperation and Conflict of Laws

The ' method ' only requires that the contract subjects should follow the rules of contract conclusion, but it does not specify the requirements for the specific personal information exit. How to realize the safety and controllability of personal information exit on the basis of respecting the autonomy of the contract subject still needs to be further clarified.

Taking Article 6 of the " Measures " as an example, " Provisions to be observed by data receivers in carrying out data outbound activities, " although proposed for cross-border data transmission, it is actually applicable to any country and region. This clause only requires ' personal information collected and generated during operation in China ', but does not specify what kind of situation belongs to ' personal information collected and generated during operation in China '. If only ' personal information collected and generated in the operation in China ' is used to define the data receiver to carry out data outbound activities, then whether it is operating in China or cross-border transmission, as long as the agreement is reached between the contract subjects, it belongs to the ' personal information collected and generated in the operation in China ' required by the ' method '. Therefore,

it needs to be further clarified in the specific practice process. In addition, Article 13 of the ' Measures ' clarifies the scope of the subject of personal information transmitted across borders, including ' outbound personal information processors ' and ' personal information processors '.

The former refers to the data processor in the territory, that is, the data processor who collects and generates personal information in the territory ; the latter refers to the data processing institutions established in the territory, that is, ' overseas organizations and individuals carrying out data processing activities involving the transmission of personal information to the territory shall abide by these measures '. This provision actually expands the scope of the subject of ' personal information collected and generated in domestic operations ', and lays the foundation for subsequent cooperation with different countries and regions.

In practice, some overseas enterprises may use their overseas branches to carry out data outbound activities. If an overseas enterprise regards its overseas branch as a " personal information processor " within the meaning of the " Measures, " then the personal information collected and generated during its operation in China is within the meaning of the " Measures. " Personal information collected and generated during operations in China. This provision will undoubtedly have a greater impact on domestic enterprises to carry out overseas data outbound activities.

2.7. Risk Response to Emergencies

2.7.1. Emergencies that May Occur During the Cross-border Flow of Data

In the process of cross-border data flow, the possible emergency events mainly include data leakage, network attack, network security review by overseas anti-intelligence agencies, other countries or regions, network security risk assessment in cross-border data transmission, key information infrastructure attacks affecting national security, and large-scale hacker attacks.

2.7.2. Causes of Emergency Response Risk

The risk of inter-country data flow caused by inter-country data flow and the risk of cross-border data flow caused by external factors are the root causes of the emergency response risk of cross-border flow of personal information. Fundamentally speaking, it is because of the inconsistency of cognition and legal system of data protection among countries (regions), which leads to the game of interests among countries (regions).

Judging from the security incidents of cross-border flow of personal information in China in recent years, most of them are caused by the violation of the relevant requirements of the " Personal Information Outbound Standard Contract Measures " by overseas data recipients. For example, the " Didi Chuxing " platform data leakage incident last year was mainly due to the fact that the overseas data receiver violated the relevant requirements of the " Personal Information Exit Standard Contract Approach " and did not communicate and consult with the domestic data processor on the exit matters. This shows that the understanding of personal information exit security incidents at the national level is inconsistent, and it also shows that personal information exit security incidents are not handled well. From this point of view, China should timely modify the ' personal information exit standard contract approach '.

2.7.3. Possible Consequences of Inadequate Risk Response in Emergency Response

If the data processor or the overseas data receiver does not take effective measures to deal with the data outbound emergency in time, the possible consequences are mainly the following two:

One is the serious consequences. That is, the failure of data processors or overseas data receivers to take timely and effective measures to respond to data exit emergencies may lead to the following consequences : overseas receivers or overseas data processors directly or indirectly suffer economic losses ; it may lead to the spread of personal information exit security incidents, and further lead to the occurrence of personal information exit security incidents.

The second is the possible consequences : if the network information department believes that it is necessary to investigate and deal with the incident, it can require the data processor and the overseas data receiver to take disposal measures such as stopping transmission, deletion and destruction. Article 9 of the " Measures " stipulates : ' Any organization or individual has the right to report any violation of the provisions of this Measures to the network information department. However, the network information department can only deal with the events that have occurred, and cannot investigate and deal with the events that have not yet occurred.

3. SOLUTIONS TO RISKS

3.1. Limited Scope of Application

The " approach " is mainly aimed at the behavior of Chinese enterprises to transmit personal information abroad, and the behavior of foreign enterprises to transmit personal information to China has not been clearly defined. This may lead to the failure of effective supervision of overseas enterprises in dealing with the personal information of Chinese citizens. This approach is applicable to the domestic processing and transmission of personal information to foreign countries, including data transmission with foreign enterprises, and the transmission of personal information to foreign countries by domestic enterprises in China. The " measures " do not clearly stipulate the behavior of foreign enterprises to transmit personal information to China, which leads to the inability to effectively supervise all behaviors involving personal information outbound.

For example, for the storage of personal information in China through technical means such as cloud platforms, it is difficult to achieve effective supervision because it is not licensed by users. With regard to cross-border transmission of important data that partially involves personal privacy, the ' Measures ' only mentions in Article 4 that ' exit control is deemed necessary by the assessment of the national network information department '. For such enterprises, there may be compliance risks when conducting cross-border data transmission with overseas enterprises. If they cannot pass the assessment, they need to reconsider whether they need to comply with the ' measures '.

3.2. Insufficient Supervision

One of the highlights of the " Personal Information Outbound Standard Contract Measures (Trial) " is that under certain conditions, overseas enterprises can entrust personal information to a third party for processing. This provides a new choice for Chinese enterprises to transfer personal information overseas by signing standard contracts. However, there is no clear stipulation on how to determine whether the behavior of overseas enterprises is compliant, whether they are qualified, and when entrusting third parties to process personal information.

Therefore, in practice, the regulatory authorities may face the following difficulties:

1) High labor costs: In the absence of sufficient manpower in the regulatory authorities, it is impossible to conduct a comprehensive and detailed review of all outbound personal information. This may lead to the failure to detect and stop some non-compliant personal information outbound behavior in time.

2) High law enforcement costs: In the absence of clear regulatory rules and law enforcement basis, the regulatory authorities may face difficulties in obtaining evidence and high law enforcement costs, and it is difficult to effectively crack down on non-compliant personal information outbound behavior.

3) Cross-border collaboration problems: Due to the different legal systems, regulatory policies and enforcement efforts of different countries, regulatory authorities may encounter great difficulties in cross-border collaboration. For example, in the case of foreign enterprises, it may be difficult for

China 's regulatory authorities to effectively supervise them and stop the illegal exit of personal information in a timely manner.

4) Technical means can not keep up: With the rapid development of Internet technology, the ways and means of personal information outbound are increasingly diversified. It may be difficult for the regulatory authorities to keep up with these changes in technical means, resulting in the inability to effectively supervise all outbound personal information.

5) Insufficient self-discipline of enterprises: Some enterprises may be driven by interests and leave personal information out of the country without full review, and even have illegal acts. In the absence of clear legal constraints, the lack of self-discipline of enterprises can easily lead to the exit of non-compliant personal information.

3.3. Limited Binding Force of the Contract

The implementation of the " Personal Information Exit Standard Contract Method " provides a reference contract for enterprises and personal information subjects to ensure the safety and legitimacy of personal information in the process of cross-border transmission. However, the signing and implementation of standard contracts mainly depend on the consciousness of the enterprise, which has certain risks.

In the absence of effective supervision and strict legal liability, enterprises may intentionally or unintentionally violate the contract and cause damage to the rights and interests of personal information subjects. For example, in cross-border data transmission, companies may disclose personal information or use personal information for illegal purposes. These acts may pose a threat to the privacy, property and even personal safety of the subject of personal information.

In addition, the specific terms and contents of the standard contract may also be controversial and uncertain in interpretation, resulting in difficulties in contract enforcement. For example, there may be ambiguity or ambiguity in the contract regarding the protection of personal information, the conditions and methods of cross-border transmission of data, etc., which requires consultation and communication between enterprises and personal information subjects to ensure that the implementation of the contract is in line with the interests and needs of both parties. However, in practice, there may be problems such as information asymmetry and conflict of interest between enterprises and personal information subjects, resulting in poor negotiation and communication, which in turn affects the implementation of the contract.

3.4. Differences in Data Protection Level

The " Personal Information Exit Standard Contract Method " clearly states that when performing the contract, each participant shall ensure the security of data according to the purpose, scope and method agreed in the contract, and shall not use personal information beyond the agreed purpose and scope. However, in practice, there may be differences in the level of data protection in different countries and regions, which will affect the legality of foreign enterprises ' processing of personal information of Chinese citizens.

For example, for the EU, its data protection level may be higher than that of China. EU law clearly stipulates the principles and standards to be followed in the process of personal data processing, as well as the obligation to protect the personal data of EU citizens. For example, the General Data Protection Regulation (GDPR) stipulates that enterprises should follow the principles of legality, fairness and transparency when dealing with personal information, take appropriate technical and organizational measures to ensure the security of personal information, and inform the subject of personal information of their rights and protection measures. In addition, the GDPR also stipulates strict conditions for cross-border data transmission, requiring companies to take appropriate

safeguards when transferring personal information across borders, such as signing standard contracts and obtaining sufficient authorization.

Therefore, the processing of personal information of our citizens within the EU will face higher compliance costs and higher legal risks. For example, companies may need to invest more resources to ensure the security and compliance of personal information, including adopting appropriate technical measures, formulating sound internal policies and procedures, and conducting employee training. In addition, companies may also face higher risks of fines and penalties. If they violate the EU 's data protection regulations, they may be subject to high fines or even prohibited from operating within the EU.

3.5. Technical Means is Difficult to Keep up

With the rapid development of network and information technology, security risks such as network attacks and data leakage are constantly emerging. In the current context, it is difficult to effectively prevent various types of security risks only by the company 's own security protection measures.

For example, in February 2023, ByteDance was banned from using TikTok by the US government due to serious data security risks. This incident has aroused worldwide attention to data security. TikTok is a popular short video application with hundreds of millions of users. However, due to loopholes in its data processing methods, the user 's personal information is leaked to third parties. Therefore, data security has become an important issue for enterprises and individuals. In the current network environment, enterprises should establish their own network security protection system as soon as possible to cope with the increasingly complex and diverse network environment.

The ' method ' puts forward three technical requirements for enterprises : first, to establish and improve the network security level protection system ; second, the development of data classification and grading guidelines ; third, formulate a personal information outbound risk management plan. However, it should be pointed out that the technical requirements stipulated in the ' approach ' are too simple to cover all types of enterprises. Due to the differences in the processing of data in different industries, the technical measures adopted by different enterprises in the same industry may also be different. In addition, the ' approach ' only puts forward general requirements for enterprises, and it is difficult to stipulate specific measures for enterprises in special industries and special fields. Therefore, enterprises should formulate personalized and differentiated safety programs according to their own conditions, and constantly optimize and improve them in practice.

3.6. Cross-border Cooperation and Legal Conflicts

In the process of cross-border transmission of personal information, both individuals and enterprises will inevitably involve laws and regulations of different countries and regions. Especially in cross-border cooperation with China, it is necessary to abide by the laws and regulations of two or more countries and regions at the same time. For example, when conducting cross-border data transmission with the United States, it should comply with relevant legal provisions such as the " Foreign Intelligence Surveillance Act " of the United States to clarify the legal use of overseas data and the " Cloud Act " ; when conducting cross-border data transmission with Russia, it should comply with Russia 's " personal data law, " the Russian Federation 's national security law and other relevant legal provisions.

In addition, there are some other legal cases involving cross-border cooperation and conflict of laws. For example, in 2020, U.S. President Donald Trump signed an executive order requiring ByteDance to sell its short video app TikTok 's U.S. business because the U.S. government considers TikTok a security risk. This incident has aroused worldwide attention and controversy. In this case, TikTok is facing legal proceedings and investigations from the United States. The U.S. government has accused TikTok of security risks and banned it. In addition, the U.S. government has also tried to suppress

TikTok through other means, such as threatening to ban U.S. companies from doing business with TikTok.

This case reflects the complexity and sensitivity of cross-border cooperation and conflict of laws. In cross-border cooperation, enterprises need to understand and comply with the laws and regulations of different countries and regions to ensure their own legal compliance. At the same time, governments also need to strengthen cooperation to jointly deal with legal conflicts and risks in cross-border cooperation.

4. MANAGEMENT SYSTEM OF INTERNATIONAL DATA FLOW ACROSS BORDERS AND ENLIGHTENMENT OF CHINA'S MEASURES

4.1. Clarifying Basic Ideas for Data Flow Management Across Borders

Both the United States and the European Union adhere to their core strategic interests and adopt different management strategies to handle data input and output.

The National Security Strategy Report of the United States places data security as a key element of national security, with a focus on preserving America's superiority in cyberspace and data resources. Advocates for "free data flow" in data entry, leveraging U.S. IT strengths and leveraging global data resources to drive its digital economy. In terms of data export, export controls are used to restrict the export of high-tech, dual-use technical data.

The EU is guided by the Digital Single Market Strategy and adopts the idea of "internal and external tight" data flow management across borders. In 2018, the EU introduced the Framework Regulation on the Free Movement of Non-Personal Data in the EU, which forms the legal framework for data protection in the EU. On the one hand, the Framework Regulations promote the free flow of data within the EU, and on the other hand, the GDPR enhances control over the movement of data abroad.

4.2. Set up a Differentiated Data Exit Security Management System

According to the characteristics of countries, the United States, the European Union and other international organizations have adopted targeted data cross-border control measures aimed at safeguarding national security, safeguarding the public interest and protecting the legal rights of individuals.

On the one hand, personal data is generally allowed out of the country where the data recipient is located when certain security requirements are met. On the other hand, control the exit of important and personally sensitive data. According to the data attributes and the degree of influence, some countries to the banking, finance, credit and other important industries or areas of data to implement exit control; Some countries selectively implement exit bans or restrictions to prevent leakage of relatively sensitive data on health, taxes, maps, governments, etc., depending on their national circumstances and political and cultural differences.

5. ENTRY POINTS FOR REDUCING OPERATIONAL RISK IN THE SCHEME

5.1. Issues for Enterprises to Pay Attention to in the Practice of the Scheme

When conducting impact assessments of personal information protection, enterprises should conduct detailed and in-depth analyses to comprehensively identify potential risks and ensure the accuracy of the assessment results. When conducting cross-border flow of personal information data, enterprises shall pay attention to the protection of users' rights and interests, fully inform users of the purpose,

method, scope and other information of personal information processing, and obtain users' express consent. Enterprises should also formulate contingency plans for emergencies such as leakage of personal information, and clearly define the emergency response process and division of responsibilities to ensure that they can respond swiftly in the event of an emergency. When encountering doubts or difficulties in practice, promptly seek guidance from professional lawyers or compliance consultants to ensure that the enterprise's personal information handling activities are compliant. On this basis, pay close attention to the policies, regulations and guidelines issued by the relevant state departments, and adjust the enterprise's personal information protection strategy in a timely manner to ensure compliance.

5.2. Improve Relevant Legal Regulations

Enterprises are required to conduct personal information protection impact assessment when fulfilling the Measures. Some of the contents of its assessment are slightly vague, which can easily cause enterprises to make misjudgments, and further detailed regulations should be made.

In addition, it is also necessary to refine the responsibilities of information receivers such as:

1) Overseas receivers should adopt data security measures, including technical means, access control, data encryption, network security, etc., to ensure the security of personal information in the process of transmission and storage.

2) Overseas receivers should respect and safeguard the rights of the users including the rights to query, correct, delete personal information, etc.

3) Evaluate if the overseas receivers are cooperating with our supervisory authorities, and whether it can respond and deal with complaints from users in a timely manner when they are received.

4) The offshore recipient shall formulate an emergency response plan for data leakage and how it will take timely measures to mitigate damages in the event of a data leakage.

Although the Measures provide for a standard contract, the signing and fulfilment of the contract still relies on the self-consciousness of enterprises. In order to safeguard the security of users' personal information and strictly pursue legal responsibility, relevant regulations can be formulated to supervise and control. With the advancement of science and technology and the diversification of cross-border data transmission methods, the existing laws and regulations may be difficult to adapt to the regulatory needs of the new situation, which leads to the use of loopholes in regulations by some enterprises for the exit of personal information, in order to formulate relevant laws and regulations to curb the emergence of this behaviour.

5.3. Promoting International Exchange and Co-operation

In the actual operation of the Measures, enterprises are unable to do real-time supervision on whether the information receivers keep personal information properly. International efforts are being made in this regard, such as the United Nations, which promotes cooperation and coordination among countries in cross-border data flow by formulating relevant regulations and resolutions. China should actively participate in international exchanges and cooperation to minimise the risks. As there are differences in the definition of information security among countries, they should gradually reach a common understanding through communication and exchange on the premise of finding the largest common denominator, so as to lay a solid foundation for cooperation in maintaining information security. At the same time, it should also actively promote the establishment of interstate information protection treaties and other institutional mechanisms.

6. CONCLUSION

The main objective of this paper is to study the security and legality of personal information transmitted to other countries.In the course of studying the Standard Contract Method for the Export of Personal Information, We mainly identified the risks of this approach in operation. and the practical challenges faced by these risks, such as limited scope of application, inadequate regulation, differences in data protection levels, limited contractual binding, technical lag, cross-border cooperation and legal conflicts.

Through risk analysis, the revelation and suggestion of this approach are obtained. Put forward some strategies and suggestions to reduce the legal regulation of cross-border data flow. We hope that these reflections and suggestions can provide a meaningful reference for the improvement of the security of cross-border data flows in China for the relevant national regulatory departments, to better protect each country from the use of personal information by illegal elements while crossing borders, Help our country achieve better results in data protection.

This study also has limitations. It does not give a comprehensive consideration and suggestions on the risks and challenges faced by this approach in practice. In the future, the relevant legal researchers can give suggestions on the legal formulation in the light of more comprehensive and systematic analysis of the actual needs of cross-border information.

REFERENCES

[1] Ran Congjing,Liu Ruiqi,He Mengting. International personal data cross-border flow governance model and China's reference study[J]. Journal of Information Resources Management,2021,11(03):30-39.DOI:10.13365/j.jirm. 2021. 03.030.

[2] Licence. Freedom and security:China's solution to cross-border data flow[J]. Global law review,2021,43(01):22-37.

[3] Gao Shanxing,Liu Weiqi. Regulation of Cross-border Flow of Data and Its Response - A Discussion on Article 37 of the Cybersecurity Law[J]. Journal of Xi'an Jiaotong University (Social Science Edition),2017,37(02):85-91. DOI:10.15896/j.xjtuskxb.201702012.

[4] Dongfang. Comparative analysis of legal regulation of cross-border data flow in the EU and the United States and the "Chinese wisdom" to cope with the challenges[J]. Library Journal,2019,38(12):92-97+104.DOI:10.13663/ j.cnki. lj.2019.12.012.

[5] Wen Hao. Research on Information Security Issues in Foreign-related Commercial Behaviour [N]. People's rule of law, 2021-9-5.

[6] WANG Weiling. Systemic Risks of Cross-border Flow of Data: Causes, Development and Regulation[J]. International Trade, 2022(7).

[7] Pan Xiaoning. Reflections on Improving China's Personal Information Data Exit System[J]. Customs and Economic and Trade Research,2019,40(06):81-93.

[8] Wu Xuan. The construction of cross-border rules for personal information under the vision of data sovereignty[J]. Tsinghua Law,2021,15(03):74-91.

[9] Lou He, Chen Guoyu. Discussion on the Best Legal Practice of Cross-border Transmission of Personal Data of Chinese Enterprises[J]. Information Security and Communication Confidentiality,2019,No.308(08):50-62.

[10] Wei Wei. Li Xiaowei. Zhang Yuanyuan. JIANG Yuzhe. International data cross-border flow management system and its inspiration to China[J];Secrecy Science and Technology;2020.