Research on the Protection of Personal Data Rights——From the perspective of the application of privacy computing technology

Shi Yun
Southwest University of Science and Technology, Mianyang, China.
yun.shi.chn@outlook.com

Abstract. With the development of marketization of data elements, privacy computing arises at the right moment in order to solve the contradiction between data circulation and its security risks. It is widely used in financial market, medical service, government management and other scenarios. It provides a new way for the identification of personal data rights, subject self-determination, safe circulation and corporate compliance, but also brings new challenges. From the perspective of the path and application scenarios of the key technologies of privacy computing technology, we can find the problems of personal data protection put forward by the current technology; privacy computing technology still has security risks in the process of data processing, and its industrial business model limits the benefits of individuals to their own data. Meanwhile, laws and regulations related to this technology also need to be refined and implemented. In order to solve these problems, it is necessary to promote the optimization of key technologies and the formulation of standards, build self-discipline rules and associations of the industry, strengthen legislation and special supervision of personal data, and build a global governance framework for the protection of personal data rights in privacy computing. It can enhance the use value of data, promote the integration of data resources and international circulation and sharing under the condition that the rights of personal data are fully protected.

Keywords: personal data rights; privacy computing technology; personal information protection law; optimal path.

1. Definition of Privacy Computing Technology

1.1 Privacy Computing Technology Concept

Privacy computing, also known as privacy computing technology and privacy-preserving computing, is a series of information technologies that cross and integrate multiple fields to provide data open security. According to Tencent's White Paper on Privacy Computing, privacy computing is a technology and system in which two or more participants collaborate to conduct joint machine learning and joint analysis of their data without disclosing their own data. Yan Shu and other Chinese scholars also pointed out that privacy computing refers to a kind of information technology that realizes data analysis and calculation on the premise of protecting the data itself from disclosure, including the cross fusion of data science, cryptography, artificial intelligence and many other technical systems.

1.2 Overview of Privacy Computing Technology

Articles 8 and 27 of the Data Security Law require that data processing activities shall perform data security protection obligations, and take corresponding technical measures and other necessary measures to ensure data security. The technical route of data security protection mainly includes multi-party secure computing, trusted execution environment and federated learning, which are important branch technologies of these three privacy computing.

1.2.1. Multi-party secure computing technology based on cryptography

Secure Multi-party Computation refers to the fact that each data participant performs the agreed collaborative computation together without sharing their own data and without a trusted third party.
After encrypting or transforming the data, the participants can only obtain their own calculation results through computing tasks, and cannot obtain or speculate the input data of either party, so as to maintain the concealing and controllability of the data of the participants. After nearly 40-year development, the technology has made great progress and been widely used. For example, Ant Group released its own secure multi-party computation platform, Tencent released its "Shield Sandbox" and Google's open source "Private Join and Compute" database in 2019.

1.2.2. Trusted execution environment based on trusted hardware

The concept of the trusted execution environment (TEE) from Open Mobile Terminal Platform (OMTP). The technology constructs a security space independent of the operating system, so that the calculation and flow of data can be carried out in a certain secure environment. Trusted execution environment is applied to each participant node, which can effectively solve the problem of privacy disclosure caused by the attack of the machine in the node, and ensure the security of data in the process of model execution. In recent years, Intel has released SGX, Ant Group has released Hyper Enclave, and ARM has released CAA confidential computing institution. The realization of these confidential computing institutions depends on the hardware and software implementation of TEE.

1.2.3. Federated Learning revolutionizes machine learning paradigms

Federated Learning is proposed by Google. It generates a general neural network model with a central server, trains the model with the help of several local servers participating in the training and continuously updates the network content to optimize the model until it reaches the established standard. Since the data of each participant is always saved on the local server during the iterative optimization of the model, the risk of data leakage is greatly reduced. Federated learning manufacturers at home and abroad mainly include Google, WeBank, Ant Group and BaseBit.

1.3 Specific Applications of Privacy Computing Technology

1.3.1. Market application

The rising demand for data collaboration has propelled privacy computing technology to become an infrastructure technology in the market. In the financial field, privacy computing technology enables financial institutions to innovate their business while ensuring data security, and promotes financial institutions to reduce costs and increase efficiency. Taking WeDPR of WeBank as an example, the platform uses technologies such as secure multi-party computing to ensure the security of data of various financial institutions. In the process of financial data query, the query party uses secure multi-party computing to hide the key words or customer information of the queried object, but the data provider cannot get the specific corresponding query object when matching the query result, which effectively realizes the protection and control of data privacy in Internet financial business.

Privacy computing technology will also help to change the way marketing. It can not only promote enterprises to use technologies that comply with data security-related regulations, but also upgrade existing marketing models to establish a good marketing ecological environment. For example, Tianmian uses federated learning to jointly model user data, complete its learning and analysis without the data being stored in the database, and provide customized services according to consumers' consumption preferences, purchasing ability and other personal information, while fully protecting individual data security.

1.3.2. Medical services

In recent years, with the deepening of medical informatization, intelligent medical care based on big data has become possible. However, because medical data is often related to the safety of people's lives and properties, and requires a strong security guarantee, it is difficult to fully realize the value of the data.

User data in the medical industry is of high value. Through the analysis of patient case parameters, it is helpful for medical institutions to supervise the health of patients, and to treat and
prevent diseases; Joint analysis of medical visit data, payment data and financial credit can reduce medical fraud and adjust situation of drug prices and supply. At present, XDP of BaseBit has built an "open platform for health and medical big data application" in Xiamen based on privacy computing technologies such as federated learning and secure multi-party computing, creating a relatively complete medical data ecosystem. Personal data held by various medical institutions can safely participate in the training of diagnosis and treatment models, and data providers, data service providers and third parties are expected to fully use the value of medical data.

1.3.3. Administrative management

Article 42 of the Data Security Law proposes to build a unified, standardized, interconnected, safe and controllable government data open platform. Meanwhile, the application of privacy computing is conducive to promoting the interaction and circulation of data in various government departments, realizing the full release of the huge value of government data. Privacy computing technology enables the government to better mine and analyze data resources and improve governance capacity and social service level. As highly sensitive data, government data resources have great potential value and are one of the data most likely to be attacked. Because of the sensitivity, the phenomenon of isolated government data island is more serious. Whether it is the large and small population census in Germany, the proposal of the United States to establish a national data center, or the housing base case in Japan, all reveal the hidden worries about the collection and processing of personal data by the government all over the world. The PrivPy multi-party computing platform developed by Hua Kong Tsingjiao uses federated learning to update the model in the data security environment. The use of secure multi-party computing technology enables more accurate analysis of government data without appearing in plaintext, which greatly improves the security of personal data in administrative management. At the same time, it can conduct joint modeling of enterprise tax information, enterprise violation information supervision and risk assessment, which helps the government to manage the enterprise and the development on the enterprise affairs of government, and improve the efficiency of government services.

2. Analysis of Personal Data Rights in the Application of Privacy Computing Technology from the Perspective of the Rule of Law

2.1 Clearly identify the data ownership

From Article 110 of the Civil Code stipulates that "the personal information of natural persons is protected by law", Article 21 of the Data Security Law puts forward the data management system of "data hierarchical classification protection", and then to the separate legislation of personal information protection in the Personal Information Protection Law, the legal provisions on the protection of personal data are becoming more and more detailed and comprehensive. However, the problem of data ownership confirmation caused by the complexity of data application and the diversity of data analysis and mining has not been answered.

Based on the rise of privacy computing under this background, it provides new ideas for solving the problem of personal data ownership identification——Taking the selective disclosure of WeDPR as an example, in the past, in order to obtain a certain type of certification from the relevant department, an individual needed to prepare a series of certification materials bundled for unified certification, and completed more complicated procedures. WeDPR provides a solution to minimize the disclosure of authentication data. After an individual is authenticated once, all information disclosures can selectively submit required data proofs, instead of displaying specific data or all data. When an individual proves that he has certain attributes, he guarantees that the data of that attribute is not disclosed, which fully respects the data subject's ownership of personal data, and this method obviously limits the data controller or processor's access to personal data and processing. It makes the acquisition and use of each personal data subject to personal authorization. In this way, personal data rights can be truly controlled by individuals.
2.2 Highlight the value of data subjects

In order to avoid the negative impact of incomplete and inaccurate data on individual rights, the data controller or data processor may, in accordance with Article 46 of the Personal Information Protection Law, request the relevant party to suspend the use, verify and correct the use of personal data if the right subject of the data thinks the accuracy of the data is doubtful. However, WeDPR selective authentication disclosure limits the input of personal privacy data and cuts off data sources at the initial stage, thus reducing or eliminating the possibility of improper use and tampering of data, based on the greater autonomy of users. Users may correct, supplement or terminate authorized use of personal data without notice to relevant parties. At the same time, WeDPR's selective authentication disclosure solution is quite different from the traditional authentication mode. It is proved by the individual's independent choice of the disclosure data attribute, and fully abides by the personalized choice of the individual data subject, which shows the individual's self-determination as the right subject to a greater extent. Both the Civil Code and the Personal Information Protection Law highlight the core position of individuals in information protection. In the scheme based on privacy computing technology, the absolute right of individuals to data has been greatly respected. It can also be predicted that the application prospect of "people-oriented" privacy computing technology is wide.

Article 20 of General Data Protection Regulation (GDPR) of EU proposes the concept of “right to data portability”. It is stipulated that the data subject has the right to obtain specific personal data from the data controller, and has the right to request the transmission of his personal data to other data controllers, so that the data subject can obtain the ability to transfer and circulate data. Article 45 of the Personal Information Protection Law also requires personal information processors to provide individuals with a transfer path for personal information. Referring to the concept and practice of MyData Project in Korea, users can control their own information and data through the App of MyData, and actively apply the information to a series of processes of personal life such as credit management, asset management and health management, so as to fully guarantee the personal right to data portability. In addition, privacy computing can provide relatively complete value protection for the liquidity of data. For example, associating personal information with a super account. A super account for personal digital asset can be set up by privacy computing. The transaction and circulation of personal data can be realized through pricing and privacy processing, and data rating, valuation and pricing in the financial sense can be also realized, which makes the establishment of data trading market feasible and fully releases the property value of data in circulation and interaction. Data subjects have the right to gain profits and dispose of their data in circulation.

2.3 Promote the safe flow of data

Regarding the collection and use of personal data, existing laws provide a large number of restrictive and binding provisions, but also clarify the circumstances or reasons for exceptions. For example, the proviso to Article 1038 of the Civil Code and Article 42 of the Cybersecurity Law: “Except for those that cannot be identified through processing and cannot be recovered.” In other words, personal data that has been processed and cannot be identified by a particular individual and cannot be recovered can be shared with third parties without the individual's consent. Technically, privacy computing can cut off the connection between data use and original data subjects, providing a data security solution that fully mines the value of data on the premise of protecting personal data.

At the same time, the development of privacy computing and the combination of privacy computing and related technologies provide a solid practical foundation for data transnational flow. The application of privacy computing will bring considerable changes to the cross-border flow of personal information: If an enterprise in one country needs to use personal information held in another country, it can directly perform cloud computing processing in the country where the data is held through privacy computing. The original data and personal information contained in the data will no longer be transferred, and only the calculation results will be transferred during the cross-border process. In addition, the data is encrypted throughout the calculation process, and the security
performance of personal information is effectively guaranteed; the calculation process reduces the intervention of manual and third party and greatly improves the processing efficiency. Private, public and national interests can be balanced to a certain extent through technology, where results can be executed without access to the data, where the value of use can flow internationally wherever it is stored.

2.4 Guide data usage compliance

Article 51 of the Personal Information Protection Law requires that personal information processors shall take corresponding security technical measures such as encryption and de-expression of personal information according to the purpose and method of processing personal information, etc. Privacy computing is a type of security technology measures. Privacy computing can hide plaintext data from the source and prevent the leakage of additional data while using data. To a certain extent, it solves the problem of data acquisition, copying, and tampering during the transaction process, and reduces the compliance burden in enterprise data transactions. When personal information processors need to self-certify compliance, technologies such as privacy computing are expected to be used as evidence for fulfilling information security protection obligations to help enterprises reduce the risk of violations.

In 2012, China's first national personal data protection standard, Information Security Technology - Guideline for Personal Information Protection within Information System for Public and Commercial Services, put forward 8 personal information protection principles: public disclosure, clear purpose, personal consent, minimum sufficient, security guarantee, quality assurance, good faith performance and clear responsibility. The Personal Information Protection Law also emphasizes that personal information should be handled in a lawful, proper and honest manner. Collection of personal information shall be limited to clear and reasonable purposes, disclosure of processing rules, information quality assurance, information security, etc. Privacy computing transmits data in encrypted form to ensure that participants cannot obtain additional information during the entire computing process, and it is difficult to reverse the original data. Through this technology, privacy computing can only collect and use personal information within the minimum scope, and practice the principle of minimization of data processing, so that the purpose of personal information use is clear, the process is reasonable, and the quality is safe.

3. Challenges Brought by Privacy Computing Technology to the Protection of Personal Data Rights

3.1 The Data Processing Process Hides the Risk of Data Exposure

The paragraph 2 of Article 3 of the Data Security Law stipulates: “Data processing, including data collection, storage, use, processing, transmission, provision, disclosure, etc.”. Privacy computing is a computing theory and method that covers the whole life cycle of data and provides data protection, involving every stage of data processing. Therefore, in the early stage of the development of privacy computing, while involving more and more comprehensive data, it also allows more different network environments, system equipment and personnel to enter the life cycle of data. There will be more equipment or artificial exposure at each stage. The possibility of data leakage, tampering and misappropriation is greatly increased, which obviously will infringe on data ownership. Article 44 of the Personal Information Protection Law clarifies that individuals have the right to know and the right to restrict the processing of personal information. GDPR enumerates the information that should be included in the right to know personal data and the exercise of the right to restrict. However, the update of the model used in the study of privacy computing may expose the personalized characteristics of data information, which will be pushed back and intercepted by the illegal users. The stolen personal data will break away from the control of the subject of rights and be used for other purposes unconsciously by the subject of data. This has a great impact on the right to know and
the right to restrict processing of personal data subjects; the omissions or assumptions of the relevant personnel in the process of data processing will directly lead to the phenomenon of improper use or abuse of data, which is also a violation of the data subject's right to restrict processing rights.

Meanwhile, different privacy computing technologies have different security risks. For example, federated learning is time-consuming and labor-intensive for large neural network models to write basic models from the bottom, and there is a danger of being implanted by viruses; cryptographic algorithms such as secure multi-party computing are prone to test channel attacks and error injection attacks, and hardware usually encounters intrusive attacks. And any link in a system data leakage problem will lead to the loss of data protection effect. When data is illegally obtained, it means that the data is exposed. Even if data rights holders defend their rights through legal channels, it is difficult to guarantee that these data rights will not be infringed a second time.

3.2 Industrial Business Model Restricts Personal Income Distribution

The development of the privacy computing industry is still in its initial stage, and the formulation and implementation of relevant industry norms are still in process. Due to the huge dividends brought by privacy computing, companies may ignore data authorization, data modification and other compliance systems when seeking their own interests. The Personal Information Protection Law clearly stipulates the obligation to inform and the “consent-authorization” mechanism, which requires privacy computing companies to ensure users' freedom of choice. Users have the right to refuse or revoke the consent that has been given in the past, and can fully know and exercise the right to be forgotten.

However, the complexity of privacy computing technology itself and the existence of the "black box" phenomenon make it difficult for most users to recognize privacy computing technology. The subject of personal data does not have a strong sense of rights, let alone regard personal data as a factor of production that can gain benefits from it. In addition, the architecture design of privacy computing platform varies greatly among different enterprises, and the mechanism of profit distribution and transaction charges in the industry is still being explored. At the practical level, the commercialization mode still focuses on the ToB end. As the most important but weakest subject in the data life circle, it is difficult to effectively protect personal rights such as the right to modify data, the right to be forgotten, as well as data property rights such as the right to use data, and the right to profit from data property is often ignored.

3.3 Existing Legal Regulations Need to be Refined and Implemented

The legal system of data protection still needs improvement. First of all, although the Data Security Law and the Personal Information Protection Law have been issued, there are still insufficient concrete provisions that can be implemented and operated. There are still many controversies about specific scenarios such as data authentic rights and data market regulation. Existing laws and regulations are not enough to deal with various disputes arising in the era of big data. A series of supporting regulations are still needed to clarify the boundaries of data security in privacy computing, and to point out the direction for the security boundaries of the development of the data industry. Secondly, it is necessary to give data subjects certain means of information self-determination in privacy computing, so as to realize the protection and remedy of their own data rights, and to further refine the legal remedies and damage compensation standards when personal data rights are violated. Furthermore, under the framework of the Cybersecurity Law, the Data Security Law and the Personal Information Protection Law, our country also needs to speed up the legislation of the entire life cycle of data circulation, build a complete guarantee system for big data transactions, and safeguard the legitimate interests of the data rights subject in the data market. In particular, personal data rights require specialized and systematic laws to safeguard. If laws are not used to determine the ownership boundary of personal data rights, and legal governance means for data processing and transaction are absent, illegal transactions, abuse of personal data and other
phenomena will easily occur, and personal data subjects' personal rights and property rights will be violated.

Data protection regulation still needs to be strengthened. Different from the previous data rights infringement, under the background of the application of privacy computing technology, the invisibility of personal data rights infringement is better, and the subject of data collection is usually natural person, while the subjects of data processing and use are often large enterprises and governments. Therefore, the infringement of data rights is difficult to protect only by subject awareness and industry self-discipline. Strengthening data supervision is a top priority. In addition, the anonymization standards for personal data in our country are not unified, and there is a lack of corresponding regulatory authorities and technologies to supervise the storage, use, and circulation of data after cross-border. Therefore, the original “inform-consent” mode cannot be ignored.

4. Optimal Path to Protect Personal Data Rights in Privacy Computing Technology

4.1 Promote Key Technology Optimization and Standard Formulation

In the field of privacy computing, there is still great room for improvement in the development of various technologies, so there is no universally applicable international standard established at present. Such as privacy computing joint modeling and statistics are time-consuming, requiring the privacy computing industry to conduct secondary optimization of its performance through algorithm acceleration, coding acceleration and other emerging ways; for the performance and efficiency differences of privacy computing technologies, we should improve algorithm protocols and upgrade software and hardware facilities. At the same time, it can also strengthen the integration of various privacy computing branch technologies and the integration of privacy computing technology with other technologies, such as the integration with blockchain technology, which can not only ensure the credibility of data, but also return ownership and usage rights to users; it can also improve the audit supervision ability through blockchain technology to solve the problem of authentic data and pricing, which allows personal data subjects to enjoy benefits, so as to activate the vitality of the entire data market.

While optimizing computing power and performance, the development of privacy computing technology cannot ignore the information needs of individuals. Article 7 of Personal Information Protection Law requires data processors and users to maintain transparency in the processing and use of personal data in principle. And it is emphasized again in Articles 24 and 52 of the Law. In addition to requiring personal data processors to notify necessary matters in advance, disclose processing rules, and write reports regularly, it also requires that technical aspects should also be developed towards the main user side. Implementing relevant technologies in the exercise of individuals' rights to inquire, correct and delete data, makes data subjects fully understand and master the content, whereabouts and uses of their own data. It allows users to realize automatic security prediction, risk identification and reporting with the help of technical means, and avoid the black box of algorithms further deepened by technology upgrades.

At present, there are many branches of privacy computing technology development, and data processing methods are different. Therefore, domestic and foreign organizations such as IEEE, ISO, ITU-T, and China Communications Standards Association have begun to formulate or publish technical standards related to privacy computing based on frameworks and functions. Focusing on the development of key technologies and the construction of standard systems to improve the standardization capacity, computational efficiency, computational certainty and safety of products. Clear usage scenarios, frameworks and principles can also be fixed in the form of experience to guide the design, development, testing and use of relevant system models, so as to facilitate the formation and formulation of international standards for privacy computing technology. Only with clear technical specifications and unified data standards can upstream and downstream laws be linked.
On August 4, 2021, the International Telecommunication Union (ITU) released the first international standard Technical Framework for Shared Machine Learning System in the field of privacy computing technology. In the future, it is still necessary to formulate targeted standards based on the performance and security of different privacy computing products to promote the interconnection and classification of various industries and various branch technologies of privacy computing. Select authoritative and trusted data sources to carry out privacy computing trials, and gradually build an international big data trading platform.

### 4.2 Establish Self-discipline Rules and Association of Industry

Scholar Bennett divided personal data protection into five main implementation modes. From low intensity to high, enterprise self-discipline is the minimum requirement. The role of industry self-discipline is fully recognized worldwide. Article 19 of the OECD Guidelines states that member countries should encourage and support self-discipline mechanisms, whether in the form of codes of conduct or otherwise. The United States regards industry self-discipline as the core of personal data protection. By formulating industry privacy protection standards, it guides data controllers or processors to consciously abide by relevant rules in information exchange, and only pursue accountability on the basis of violating legal provisions.

At the level of personal data processing, Personal Information Protection Law not only clarifies the legality of personal information processing, but also establishes a series of obligations that personal information processors should abide by. For example, the principles of clear purpose, openness and transparency, integrity and accuracy, and security guarantee have established a reference basis for the self-discipline construction of the privacy computing industry. Some international organizations that our country has joined have also put forward new requirements for the processing of personal data. Article 8, paragraph 4, Chapter 12 of RCEP stipulates that: “Parties should encourage legal persons to publish their policies and procedures related to personal protection, including through the Internet”. It can be seen that the level of responsibility performance in the privacy computing industry is directly related to the degree of personal data protection. The privacy computing industry should first abide by professional ethics, practice social responsibility, strictly manage the behavior of employees and standardize business behavior. On the one hand, the management level should strictly follow industry standards, highlight risk prevention, strengthen internal control management, and maintain real-time monitoring of equipment and applications. On the other hand, barriers to entry for the privacy computing industry should continue to be strengthened. They should not only limit the quality and quantity of talents, so as to achieve reasonable supply and demand, but also strictly control the enterprise organization, so that it can meet the market recognition standards of the privacy computing industry. In terms of the transfer of personal data, China can refer to the BCR formulated by the EU to guide leading companies in the privacy computing industry to formulate internal regulations for the protection of personal data, help enterprises improve the formulation of their own privacy policies, and play a role of demonstration for the domestic industry. The main limitation of BCR is that it only applies internally to multinational companies. Therefore, China can also improve the BCR rules on the basis of reference, expand the scope of application of the self-discipline rules to international enterprises engaged in cross-border personal data business, and explore the interconnection of BCR between different enterprises.

Industry associations often act as bridges between the government and enterprises. The privacy computing industry association plays a significant role in privacy computing technology cooperation, market coordination, and restricting and ensuring the benign operation of public power. At the same time, it is able to establish and enforce rules, standards and open agreements between companies in the privacy computing industry. It can supervise the quality of products and services, competitive means and business style of the privacy computing industry in an all-round way, and promote the interconnection within the industry. In this regard, data supervision departments can urge industry associations to strengthen the formulation of industry norms and provide industry associations with services such as personal data protection consultation.
4.3 Strengthen Personal Data Legislation and Specialize Supervision

The Personal Information Protection Law and the Data Security Law have been promulgated successively, reflecting our country's emphasis and consideration of data rights protection. However, the current data legislation is obviously not enough to support the reasonable evolution of the big data era. Our country needs to further strengthen the legal protection of personal data and formulate specific operational norms that can be implemented. Specifically, it is suggested that the protection of individual data rights should be clarified first, so that the rights of data rights subjects can be effectively protected in the real and virtual world. At the same time, legislation can better keep up with the needs of the times. Among them, the most urgent task is to clarify the rights of data with respect to the person. On the one hand, the right to carry and modify data should be clarified. The use of data can be decided by individuals to ensure that personal data belongs to individuals. On the other hand, the right of data to be forgotten should be clarified. Data is an essential element of an individual’s digital personality. Data users need to delete some sensitive data according to the needs of personal data subjects, so as to better protect personal data rights.

As privacy computing data makes data processing more concealed, rapid and large-scale, it is difficult to fully realize the rights of data subjects, and personal data rights must be protected through the establishment of specialized agencies. The provision of specialized supervision on personal data protection is an important supplement to the self-discipline of enterprises and the industry, and also a general trend at the international level. For example, the BDSG of Germany sets up a Data Protection Commission to supervise the processing of personal data. France set up the National Commission for Information Processing and Protection of Freedom to co-ordinate government and social data processing. The CBPR rules are committed to building a personal data protection system from privacy enforcement agencies, accountability agencies, and companies engaged in cross-border transfers of personal information. At present, our country's telecommunications and Internet fields are mainly in charge of the Ministry of Industry and Information Technology; Consumers’ personal data is the responsibility of the State Administration for Market Regulation; The personal data of users in the financial industry and the medical industry are under the responsibility of the People’s Bank of China and the competent health authorities, respectively, and there is still a lack of special coordination and supervision agencies for data processing. Therefore, China should establish a special supervision department for the protection of personal data rights, coordinate the implementation of laws on the protection of personal data rights, and reduce the problem of data rights infringement caused by inadequate supervision.

In order to protect personal data in privacy computing applications, specialized agencies established in our country should perform the functions of supervision and inspection of personal data processing. First, it is necessary to supervise the use of data information in advance, and prevent behaviors that may damage the public’s data rights from the source. Because privacy computing is professional and technical, relevant supervisory staff need to have strong professional capabilities and certain research capabilities on data rights protection. Second, enterprises that have needs for the use and processing of personal data are required to register and record, and conduct irregular inspections of each enterprise to verify the use of personal data. Third, supervise the companies that have violated the rules found in the process of data use, and insist on greater punishment. In addition, cooperation with market supervision departments is also required, such as joint regulation, joint investigation and participatory litigation. On the basis of maintaining market order, it is actively implemented relevant laws and regulations on the protection of personal data rights. Fourth, connect with international personal data protection agencies to jointly build a personal data protection and flow cooperation mechanism.

In addition, there should be different regulatory priorities for different privacy computing technologies. In the federated learning mode, the number of model updates may reveal the personal characteristics of the data information. Therefore, it is necessary for the regulatory agency to strengthen the supervision of the decryption key business process in combination with technical standards and legal obligations. In a secure multi-party computing model, the processor may perform
other computing tasks with encrypted personal data without the subject's knowledge. Therefore, the focus of regulation should be placed on constraints on output. In the trusted computing model, regulators are also required to refine the security of the trusted execution environment and the obligatory provisions for data processing and data encryption synchronization. In particular, when the technology is involved in the processing of sensitive personal data, it requires technical standards that are higher than general data processing activities.

4.4 Build a Global Governance Framework for the Protection of Personal Data Rights in Privacy Computing

In the era of the digital economy, the collection, storage, use, and transmission of personal data have long transcended national and regional boundaries. As mentioned above, privacy computing will also have a profound impact on the global flow of personal data. In order to avoid the lack of effective connection between the development of privacy computing technology and the enactment of regulations and the formation of new "trade barriers", countries should have perspective, timely carry out cross-border technical coordination, establish a governance framework with international consensus, and avoid further fragmentation of data infrastructure and digital space.

The principles of regional personal data protection can provide instructive suggestions or opinions for the development of specific work to a certain extent, make up for the deficiencies caused by the lack of relevant rules, and better safeguard the rights of subjects. Therefore, countries should first promote domestic technology, supervision, rules and other institutional innovations, and then reach international and regional consensus on the conceptual scope of personal data rights and the processing principles of privacy computing. On the basis of consensus, regional and international organizations should play their leading role in promoting a global system of rules for the protection of cross-border transmission of personal information. Organizations should build bridges for cross-border protection and cooperation of personal information among member states in the region, eliminate shortsightedness and inequality caused by unilateral measures, and enhance the enthusiasm and awareness of in-depth cooperation and equal dialogue among member states in the region. This will lead to consistent rules of expectation and protection, ultimately relying on privacy computing technology, establishing global Internet infrastructure such as International Data Trading Centers, and securing global flow of personal data across multiple domains.

Article 11 of the Data Security Law of the People's Republic of China clearly states that: “The State actively carries out international exchanges and cooperation in the fields of data security governance, data development and utilization, participates in the formulation of international rules and standards related to data security, and promotes the safe and cross-border free flow of data.” Since the international rules for the protection of personal data have not yet been unified, China should actively participate in multilateral or bilateral negotiations on data security governance. On the premise of the principle of peer-to-peer and respecting the data sovereignty and interests of other countries, a unified cross-border data flow rule is established to form a mutually recognized data protection mechanism to achieve orderly and secure data flow. China can actively promote international rule-making on the basis of data governance rules under multilateral mechanisms established by the APEC, USMCA, the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), and the Regional Comprehensive Economic Partnership (RCEP). Proposing the "China’s plan" for global data security and flow under new technologies, and further establishing the "Data Fate Community", can promote the construction of a new pattern of global data governance.

5. Summary

In the era of big data, with the in-depth promotion of privacy computing applications and the continuous extension of information technology, it will inevitably lead to the security risks of data use and the dilemma of the exercise of related rights. However, many scenarios and application cases of privacy computing provide us with multiple ideas and ways to seek the protection of data subjects'
rights. On the basis of discussing the specific impact of privacy computing on data rights, this research analyzes the problems existing in the background of privacy computing, such as the risk of personal data exposure hidden in data processing, the restriction of business model on personal income distribution, and the existing legal regulations to be refined and implemented. Finally, it puts forward various countermeasures to improve the protection of data rights, including promoting the optimization of privacy computing technology and formulation of standards, establishing self-discipline rules and industry organizations for privacy computing, strengthening legislation and special supervision of personal data, and building a global governance framework for privacy computing technology on this basis.

At present, China's legal system on data is being improved in classification and distribution, privacy computing technology is developing rapidly, and its industrialization is also accelerating. Article 16 of the Data Security Law also stipulates: “The state supports data development and utilization and data security technology research. The state encourages technology promotion in the fields of data development and utilization and data security, encourages business innovation, and cultivates data development and utilization and data security products and industrial systems.” Privacy computing, in response, is bursting with new vigor in various fields. Looking into the future, enhancing the protection of personal data rights in the field of privacy computing technology is the inevitable choice to protect personal data rights in the era of digital economy, and it is also the realistic need for the government to improve data service capacity and urge enterprises to deal with personal data in accordance with the law and compliance. Moreover, it is also necessary to maximize the value of data use, realize the goal of becoming a cyber power in the new era, and enhance the international influence of China's data governance.

References


