Academic Journal of Management and Social Sciences
ISSN: 2958-4396 | Vol. 7, No. 3, 2024

Research on the Balance Mechanism of Rights Conflict in the Cross-border Flow of Personal Financial Data

Yan Lu *

Department of Civil and Commercial Economics, China University of Political Science and Law, Beijing, China
*** Corresponding author Email:** luyanottillie@163.com

Abstract: The cross-border flow of personal financial data is inevitable due to the needs of cross-border business or overseas supervision such as anti-money laundering. The conflict between national financial security and financial efficiency results in a series of unbalanced situations under cross-border financial data. The state takes measures to regulate in order to balance different demands, promote economic development, and seek economic globalization. In an unbalanced state, the lack of systematic rights protection will lead to a lack of confidence in the degree of protection of personal financial data subjects, which may hinder the construction of global economic integration. This paper first analyzes the causes of imbalance from the perspective of value orientation and makes suggestions for institutional improvement. Secondly, from the perspective of the contradictions between the subjects of personal financial data rights and processors, as well as the contradictions between regulators, it studies the feasibility methods to check and balance and resolve the conflicts, so as to achieve the goal of clarifying the basic value and coordinating the conflict relationship. It should also focus on the development of national independent artificial intelligence, science and technology to help development cooperation, and the goal of international economic integration.

Keywords: Personal Financial Data; Cross-Border Flow; The Balance of Rights; Data Security and Freedom.

1. Introduction

On December 15th, 2023, China's National Development and Reform Commission issued the Three-year Action Plan of Data Elements × (2024-2026) (Draft for Comment), which requires improving the ability of data supply, optimizing the data environment for data circulation and strengthening data security. As a kind of data, personal financial data is also applicable to its regulation, that is, "improving financial risk resistance and promoting digital". [1]

In the context of big data, financial data is no longer a single information set stored in a specific space. Data processors organize fragmented and striped data sets and process them into valuable data assets. Cloud computing, artificial intelligence and big data make the borderless nature of the Internet more obvious, the transnational and regional nature of data has also become the norm, and the property value of data can only be realized under the flow of data. a domestic isolated data processing cannot make data value and security situation.

From the national financial data supervision mode of "lenient entry and strict exit" in the United States to the strict supervision mode of data cross-border flow in the European Union, it can be concluded that the differences in national interest value judgments lead to the differences in legislation.

Personal financial data subjects' core pursuit of privacy protection and financial data processing subjects' focus on the interests of financial data and their derivatives are different, which leads to the contradiction between the two. In addition, the difference in legal value widens the distance between the rights of the individual and the financial data controller, compared with the financial data controller. Individuals may have more unequal access to overseas information with financial institutions, which makes the rights and interests of financial data at home and abroad more unequal. Or there is the problem that improper data processing of financial institutions makes it illegally used, and it is difficult for individuals to protect their rights. Therefore, it is necessary to explore specific ways to balance the conflicts of personal financial data in cross-border flows.

2. Basic Theory of Personal Financial Data Rights

2.1. The Definition of The Concept in the Legal Relationship of Cross-border Flow of Personal Financial Data

2.1.1. The Connotation of the Right of Personal Financial Data

Financial data refers to the data collected, processed and stored by the subject for business needs when conducting financial activities (including deposit and withdrawal, lending, acceptance, financing, etc.). In general, financial data includes personal financial data, corporate financial data and data generated during the operation of institutions. However, many normative documents mix data with information. For example, in the Technical Specification for the Protection of Personal Financial Information, "data" [2] is mentioned in the introduction, but "information" [3] is used in the provisions, that is, the term "financial information" is used. For the definition of "personal financial information", China's relevant technical specifications have specific provisions, that is, "financial institutions through the provision of financial products and services or other channels to obtain, process and preserve personal information." [4] This includes "account information, identifying information, financial transaction information, personally identifiable information, property information, borrowing information, and other information that reflects certain circumstances of a particular individual financial information subject." [5] Personal financial information is the refinement of personal data in finance, with the commonality of personal information, "virtuality, identifiability and certainty, personality rights and property

rights", because the collection, storage, utilization, transmission and disclosure of personal information in financial institutions has its own characteristics, so it also has its own characteristics. [6] This paper studies the universally applicable way of checks and balances, so it takes "personal financial data" rather than personal financial information as the research object.

2.1.2. The Connotation of Personal Financial Data Subject

The extension of the subject of personal financial data is greater than that of financial consumers. "personal financial data subject" is "the natural person identified by personal financial data". [7] Financial consumers refer to "natural persons who purchase and use financial products or services provided by banks and payment institutions". [8] The former also includes the natural persons of financial institutions who obtain, process and save financial data through other channels other than products and services, so this paper uses the term personal financial data subject in order to study the universality.

2.1.3. The Subject of Personal Financial Data Processing

The European Union's General Data Protection Regulation (GDPR) divides the subject of data processing into two categories: data controllers and data processors. A data controller is an entity that "determines, alone or jointly with others, the purpose and manner of processing of personal data," as opposed to a "data processor," which, as its name suggests, is merely an entity that authorizes the processing of data on the basis of a delegated relationship. [9] The former has more discretion over data processing than the latter. As one of the types of data, the processing subject of financial data is also classified in this way. In China, normative documents with different definitions and scopes of data processing subjects have different definitions and scopes. Some refer to all the processing subjects as "personal data processors", [10] and it is not difficult to see from the text of the whole law that its scope includes the data processing subjects of the above two categories of GDPR. Others only emphasize "personal financial data controller", [11] which is obviously greater than other countries' processing control authority, but what kind of financial institutions have the right to decide its scope has not been further confirmed. In other normative documents, although "personal information controller" is emphasized, combined with other provisions, it includes the scope of the controller and processor. [12] This uncoordinated definition of scope will cause more problems under the background of cross-border data flow, further aggravating the risk of personal data leakage and even endangering national social security. Therefore, the definition scope of the subject of financial data processing in China should be further clarified by normative documents with strong legal effect. This paper tends to analyze and study the term of personal financial data processing subject with higher level of effectiveness.

2.1.4. "Cross-border" Flow of Personal Financial Data

The "cross-border" flow of personal financial data usually refers to the active or passive flow of personal financial data outside the territory when individuals conduct financial activities in response to specific needs. In special circumstances, individuals or enterprises put relevant data in domestic servers, but the data can be obtained by overseas entities. Whether this situation can be regarded as a cross-border flow of relevant data is controversial. Those who deny it believe that individuals do not actively upload and modify data, and if it is applied without authorization [13], it may interfere with personal rights and make the relevant legal system applicable in an expansive manner. Supporters believe that if it is not interfered with, it will not only damage the rights of data subjects, but also increase the workload of data controllers. Therefore, the current general practice is to further refine the regulations on the basis of recognition, and it is necessary to protect or supervise them when they reach a certain stage. [14] In China, personal financial information generated in the process of practical financial products or financial services is sensitive, which involves not only personal data security but also national security. [15] Therefore, unless otherwise stipulated by law, the principle of data localization should be maintained.

2.1.5. Personal Financial Data Rights

Personal financial data rights refer to the rights enjoyed by personal financial data during the collection, processing, transmission, and storage process. According to their nature, they can be divided into personal financial information rights (personal financial data rights in a narrow sense) and personal financial privacy rights, while personal financial information rights can be divided into general financial information rights and sensitive financial information rights. This article mainly studies the broad personal financial data rights from the perspective of combining financial law with private law.

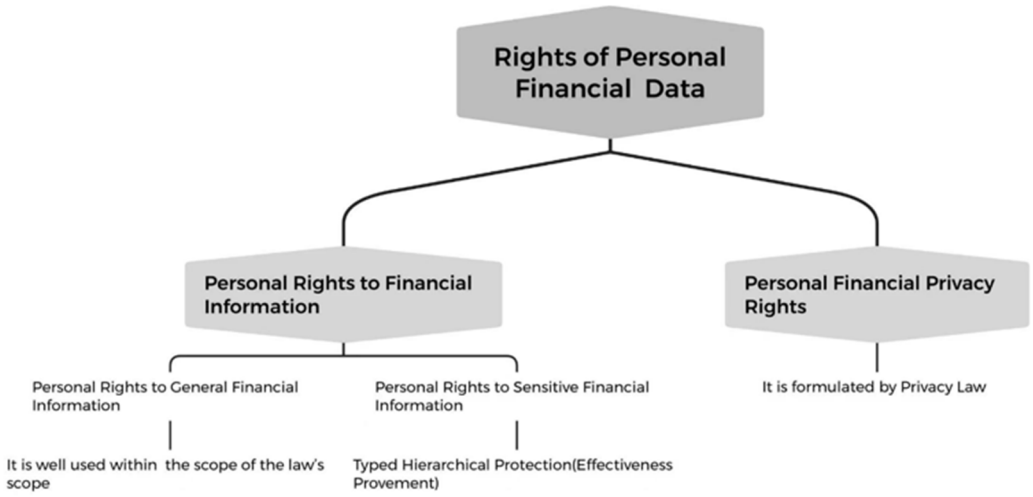

Fig 1. The sub content of the personal financial data rights
Source: author collation

2.2. The Necessity of Protecting the Rights in the Cross-Border Flow of Personal Financial Data

2.2.1. The Realistic Demand of the Cross-Border Flow of Personal Financial Data

In the context of economic globalization, the scope of financial data controllers has expanded from financial institutions to the Internet field, including licensed financial institutions regulated by national financial regulators, licensed non-financial institutions and enterprises that provide services and support to licensed financial institutions. Financial data controllers will also pose different risks to national security in the process of collecting personal data for legitimate and specific purposes. [16] Cross-border personal financial data not only includes the needs of cross-border business, there are mainly branches of one country for the transmission of domestic data to the headquarters of other countries, data sharing or transfer between financial institutions and third-party institutions in other countries, service outsourcing, etc.; it also includes overseas regulatory requirements such as anti-money laundering. [17]

2.2.2. Lack of Effective Protection Means in the Cross-Border Flow of Personal Financial Data

In the cross-border flow of data, due to the limitation of the rights of the data subject, there is a lack of the right to know the collected personal financial data, even if it is infringed or even known, but the rights cannot be safeguarded due to the high cost of safeguarding rights abroad; due to improper acts such as illegal collection and illegal disclosure of data processing subjects, infringe upon personal financial data rights and endanger national financial security. Due to the lack of careful protection of the required data or lack of technical skills, the rights of personal financial data have been infringed. At present, the general management of the outbound transfer of personal data is the individual's obligation to inform, that is, the individual shall explain the purpose, content and scope of the outbound transfer of personal financial data and the data recipient country, and the data controller's assessment obligation, that is, the network operator shall organize a security assessment of the outbound transfer of data on its own and be responsible for the assessment results. When important data is involved, it shall be reported to the competent industry department. [18] For important data, the law has obligations on data security protection, notification before cross-border transmission and security assessment of data controllers. [19] However, the extension boundary between important data and personal financial data is not clearly defined, which leads to the low feasibility of rights protection, so it is necessary to reiterate the importance of rights protection and study its implementation path.

2.2.3. Necessity of Legal Intervention in Cross-Border Flow of Personal Financial Data

Technological innovation makes the cross-border flow of personal financial data more convenient and popular. On the one hand, the personal financial data of our country will be exposed to the vision of other countries, and other countries may analyze the financial security-related data of related countries such as their own economic situation based on this information, which will endanger national security.

On the other hand, it will increase the gap in information acquisition between financial institutions and individuals, and even if individuals guide infringement, they will be unable to defend their rights because of insufficient strength, thus endangering social stability. Therefore, it is necessary to define the relevant power and balance the imbalance in the cross-border flow of personal financial data in order to safeguard national security, maintain financial stability and security, and protect citizens' individual rights. Traditional cybernetics of personal data holds that personal (financial) data processing needs the consent of the subject of personal (financial) data. For example, Europe focuses on the protection of personal freedom and human rights, and the theory of personal data protection based on privacy protection in the United States provides theoretical support for the protection of personal data. [20] But in the long run, the excessive emphasis on data self-determination will increase the operating cost of the whole financial society and reduce financial efficiency, which is contrary to financial goals. Therefore, it is necessary to carry out legal intervention and stipulate the boundary of individual financial rights protection.

2.3. The Basis of Rights Protection in the Cross-border Flow of Personal Financial Data

In the cross-border flow of personal financial data, the risk of personal financial data rights and the risk of financial privacy are essentially different, and the legal provisions applicable to their protection are also different. "In order to solve the contradiction between system interpretation and value evaluation, it is the most convenient and effective way to regulate the right to privacy and personal data protection separately." [21] Privacy data involved in personal financial data are intervened by the privacy law with a complete set and corresponding relief system, while the classified protection of other personal financial data can improve financial efficiency and reduce the conflict between financial data processing subjects and financial data subjects through clear and clear authorization, especially under the background of cross-border financial data flow, because the unknown and uncontrollable data flow is greater than domestic data flow, it is easy to produce social instability.

3. Imbalances in the Cross-Border Flow of Personal Financial Data

The requirements for the cross-border flow of personal financial data in China are very strict: the cross-border flow of personal financial data in accordance with the regulations, not only need to comply with the requirements of special circumstances of relevant laws and regulations, after obtaining the express consent of the subject of personal financial data, after the security assessment of relevant institutions, but also need to sign agreements with data recipient countries to ensure the security of data after cross-border flow. [22] However, in the process of implementation, the problem of imbalance is still common.

3.1. Unbalance between Free Flow of Personal Financial Data and Financial Security under Cross-border Conditions

The cross-border flow of personal financial data is not only for the needs of multinational enterprises because of their business behavior, but also conducive to strengthening

cooperation between countries, realizing a unified world market, breaking the information barrier of the market, optimizing the allocation of resources in the world, and promoting the application of domestic science and technology to the market under the background of new quality productivity, thus realizing economic globalization and integration. However, the cross-border flow of personal data also increases security risks. Technological progress makes it more convenient for data receiving countries to obtain financial data of data producing countries through the analysis of personal financial data, which increases the risk of national security. Therefore, it is of great significance for domestic and foreign financial institutions to participate in the globalization of China's financial market, attract foreign investment to build the China market and expand the opening of China's financial market to balance financial security and cross-border flow of personal financial data.

3.2. Cross-Border Value Imbalance between the Subject of Personal Financial Data and the Subject of Financial Data Processing

The cross-border flow of personal financial data increases the information gap and increases the difficulty of personal rights protection. First of all, in the field of cross-border financial business, the power of data processing is entirely in the hands of financial institutions, and as a result of multi-link data processing, the data is no longer within the control of the original data collectors, even overseas institutions, compared with the traditional domain to transmit personal financial data, it is very difficult for data subjects to understand how financial institutions deal with their personal data. As well as whether there are cases of unauthorized or excessive handling of cross-border flows, it is difficult to know whether their rights have been violated. Even if the receiving country fulfills the obligation of disclosure in strict accordance with the law, it has long been unable to identify the data subject because of the large number of links. Therefore, while paying attention to financial efficiency, what kind of institutional system should be taken into consideration. Secondly, the cost of safeguarding rights is high, and many subjects who infringe upon the right to personal financial information are abroad, while the factors of poor information and geography, different legal systems and timely bilateral agreements still increase the cost of safeguarding rights compared with China. Therefore, how to use industry associations and standardize the responsibilities of data processors to balance conflict points is worthy of further study.

Secondly, because of the demand of financial activities and the attribute of public interest, individuals will transfer their personal financial rights to financial data processors in financial activities. It is still more clear whether derivative data and value-added data fall within the scope of the rights and interests of financial institutions and whether data can be shared without personal consent. [23]

3.3. The Imbalance between the Main Body of Personal Financial Data Processing and Financial Supervision and Management Across Borders

First of all, there is an irreconcilable contradiction between the pursuit of the interests of the subject of personal financial data processing and the positioning of financial regulatory institutions to maintain national financial security. Countries have different legal positions according to their own financial conditions and the development level of financial science and technology. However, the cross-border flow of data will make different legal positions conflict. How to reconcile the conflict between financial data producing countries and financial data receiving countries on the degree of protection of personal financial data is of great significance. For example, the United States is a leader in the development of financial technology at the world level, and its pursuit of market efficiency is higher than other values, so it is more inclined to the concept of free flow of financial data across borders. In the formulation of legal rules for the flow of cross-border personal financial data, it tends to lower the threshold for data flow so that it can take advantage of high technology to analyze and process data. On the other hand, the European Union is more inclined to the protection of personal data. In order to reconcile the needs of financial data security and cross-border flows, the EU has even established a whitelist mechanism to fully protect it. However, the legal positioning of the world's two major economic entities did not stop their cooperation. After the U.S.-EU Privacy Shield Agreement was declared invalid by the European Union in July 2020, the two further promoted the cross-border flow of data in 2023 to negotiate a new framework, the U.S.-EU data Protection Framework. The supervision of cross-border flow of financial data is essentially a legal restriction of national public power on the management of financial markets and economic and social life. [24]

Secondly, there are also imbalances within the financial supervision departments. The domestic supervision of personal financial data adopts the dual-track parallel supervision system of online information department and financial supervision. The online information department is only responsible for the cross-border coordination and overall planning of data, [25] but it is further detailed. No matter between the online information department and the financial supervision department or between the central and local financial supervision departments, the supervision subject of cross-border flow of personal financial data is not clear, resulting in the cross-border flow of personal financial data or the internal vacuum or overlap of supervision. For example, the legal provisions on the protection of financial data in the Regulations on the Management of Financial Information Services formulated by the Information Office in 2018 are vague; In 2020, the central bank issued the "Guide to Financial Data Classification", "Technical Specification" and other industry self-regulatory normative documents, which separated the protection of personal financial data rights and made it easy for owners to have conflicts when defending their rights.

4. Checks and Balances in the Cross-border Flow of Personal Financial Data

4.1. Ways to Balance the Value Orientation in the Cross-Border Flow of Personal Financial Data

4.1.1. Legal Regulation of the Hierarchical Flow of Personal Financial Data

First of all, standardize and legalize. At present, China only has the industry standard "Information Security Technology personal Information Security Standard" to carry out fine

evaluation according to the types and uses of data, and there are no legal provisions. Based on the flow of personal and corporate customer information for commercial purposes, emphasis is placed on the rights of the data subject and the assessment of the information security status of the place of receipt. The definition + enumeration method is adopted to make clear the difference between personal information and personal sensitive information, but the coercive force of this operating standard is not as strong as laws and regulations, and its direct applicability is reduced in the era of globalization.

Secondly, evaluate the background. Sensitive personal information should be stored and transmitted by means of encryption, separate storage, summary storage and so on. But sensitivity may vary from background to background. Therefore, we can make use of data environment assessment, consider its sensitivity under different political and cultural backgrounds, and make full use of the principle of equality. The degree of legalization, the ability of data protection and the intensity of supervision of the countries or regions that plan to realize the cross-border flow of financial data will be taken into comprehensive consideration, on the premise of meeting the laws, regulations and regulatory requirements of our country. Further refine the general rules and general applicable principles for guidance, which is conducive to the use of multilateral cooperation.

4.1.2. Rational Application of Science and Technology to Help

Law is the cornerstone of personal information protection, while technology is an important means to achieve effective protection. Therefore, we should strengthen cooperation in the field of law and technology, jointly formulate and improve relevant laws and regulations, and at the same time promote the research and development and application of technology, so as to better meet the challenges brought by cross-border data flows. For example, the EU requires processors to implement appropriate technical and organizational measures to ensure a level of security commensurate with risks. The law requires controllers and handlers to consider the "level of technology", the cost of implementation, the nature, scope, background and purpose of the treatment, as well as the possibility of changing risks, as well as the severity of the rights and freedoms of natural persons. [26] Therefore, it is also very important to make clever use of science and technology.

4.2. The Balance of Rights between Data Subjects and Processors in the Cross-border Flow of Personal Financial Data -- Detailed Scope and Infringement Protection

4.2.1. Solution of Internal Problems of Data Processors

4.2.1.1 Range of Data Controllers

To clarify the scope of data personal financial data processors, there are differences in the current "Network Security Law", "Information Security Technology personal Information Security Standard", "personal Financial Information Protection Technical Standard" and the supervision and management regulations of various industries. It is necessary for the subject with power to determine the scope in order to better regulate its behavior within the scope. The definition of "personal information processor" in the OECD framework refers to specific processing activities, that is, "collection, holding, processing, use, disclosure or transfer of personal information". This is a list that is more limited than the definition of "processing" as defined in the General data Protection regulations. The OECD framework defines controllers from the perspective of controlling data processing and excludes natural or legal persons acting under the instructions of others or organizations. (the definition includes instructions to another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf, but does not include a person or organization performing such functions in accordance with the instructions of another person or organization.) the definition of the controller in the General data Protection regulations is similar, but more comprehensive, as it includes joint control and is particularly applicable to individuals and organizations that process data on behalf of the controller. In the General data Protection regulations, the controller is defined as "a natural or legal person, public body, institution or other group that alone or jointly with others determines the purpose and manner of personal data processing". [27] The U.S.-South Korea Agreement is defined as "a financial institution is any financial intermediary or other enterprise that is authorized to conduct business in accordance with the law of the party where it is located and is regulated or supervised as a financial institution." [28] The Euro-Korean Agreement provides that "financial service provider means any natural or legal person of a Party that wishes to provide or make available financial services", [29] and similar bilateral agreements include the EU-Singapore Agreement, Organization for Economic Co-operation and Development (OECD) and others. The third is represented by the United States-Mexico-Canada Agreement, which refers to "a financial institution of the other party or a cross-border financial service provider of the other party that is regulated, supervised, licensed, authorized or registered by the financial regulator of the other party". [30] Therefore, the definition of the term in our country should be clearly defined in the law so that it can be used in the conclusion of bilateral agreements.

4.2.1.2 Refine the Obligations of Personal Financial Data Processors in the Cross-Border Flow of Financial Data

Although various laws and regulations stipulate the legal obligations of financial institutions to collect, process and delete all data cycles, it is necessary to recognize that what obligations should be borne in cross-border flows are different from those in China, so it is necessary to refine and specialize them. The OECD framework requires that data processors conduct due diligence if personal information is to be transferred nationally or internationally to another person or organization. -without the consent of the data subject, the controller shall "perform due diligence and take reasonable measures" to ensure that the recipient will protect the information in accordance with the principles in the framework. For example, what level of personal financial data should be protected and what level of security protection should be adopted, and how to cooperate to protect data security after arriving in the receiving country. For example, the new data protection framework in Europe and the United States makes it clear that the processor is responsible for the data transferred to a third party. According to the new EU agreement, in order to transfer personal information to a third party as the controller, it must comply with the notification and selection principles and sign a contract with the third party controller, stipulating that such data can only be

processed for limited and specific purposes consistent with the consent provided by the individual. And the recipient will provide the same level of protection as the principles of the data Protection Framework and notify the organization when it determines that this obligation can no longer be fulfilled. [31]

4.2.2. The Protection of the Subject of Personal Data Right Infringement

4.2.2.1 Prevention of Infringement

In the context of the European Union, it is required to evaluate data incidents, and when the rights and freedoms of natural persons are at high risk, the data subject should be clearly informed of the data leakage incident without undue delay. If the controller has implemented appropriate technical and organizational protection measures, and these measures have been applied to the data affected by the violation of personal data, there is no need to inform the data subject. In addition, it is required to appoint a "data protection officer", that is, "a person with professional knowledge in data protection law and practice to assist the controller or processor in monitoring internal compliance."[32] Similarly, Asia-Pacific Economic Cooperation (APEC) also requires personal information processors, agents, contractors or other service providers who transmit personal information to it to promptly notify the data controller of data leakage. At the same time, participants "take reasonable measures to ensure" that the service providers with whom they share personal information comply with the privacy policy; And "abide by the rights and obligations of participants on the safety, confidentiality, integrity, use and disclosure of personal financial data." [33]

4.2.2.2 Determination of Infringement

First of all, the criteria for determining the rights of personal financial data, in the European Union, emphasize the protection of basic rights and freedoms of citizens, [34] while APEC aims to promote the cross-border flow of data.[35] Different overall goals lead to different degrees of infringement recognition for the two. In the EU, simply violating human rights is enough; damage in the traditional sense of infringement does not need to be proved, and the infringement of personal financial data protection rights is itself a kind of harm. The APEC standard is like the standard of ordinary tort law because it applies to many APEC jurisdictions, but in some cases its standard of proof is lower than the standard of ordinary tort law, but generally it is higher than the standard of EU infringement. [36] Therefore, it is concluded that the level standard of the identification standard is linked to the value pursuit of the country. Combining the demand of financial security and the demand of protecting financial individuals, the author thinks that it is more intentional to compromise between the two. Secondly, the principle of tort exemption is expressed in "reasonable" terms in APEC, and many requirements are judged by "appropriate" attribution, which depends on the risk and type of injury to the individual. [37] However, because it is the minimum data protection standard, it can not reach the details and clarity of the EU General data Protection regulations, so our country should consider what is "reasonable" and "appropriate" and make exemplary provisions in the determination of the exemption principle.

As for the determination of rationality or appropriateness, Article 104 of the Introduction to the General Data Protection Regulation stipulates that rationality is basically equivalent to equivalence, that is, a third country or a specific entity ensures that "an adequate level of protection is basically equivalent to that ensured within the [European] Union." Article 107 states that adequacy decisions are also subject to periodic review to determine whether the entity still ensures an adequate level of data protection. Article 108 stipulates that the Committee shall consult with the entity and take into account relevant developments of the entity and information from other relevant sources, such as the findings of the European Parliament or the Council. Of course, there are exceptions. Without adequate protection, it is allowed to derogate from or exceptionally prohibit the transfer of personal data outside the EU. But only in special circumstances, such as the consent of the data subject after full knowledge, the pre-contract measures taken at the request of the data subject, the transfer is necessary and in the public interest, etc. [38]

4.2.2.3 Remedies for Infringements

The regulatory authorities may, in conjunction with overseas institutions, set up an international financial data tracking system to recover from the infringers in a timely manner. The network information department and the financial supervision department should undertake the obligation of education supervision, do a good job in popularizing the security risks of cross-border financial services, remind users to protect their personal data, and establish and improve the informed consent and authorization system for the use of data in the cross-border flow of users' personal financial data. [39] In addition, it can learn from the relevant rules of the European Union and the United States on the cross-border flow of personal financial data, clarify that commercial institutions should take security measures in the cross-border flow of financial data, and establish a responsibility investigation mechanism with the main country of financial data generation as the core. [40] The EU-US Data Protection Framework requires: providing free and convenient dispute resolution (individuals can complain directly to the industry, and participants must respond to individuals within 45 days); providing individuals with an independent recourse mechanism free of charge, through which everyone's complaints and disputes can be investigated and quickly resolved. This independent recourse mechanism needs to be established before entering the organization's self-certification. [41] Where there is a dispute, appeals may be made. Recourse available to individuals must be readily available and free of charge to individuals, as required by the principles of recourse, enforcement and liability. Independent recourse mechanisms must publish an annual report providing summary statistics on their dispute resolution services. [42]

4.2.3. Balance of Power Conflict between Right Subject and Supervision Institution in Cross-Border Flow of Personal Financial Data

4.2.3.1 Clarify the Value and Power of the Supervisory Body

First of all, the importance of each value subject is sorted in sequence. The free flow of data, the protection of data property rights, the autonomy of data and the social control of data are difficult to take into account at the same time, and should be sorted. China's financial sector is strictly regulated by the state. From the perspective of the overall national security concept, based on the social public product attributes of financial data and the theory and practice of social control of data flow, the author believes that the legal mechanism system for the supervision of transnational financial data flow

should be constructed with national security as its core value and the international law position that the state enjoys sovereignty over financial data. [43] Secondly, it is clear about the exercise process of the right of the supervisory body to exercise its power. Pre-evaluation, in-process supervision, and post-event problem handling. France passed a law requiring due diligence not only on the activities of companies and their subsidiaries, but also on the activities of suppliers and subcontractors in the fields of human rights, health and safety and environmental risks. [44] The EU requires data processors to submit a compliance draft to the appropriate regulatory authorities to determine whether it provides "adequate and appropriate safeguards". The approved code of conduct must be capable of "mandatory monitoring of compliance with its provisions"; The supervisory body must prove that there is an appropriate level of expertise in compliance with the behavior, and then it will be recognized by the competent supervisory authority. [45]

4.2.3.2 Collaborative Governance within the Supervision Subject

The supervision mode of personal financial data cross-border flow in China is relatively simple, that is, the supervision mode based on the unified leadership of the government, which leads to a vacuum in both horizontal financial supervision departments and cross-industry departments or social subjects participating in collaborative governance. [46] Therefore, it is necessary to explore the greatest common denominator of financial data supervision across or across industries and build a collaborative governance mechanism. In addition, after the cross-border flow of financial data is over, personal financial data is on the data server of the receiving country, and domestic regulatory agencies are unable to do so. At this time, in addition to signing agreements with the receiving country, self-regulatory organizations such as financial industry associations can jointly regulate the behavior of personal financial data processors in the cross-border flow of data.

In terms of internal governance, the specific rules can be macroscopically prudently supervised by the people's Bank of China, and the State Financial Supervision and Administration is responsible for the micro-supervision of personal financial data. First of all, the overall supervision of the cross-border flow of personal financial data is carried out by the State Financial Supervision and Administration, including the balanced positioning of financial value, the detailed supervision of the implementation of industry rules for the cross-border flow of personal financial data, the supervision of various industry organizations, and the coordination between domestic and foreign organizations in the event of rights conflicts between China and foreign countries in the cross-border flow of financial data. Deal with various financial conflicts and imbalances. Secondly, the State Administration of Financial Supervision and Administration should promote the cross-industry and inter-departmental interconnection of financial data and strengthen the ability of cross-departmental and cross-business coordination with the State Internet Information Office and the State data Bureau. [47]

4.2.3.3 Punishment of Supervisory Bodies

In order to prevent the abuse of supervisory power and give certain relief to the injured party after the abuse of power by the financial supervision department, it is necessary to punish the supervisory agency when it infringes on the right of personal financial data. For example, the EU's approach is that when there is a problem with a supervisory body and the relevant supervisory restraint mechanism is violated, the legally mandated checks and balances body should "take appropriate action," including suspending the infringing party or excluding the infringing party from the code. According to Article 83 (4) (c) of the EU General Data Protection Regulation, when the controller or processor violates the code of conduct, the recognized supervisory institution faces a maximum fine of 10 million euros for failing to "take appropriate action". Therefore, while providing relief to the infringed subject, China should not neglect the punishment of the supervision institution for the cross-border flow of financial data, and restrict the exercise of its power from this aspect.

5. Conclusion

To sum up, there are many conflicts and imbalances in the cross-border flow of personal financial data due to the different positioning of interests. It is a systematic new project to check and balance all parties in order to maintain financial security and economic efficiency. It requires the joint efforts of regulatory subjects, data processing subjects and individuals, sound legal protection, strengthening the sense of responsibility and self-protection in order to better deal with international cooperation and exchanges. In the process of future development, we should continue to pay attention to the trends and changes of the cross-border flow of personal financial data, and constantly improve relevant measures and strategies to ensure the security and integrity of personal financial data. Contribute to the construction of a more secure and harmonious data era. At the same time, in the context of the development of new quality productivity, we also need to pay attention to the promotion of regulation and cooperation through technological innovation. For example, through the establishment of intelligent monitoring and early warning systems, we can monitor the cross-border flow of data in real time, identify potential security threats in a timely manner, apply science and technology to data desensitization and anonymization, reduce the risk of personal information disclosure, and so on. In a word, under the condition of defining the basic value goal of our country and coordinating the conflict relationship, we should also pay attention to the development of our independent artificial intelligence, science and technology to promote the development of cooperation and the construction of international economic integration.

References

[1] National Data Bureau of China, "Three-year Action Plan of" Data Elements× "(2024-2026) (Draft for Comment), 2024, chapter 8.

[2] Financial Standards Committee, "Technical Specification for the Protection of personal Financial Information", 2020: "personal financial information is an important basic data accumulated by financial institutions in the process of providing financial products and services".

[3] Financial Standards Committee, “Technical Specification for the Protection of personal Financial Information”, 2020, Article 3.2: "Financial institutions obtain, process and preserve personal information through the provision of financial products and services or other channels".

[4] Id.

[5] Financial Standards Committee, Technical Specifications for the Protection of Personal Financial Information, 2020, Article 4.1.

[6] See Sun Dengke, “Research on the Legal Application of Cross-border Protection of Personal Data”, Liaoning University Press Co., LTD., 1st edition, November, pp.48, 2020.

[7] Financial Standards Committee, “Technical Specification for the Protection of personal Financial Information”, 2020, Article 3.4.

[8] The People's Bank of China, “The Measures for the Protection of the Rights and Interests of Financial Consumers of the People's Bank of China” a, 2020, Article 2.

[9] The EU, “General Data Protection Regulation”, 2018, Article 4 (7) .

[10] This term is used in “ the Personal Information Protection Law of China”, 2021.

[11] Financial Standards Committee, “the Technical Specification for Personal Financial Information Protection”, 2020, Article 3.5: "An institution that has the right to decide the purpose and method of personal financial information processing".

[12] China Information Security Standardization Technical Committee, “the Information Security Technology Personal Information Security Standard”, 2020, Article 3.4 : "Organizations or individuals who have the ability to decide the purpose and manner of personal information processing", as well as the express consent of Article 3.6, the authorized consent of Article 3.7, and the requirements for personal information controllers.

[13] Bodil Linqvist, Case-101/01 [2003] ECR I-12971.

[14] See Li Dong, “Research on Legal Regulation of Cross-border Flow of Personal Financial Data”, Master thesis of Shanghai Jiaotong University, 2018.

[15] Financial Standards Committee, “the Technical Specification for the Protection of Personal Financial Information”, 2020, Article 7.1.3(d) stipulates that four conditions need to be met: compliance, consent, exit assessment, and clear security conditions abroad. For security assessment, Article 4 of the Measures for the Security Assessment of Data Exit stipulates the situation that general data needs security assessment.

[16] See Guo Ziyi, "Regulation of Cross-Border flow of Financial data from the Perspective of National Security", seeking Truth from Facts, vol.3: pp.62 ,60-66, 2021.

[17] See Fan Sibo, "Research on the Governance of the Cross-Border flow of personal Financial data", Journal of Chongqing University (Social Science Edition): vol.12, pp.12,1-17.

[18] See National Internet information office of China, “the Draft Measures for Security Assessment of the Transfer of Personal Information and Important Data Abroad”, 2017, Articles 3, 7 and 8.

[19] See National Internet information office of China of the Measures, “the Assessment of Exit Safety of Personal Information and Important Data”, 2017, Articles 3, 4, 5, 7, 8 and 11.

[20] See Ren Longlong, “On consent is not the legitimate basis of financial data processing”, in Politics and Law, vol.1, 2016.

[21] See Wang Yuan, “The Trend of Personal Information Protection from the Perspective of Data Power-Centering on the Separation of Personal Information Protection and Privacy”, Journal of Beihang University (Social Science Edition), vol.1, pp.52,45-57, 2022.

[22] See Financial Standards Committee, “Technical Specification for the Protection of personal Financial Information”, Article 7.1.3.

[23] See Wu Jiangyu, "Construction of Legal Framework for Financial Data Regulation in the Context of Fintech," in Southwest Finance, vol.11, pp. 80,76-85,2020.

[24] See Han Long, “Frontier Issues in International Financial Law”, Tsinghua University Press, pp. 54, 2010.

[25] See the Cyberspace Administration of China, Measures for the Assessment of Data Exit Safety: "When providing data abroad, the data processor shall report the data exit safety assessment to the national network information department through the local provincial network information department", 2022, Article 4.

[26] The EU, “General Data Protection Regulation”, 2018, Article 32.

[27] Id.

[28] “U.S.-Korea Free Trade Agreement”, 2017, annex 13,section B of Murray B.

[29] “Euro-Korean Free Trade Agreement”, 2009, Article 7.43.

[30] “United States-Mexico-Canada Agreement: Article 19”, paragraph 11.

[31] “EU-U.S. Data Privacy Framework”, 2023, Article 1.1.

[32] Id.

[33] APEC Cross-Border Privacy Rules System Program Requirements, 35 a). Question 35.c).

[34] The EU, “General data Protection Regulations”, 2018, Article 1, paragraph 1.

[35] APEC Privacy Framework, Description at https://www. apec. org/Publications/2017/08/APEC-Privacy-Framework(2015) which states that the APEC Privacy Framework “aims at promoting electronic commerce throughout the Asia Pacific region, is consistent with the core values of the OECD’s Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data (OECD Guidelines), and reaffirms the value of privacy to individuals and to the information society.

[36] Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd (2001) 208 CLR 1999, and Grosse v Purvis (2003) QDC 751, Grosse v Purvis (2003) QDC 751.

[37] TRUSTe APEC CBPR Program Requirements Map, page 41 at http://www. cbprs.org/GeneralPages/ APECCBPR System Documents.aspx.

[38] Judgment of the Court of Justice of the EU of 6 October 2015 in Case C-362/14, Maximillian Schrems v Data Protection Commissioner, points 73, 74 and 96.

[39] See Zhang Jiuzhen: Research on the Self-discipline Mechanism of Network Information Dissemination, Bibliographic Literature Publishing House, pp.35, 2005.

[40] See Guo Ziyi: “Regulation of cross-border flow of financial data from the perspective of national security”, Seeking Truth from Facts, vol.03, pp. 63, 60-66, 2021.

[41] “EU-U.S. Data Privacy Framework”, 2023, Articles 1.1 and 3.3.

[42] “EU-US Framework for Protecting Cross-Border Data Flows”: 1.3.11(a)-(c): Individuals should be encouraged to raise any complaints they may have with the organization before resorting to an independent complaints mechanism. This can take different forms, but must meet the requirements of the principles on recourse, enforcement, and liability. An organization meets the requirements by: (i) complying with a privacy program developed by the private sector that incorporates the principles into its rules and includes an effective enforcement mechanism of the type described in the principles on recourse, enforcement, and liability; (ii) complying with a legal or regulatory supervisory body that provides for the handling of individual complaints and dispute

resolution; or (iii) committing to cooperate with a DPA or its authorized representative located in the EU.

[43] See Guo Zi, “Regulation of cross-border flow of financial data from the perspective of national security”. Seeking truth from facts, vol.03, pp. 63,60-66, 2021.

[44] See Constance Z. Wagner, “Evolving Norms of Corporate Social Responsibility: Lessons Learned from the European Union Directive on NonFinancial Reporting”, 19 TENN. J. BUS. L. 619, 669 ,2018.

[45] Article 41 (2) of the EU General Data Protection Regulation: In order to be recognized, the institution must show: (a) to prove its "independence and expertise in the subject matter of the code to the satisfaction of the competent supervisory authority"; (b) "Procedures have been established to enable it to assess the qualifications of relevant controllers and handlers in applying the Code, monitor their compliance with the Code and regularly review their operation"; (c) "Procedures and structures have been established to handle complaints about violations of the Code, or the manner in which the Code has been or is being implemented by the controller or processor, and these procedures and structures are transparent to the data subjects and the public"; And (d) "to prove to the competent supervisory authority that its tasks and responsibilities will not lead to conflicts of interest".

[46] See Zheng Dinghao, “On the Collaborative Governance of Financial Data in China”, Economist, ,vol.12, no.12, pp.76-85, 2022.

[47] See You Yiting, “The dilemma of regulating the cross-border flow of personal financial data and China's countermeasures”, Yantai University, 2023.

[48] René M. Stulz, Rethinking risk management, pp.1-22, 1996.

[49] Andrew W. Lo, “The Adaptive Markets Hypothesis: Market Efficiency from an Evolutionary Perspective”, pp.1-31, 2004.

[50] W. Gregory Voss, “Cross-Border Data Flows, the GDPR, and Data Governance”, Washington International Law Journal, vol.29, no.3, pp.485-532 ,2020.

[51] Donald MacKenzie, Yuval Millo, constructing a Market, Performing Theory: The Historical Sociology of a Financial Derivatives Exchange, American Journal of Sociology, Vol. 109, No.1, pp.107–145, 2003.

[52] Office of Privacy and Open Government, SAFEGUARDING INFORMATION, Arrival at: https://www. osec.doc. gov/ opog / privacy/PII_BII.html, 2021.

[53] Andrew W. Lo, The Adaptive Markets Hypothesis: Market Efficiency from an Evolutionary Perspective, pp.1-31, 2004.

[54] W. Gregory Voss, “Cross-Border Data Flows, the GDPR, and Data Governance”, Washington International Law Journal, vol.29, no.3, 485-532, Available at: https://digitalcommons. law. uw. edu/ wilj/vol29/iss3/7, 2020.

[55] Donald MacKenzie, Yuval Millo, “Constructing a Market, Performing Theory: The Historical Sociology of a Financial Derivatives Exchange”, American Journal of Sociology, Vol.109, No.1, pp.107–145,2003.

[56] Shao Xun. “Debate on liberalization and localization of cross-border data flow regulation”, Series on Politics and Law, vol.5, pp.139-148, 2023.

[57] Yin Fei, Li Dong, “On the adaptive construction of data-carrying right in China”, Journal of Guizhou normal University (Social Science Edition), vol.5, pp.103-113, 2023.

[58] Wang Ting, “Current situation and countermeasures of cross-border financial data flow mechanism in China”, Foreign Trade and Economic Cooperation, vol.11, pp.74-77+105, 2022.

[59] Guo Dexiang, Li Xiaoyu, “Legal protection of cross-border flow of personal financial data in China”, Journal of henan university of economics and law, vol.37, no.06, pp.80-88, 2022.

[60] Zhuo Zihan, Wang Yinan, Quan Wanqing, etc, “The promotion and regulation path of cross-border flow of personal financial information in China”, Information Security Research, vol.8, no.09, pp.931-938, 2022.

[61] Pendray, Zhang Zilin, “Research on the risk and regulation of cross-border flow of financial data in the digital age”, International Business Research, vo.13, no.1, pp.14-25, 2022.

[62] Lin Jie, Tian Chen, “Research on the regulation of cross-border flow of personal financial data [J]. Journal of Shanghai University (Social Science Edition)”, vol.38, no.06, pp.95-107, 2021.

[63] Luo Wenhua, “Procedural and substantive supervision of cross-border data flow based on life cycle”, Journal of China University of Political Science and Law, vol.05, pp.142-154, 2021.

[64] Huang Xianqing, “Construction Path of Supervision Rules for Cross-border Flow of Data in China under the Background of Digital Trade “, Southwest Finance, vol.08, pp.74-84,2021.

[65] Li Mengyu, “Characteristics and Enlightenment of Data Governance in International Financial Industry”, Tsinghua Financial Review, 2021(05):35-38.

[66] Tian Xiangyu, “Special Regulation of Cross-border Flow of Financial Data”, Hainan Finance, vol.04, pp.51-58+87, 2021.

[67] Chen Zhi, “The practice of cross-border data flow in Asian countries and its enlightenment to China”, Beijing Financial Review, v01):55-61.

[68] Ma Lan, “The Core Issues of Cross-border Flow Regulation of Financial Data and China's Response”, International Law Studies, vol.3, pp.82-101, 2020.

[69] Wang Yuanzh, “Legal regulation of cross-border flow of financial data of banks in China”, Research on financial supervision, vol.1, pp.51-65, 2020.

[70] Li Wei, “Thoughts and Suggestions on the Construction of Cross-border Flow Rules of Financial Data in China”, China Banking, vol.1, pp.41-44, 2020.

[71] Liu Shaoxin, “Cross-border flow of personal data under the background of globalization”, China Finance, vol.23, pp.68-70, 2019.

[72] Zhang Jihong, “Legal Protection of Financial Information in the Age of Big Data”, Law Press, 1st Edition, September, 2019.

[73] Huang Chunlin, "Internet and Data Legal Practice - Legal Application and Compliance Implementation", People's Court Press, 1st edition, December 2019.

[74] Yao Xu, "EU Cross-Border Data Flow Governance: Balancing Free Flow and Regulatory Protection", Shanghai People's Publishing House, 1st edition, December 2019.

[75] Li Yi, Zhang Juan, "Research on the Legal Protection System of Private Information under Big Data", Jilin University Press, 1st edition, January 2019.

[76] Chi Jianxin, International Comparative Study of Personal Information Protection Policies, Southeast University Press, 2nd edition, January 2022.

[77] Zhang Ning, Research on the Construction of Personal Information Protection System in the Big Data Era, Economic Science Press, 1st edition, October 2021.

[78] Sun Dengke, "Research on the Legal Application of Cross-border Protection of Personal Data", Liaoning University Press Co., Ltd., 1st edition, November 2020.

[79] Liu Xinyu, Data Protection Compliance Guidelines and Rules Analysis, China Legal Publishing House, 1st edition, August 2020.

[80] Liu Hong, "Research on Data Protection Law in the Big Data Era", China University of Political Science and Law Press, 1st edition, October 2018.

[81] Huang Zhixiong, The Legal Logic of Data Governance, Wuhan University Press, 1st edition, December 2021.