Scientific Research Publishing

Open Journal of Social Sciences, 2023, 11, 533-550
https://www.scirp.org/journal/jss
ISSN Online: 2327-5960
ISSN Print: 2327-5952

The Failure and Response of Risk Prevention Regulations: Taking Privacy Computing as an Example

Xinhui Liu

School of Economic Law, Shanghai University of Politics and Law, Shanghai, China
Email: wabbmm0620@163.com

How to cite this paper: Liu, X. H. (2023). The Failure and Response of Risk Prevention Regulations: Taking Privacy Computing as an Example. *Open Journal of Social Sciences, 11,* 533-550.
https://doi.org/10.4236/jss.2023.1111035

Received: November 5, 2023
Accepted: November 27, 2023
Published: November 30, 2023

Copyright © 2023 by author(s) and Scientific Research Publishing Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).
http://creativecommons.org/licenses/by/4.0/

Open Access

Abstract

Against the backdrop of the continuous development of the data economy and the widespread application of algorithm technology, the protection of data security and privacy has increasingly become a concern for countries, society, enterprises, and individuals. As a new algorithm technology, privacy computing is known as the "optimal solution for data security and privacy protection" due to its "available and invisible" technical characteristics and wide applicability. However, the issue of immature privacy computing technology is becoming increasingly prominent, and the deep-seated contradiction between data utilization and data protection cannot be fundamentally resolved, which seriously restricts the practicality of privacy computing application scenarios. The risks faced by privacy computing not only have their own technological flaws, but also traditional risk prevention and regulation methods still have incompatibilities in addressing compliance issues in privacy computing. There are a series of risks such as unclear legal status of participating methods, high cost of algorithm interpretation, and inaccurate calculation results. Resolving these risks requires starting from the current development status of privacy computing. Targeted modifications and improvements should be made to the application difficulties of China's risk regulation methods for privacy computing, in order to explore the establishment of a data governance compliance system to solve algorithmic problems and promote the practicality of new algorithmic technologies represented by privacy computing.

Keywords

Privacy Computing, Data Security, Technical Compliance, China

1. Privacy Computing Development Status and Issues Raised

The Origins of Privacy Computing

In the era of digital economy, data, as a new production factor, plays a great value in the digital economy, such as artificial intelligence, big data, Internet of Things and other technologies. However, data leakage incidents have surged year after year, greatly affecting data utilization. Emphasizing data security has been a major trend in digital economy governance. At the same time, the contradictions and conflicts between data utilization and privacy protection have become more and more acute. For these reasons, the concept of privacy computing has emerged.

Privacy-Preserving Computing (PPC) technology, which appears as "enabling technology", has unique advantages in opening up application channels, breaking down industry barriers, and resolving information silos, and has become a technological high ground that countries all over the world are competing to pursue. Privacy Computing, also known as Privacy Enhancement Technology, is "a computational theory and methodology oriented to the full lifecycle protection of private information, and a computable model and axiomatic system for the complexity of privacy metrics, the cost of privacy breaches, and the complexity of privacy protection and privacy analytics in the context of the separation of ownership, management, and use of private information". Despite the broad application prospects, the potential risks of privacy computing should not be ignored. As an underlying technology deeply integrated with other AI technologies, privacy computing has the potential to subvert and reconfigure the application process of algorithms.

Privacy computing is a type of technical solution that can maintain data opacity, non leakage, and inability to be obtained by calculation methods and other unauthorized parties during the processing and analysis of computational data, achieving the "availability and invisibility" of data during use and circulation. Generally speaking, privacy computing cannot be simply attributed to a specific disciplinary field. It is actually an interdisciplinary fusion system that includes numerous technical fields such as security hardware, data science, artificial intelligence, etc. Privacy computing can achieve data security protection that is "available but not visible", effectively protecting personal identification, user privacy, enterprise operations, and other information during data circulation, providing effective technical means for data fusion applications and value release.

2. Analysis of the Legal Risks Presented by Privacy Computing

"Although there is a broad application prospect, the potential risks of privacy computing should not be ignored, as a deep integration with other artificial intelligence technology underlying technology, privacy computing has the potential to subvert the reconstruction of the algorithm application process." (Tang,

2021) From the technical level, each of the three directions of privacy computing has certain shortcomings, and the "old problem" of guaranteeing the technical purpose of data security is still not enough: the trusted execution environment needs to trust the hardware vendors, while the current computing and storage capacity is relatively limited; the security of federated learning has not been adequately researched, and generally still needs to be combined with encryption technology, and lacks independent and strict security. The security of federated learning has not been sufficiently studied, and generally still needs to be combined with cryptography, lacking independent and rigorous theoretical proof; cryptography has certain performance bottlenecks, and the threshold of use and understanding is high.

At the same time, on the legal level, as an algorithmic technology to regulate risks, privacy computing may also induce risks due to the factors of the technical means itself, creating "new compliance problems", and thus falling into the dilemma of "risk - regulation - secondary risk - re-regulation". That is to say, in response to the existing data problems in society, new algorithmic technologies have been spawned, and new models and application standards have been established, but the technology itself can also bring new social risks and conflicts, and the new problems call for new social risks and contradictions. However, the technology itself can also bring new social risks and contradictions, and new problems call for new technologies, thus cyclically falling into a governance circle, deviating from the original intention of protecting data security and maintaining data utilization and privacy protection. At the same time, due to the lack of mature technical standards, under the cover of technical "surface compliance", the legal risk is also correspondingly blurred, decentralized, and even difficult to identify. In fact, as long as the contradiction between data utilization and data security continues to exist, it is difficult to avoid the new compliance problems brought about by data technology itself.

2.1. Ambiguity in the Legal Status of Participants

The complexity of privacy computing technology itself makes its various participants different from general data use activities, including data providers (users), data processors, technology providers, and result users. In specific privacy computing application scenarios, there are also plural forms of the same type of participant, e.g., the construction of models in federated learning usually requires two or more data processors to provide integrated data collected by each of them. There is also cross-fertilization of participant identities, with data processors often providing algorithmic technology in certain scenarios; technology providers may also be entrusted with data processing and become data processors. Therefore, under the current legal framework, the legal relationship between participants in privacy computing is complicated by the diversity of specific practices, and the same participant's status in different legal relationships varies according to his or her identity, which often results in a conflict of rights

and obligations, making the corresponding responsibilities fall through the intersection of legal relationships.

It is difficult for traditional risk prevention and regulation methods to provide comprehensive coverage. In the author's opinion, it is undoubtedly an important proposition worth thinking about to deeply reflect on the inadequacy and causes of traditional risk regulation and how to amend it through new means and new ways to cope with the new risks and challenges brought by privacy computing.

2.2. High Cost of Algorithmic Interpretation

The "black box property" of privacy computing has resulted in its inherent characteristics of poor interpretability and high cost of interpretation, which is also a common problem faced by data compliance technology at present. On the one hand, as an interdisciplinary technology system integrating cryptography, artificial intelligence, and distributed systems, the technical threshold of privacy computing is relatively high, and it is difficult to understand the principles of privacy computing thoroughly without relevant technical background; on the other hand, ensuring that some assumptions set by the security foundation are valid is a prerequisite for realizing the algorithmic justice and data security requirements, for example, each data processor participating in multi-party computing truthfully complies with the requirements of the protocol, and there is no potential collusion. Thus, in application scenarios involving national interests, social public interests and personal privacy, forcing the disclosure of technical details in order to balance interests is not only difficult to realize, but also contrary to the original intent of the technology.

2.3. Inaccurate Operational Results

Privacy computing is not the same as data compliance, and the technology itself cannot address the legality of the data source. If the data processor obtains data without the user's authorization and consent, in the process of data fusion among multiple participants, the whole body will be affected, and the violation of one data source will "contaminate" the whole data group, which will not only fail to achieve the purpose of privacy computing compliance, but also may induce new data security risks. At the same time, the complexity of the relationship between the subjects involved in privacy computing increases the possibility of contamination of data sources. Discrete data violations are superimposed on each other in the "black box" environment, and small deviations are further amplified, resulting in even more erroneous results, and the data processed by privacy computing needs to meet the requirements of anonymization, which is a key requirement for privacy computing. Moreover, the data processed by privacy computing needs to meet the requirement of "anonymization", which does not allow the original data to be restored through reverse computation according to the technical purpose, so it is usually difficult to identify the source of contamination from the computation results, which also increases the computation

cost to a certain extent.

3. The Dilemma of Applying Traditional Risk Prevention Approaches from a Privacy Computing Perspective

He ethical foundation of the traditional approach to risk regulation rests on three major liberal ethical principles, namely Kant's principle of autonomy, Mill's principle of harm, and Locke's principle of the individual. Specifically, "relevant technological applications fall within the bounds of legality and legitimacy if they have been communicated in advance and agreed to by the parties involved, and if they do not cause explicit harm to individuals." However, in the new technological era, digital technology applications represented by big data and algorithms are massively complex, risky, and anonymous, such that the application of the above three major ethical principles of libertarianism faces dilemmas under the perspective of privacy computing.

3.1. Dilemmas in the Application of the Informed Consent Rule

First is Kant's principle of autonomy. According to Kant, every rational person has the capacity to use reason to take responsibility for actions autonomously. Because this is related to the moral dignity of the subject, he enjoys the right to make autonomous decisions. It is intended to build a "personal autonomy", respecting each person as an independent and autonomous individual who can decide to act or not to act in a way that affects his or her personal interests, and in fact, this spirit forms the basis of our social life, as typified by the principle of autonomy in civil law, the principle of autonomy. Natural persons, legal persons and other organizations influence the establishment, change and termination of civil legal relations according to their own subjective will, without external coercion and in an environment of voluntary equality.

A typical application of this principle is the rule of "informed consent", which means that every person has the right to be informed of the risks that may be associated with his or her own actions and to make choices of his or her own free will, with the key being that the other party should fulfill the obligation of informing the other party and obtaining the right holder's clear and specific consent. In the field of personal data protection, the architecture of informed consent can be understood as the decision of a natural person, as an information provider who has a stake in the benefits and risks associated with information processing activities, to consent to the relevant information use and circulation activities (Zhao, 2022). Therefore, the traditional risk governance approach only emphasizes the regulation of the "lack of knowledge" of the right holder, in other words, as long as the data processor has fulfilled the obligation to inform the risk of privacy calculations, it can be regarded as complying with the basic requirements of the informed consent rule. However, big data and algorithms and other auxiliary digital science and technology applications are extremely intelligent and ethically sensitive, and users are prone to form dependence, and their

personal emotions, thinking and even behavioral choices are swayed and influenced by the network group. Taking the filtering of the information cocoon as an example, in the environment of the digital society, intelligent algorithms have been able to more accurately and extensively control the behavior of human beings in transmitting and accepting information, and to a certain extent control the way human beings experience the way of the world, it can accurately filter out the user "want" information content, over time in the "cocoon" to form thinking inertia. The question is, therefore, whether relying on big data and algorithms to make decisions and choices is contrary to the autonomy of rational human beings?

In the author's view, big data and algorithmic processing have alienated the user's "consent" in the usual sense. Taking ChatGPT as an example, when we ask it whether the corresponding data processing is favorable, can we be regarded as making choices and decisions out of our own autonomy by relying on this kind of "smarter" artificial intelligence instead of or to help us make choices and decisions? Or is it possible to recognize the autonomy of algorithms as "human-like" or even "superhuman"? Based on the operational structure of AI, algorithms can learn and interact to acquire capabilities close to or even beyond those of humans. In fact, the function of filtering, optimizing, and synthesizing new data implies the essence of autonomous creation. Therefore, although it is an artificial product, it may not be able to be controlled and utilized by human beings, who are unable to precisely analyze and locate the direction of their choices and decisions. In the data era where algorithms are deeply embedded in human society, algorithms "control" people's communication, consumption, entertainment, and all kinds of decisions, big and small, and algorithms are gradually weakening human autonomy by integrating and intertwining with people's own autonomy with their human-like "autonomy", on the one hand making individuals dominated by capital, and on the other hand making individuals dominated by capital. On the one hand, algorithms make individuals the tools of capital's domination, and on the other hand, they make it difficult to recognize individual consciousness, thus reducing the possibility of redressing rights and preventing risks. Under the control of the dictatorship of capital, "the individual no longer reflects on himself, but is immersed in the gaze of an ever-increasing number of symbols of objects and in the energetic order of social status".

Further, the technical goal of privacy computing is to be "usable but invisible", which is inherently paradoxical as a black-box construction, and thus undermines the "informed" premise of user consent. In short, privacy computing is like a black box in which data processors, in order to protect the privacy of their data, do not need to see how the black box works in order to obtain the results of their calculations. On the other hand, the difficulty of understanding the data leads to the opacity of the algorithms, which manifests itself in the complexity of the data code and algorithmic structure, exacerbating the information asymmetry between human and machine models. Through the virtual common model

constructed by privacy computing, the algorithm can realize data optimization, processing and real-time feedback, but because of its black-box construction, the data processor can't guarantee its learning direction and the reasonableness of the result, not to mention the user who is in the position of even more asymmetric information, which is neither aware of the purpose and structure of the algorithmic model, nor can it understand the relevant information about the data processor, so naturally, it can't talk about "informed" and "uninformed". For the user who owns the data, it may be difficult to anticipate that allowing data processors to process and utilize the user's data will create potential data protection loopholes and corresponding risk issues; it is equally difficult to imagine that their original intention to protect the interests of the State and the public interest of society will be exploited, and that expanding the scope of data collection will exacerbate the misuse of data rights and the leakage of privacy.

In short, the problem of algorithmic discrimination based on data and algorithms, such as data profiling, information cocooning, and big data kills maturity, has become increasingly prominent. Under the manipulation of technology, algorithms are able to accurately filter out personalized push content and create tailored network environments, and this "cocooning" network structure leads to the homogenization of individual preferences, labeling, and the reliance of people on intelligent algorithms, as well as the reduction of the possibility of autonomy of access to new information, which makes it difficult for the application of the technology of privacy computing to meet the requirements of the principle of autonomy.

3.2. Lack of Legislation on the Concept of Group Privacy

The second is Lockean individualism. "Individualism" focuses on the real status of the individual, who is regarded as the logical starting point of society, the individual is the purpose of society, and all ideas are regarded as the product of the individual, denying the legitimacy of collective wisdom. For this reason, the legal interests protected by the law are mainly the rights and interests of the "individual", and group legal interests such as the national interest and the public interest are excluded from its scope of application.

The problem is that the data network breaks the physical space on which people have long depended for survival, and in the virtual world of data, "everyone is not an island". Big data technology is the product of individual data collection, its concern is not just a flesh and blood of individuals, but a large number of individuals composed of integrated data, a large number of individual data is connected to the algorithmic technology of the huge network of interests, more valuable data utilization is the whole system of the "network" rather than only the "point". It is the "net" of the whole system rather than just the "points" that has more value in the utilization of data. As a result, individuals are gradually blurred and appropriated in the group-based information environment, and the concept of group-based rights protection is becoming more and more

prominent. Thus, in the field of privacy computing, it is necessary to define the scope of the concept of "privacy" in order to clarify the scope of risk regulation and protection of legal interests.

The privacy of privacy computing is not the "right to privacy" in the usual sense as the basic human rights of individuals, but the right to ensure that the data held by the data processors are not disclosed in the process of data circulation and utilization, so as to ensure that the data processors are not infringed upon in their independent rights and interests in data. Traditionally, the right to privacy refers to the right of citizens to enjoy the peace of private life and private information to be protected by law from unlawful intrusion, knowledge, collection, utilization and disclosure by others. Obviously, this is defined from the standpoint of individual and human rights. Entering the digital era, the physical boundaries between people have been broken, and data and information have become the "oil" of great significance, and people's identity status, occupational habits, and life behaviors are all presented in the form of data and information. At the same time, a large amount of personal information is controlled and profited by technology companies and commercial platforms, which have "quasi-legislative" and "quasi-judicial" powers, and at the same time, for the sake of protecting public interests, government agencies also have the necessity to make use of the data and information in their possession. At the same time, for the protection of public interests, government departments also have the need to utilize the data and information in their possession. How to achieve a balance between data rights protection and data circulation and utilization? In the author's view, it may be possible to consider the definition of the subject of information privacy. If natural persons have privacy, do groups of people also have "privacy"? Do they also have the need for protection?

What is "group privacy" or "organizational privacy"? Luciano Floridi, Director of the Digital Ethics Laboratory at the University of Oxford, defines the concept as "the right to group privacy as a right enjoyed by the group itself, rather than by the members of the group individually." Thus, group privacy, as an abstract collective right, cannot be attributed to separate individuals within a group. This definition clearly distinguishes the right to privacy of individual natural persons from the right to privacy of a group, and in the process of transforming personal information privacy into group data privacy, its individualized privacy is dissolved, and the subject of risk-bearing is shifted from the individual to the group as a whole. In this way, it seems to be possible to say that groups of people have an abstract "personality right" in the matter of privacy. The legitimacy of protection is based on the fact that, on the one hand, abstracted data privacy has the same or similar attributes, and group protection is conducive to improving the efficiency of risk regulation and protection of rights and interests; on the other hand, new algorithmic technology gives additional value to the integrated data, and the group data privacy itself has the necessity of independent protection.

From an industrial and technological perspective, the private data held by data processors has both personality and property rights attributes, including not only individual privacy, but also the "organizational privacy" of enterprises and governments as data assets. In the case of the latter, it has already exceeded the purpose, applicable subjects and applicable scenarios of traditional privacy protection. In fact, the purpose of defining such group or organizational privacy in the context of privacy computing is to enable cross-border data flows under the premise of safeguarding data security and protecting data property rights. Comparatively speaking, privacy protection for individuals is a matter of compliance with personal information protection regulations, and from the perspective of privacy protection for cross-border data flows, privacy protection for organizations is a matter of protecting their own data property rights. If the problem of "privacy" protection cannot be solved, even if privacy computing can create huge profits, it is not practical in view of data security, and data processors are unwilling to take the risk of having no legal protection, and similarly there is no legal basis for governmental agencies to utilize massive amounts of data to protect the public interest.

However, the concept of group privacy is destined to be incompatible with the current construction of an individual-oriented system. From the viewpoint of China's legislation, Article 38 of the Constitution stipulates that citizens' personal rights shall be free from unlawful infringement and restriction, and Article 102 of the Civil Code stipulates that natural persons shall enjoy the right to privacy, and that no organization or individual shall infringe upon the privacy of others, which is clearly an individual-centered definition of the concept of privacy. In addition, according to the newly introduced Personal Information Protection Law, its legislative purpose is to regulate personal information processing activities, protect the rights and interests of personal information, and promote the lawful use of personal information, with the values of protecting the rights of personal information, restricting disclosure by the processor, prohibiting unlawful infringement or jeopardizing the public interest, and safeguarding national security, and also with the protection of the rights and interests of individuals' information as the first aim. Paradoxically, the current direction of privacy computing in this regard runs counter to the current state of the legislation and needs to be supplemented accordingly.

3.3. Blurring of Risk by Inherent Technical Characteristics

Finally, there is Mill's harm principle, which refers to freedom of action as long as it does not cause harm or interference. In the context of the application of specific algorithmic technology, it can be understood as follows: the freedom of practice of algorithmic technology presupposes that it does not cause explicit harm, and if there is no obvious harm or danger after exercising reasonable care, the algorithmic technology should be allowed to be applied. The important premise for the application of this principle lies in the identifiability and concretiza-

tion of the harm, for example, in the field of civil compensation, the determination of the result of the damage is one of the elements for the formation of the right to claim for damages. In the era of big data, there are many difficulties in defining "harm". The harm caused by algorithmic technology is non-direct and usually difficult for people to perceive. In scenarios such as the big data kill familiarization, it is difficult for the victims to perceive the improper treatment they have been subjected to, and they are unknowingly reduced to the tools of capital self-management. Coupled with the fact that it is difficult for individuals to understand the principles of the algorithm, the huge information gap makes them exploited without realizing it, and the information cocoon solidifies their limited data space, the algorithm layer by layer blurs and decentralizes the discrimination and harm suffered by individuals.

In the field of privacy computing, an important reason why "harm" is difficult to specify and particularize is the inherent characteristic of poor interpretability. Privacy computing involves a variety of algorithms that need to ensure that some of the assumptions set by the security foundation are valid. In practice, however, these assumptions may not always hold due to various constraints. At the same time, one of the major difficulties encountered in the practical realization of privacy computing is that the complexity of the operation of data in the objective world is far beyond the scope of a few simple mathematical models, no matter how fine the deep neural network simulation may be, it may be far from the actual operation mechanism. The best models available today can cover certain situations, but they cannot form the same operating principle. In addition, the deep learning network can explain the characteristics of the messenger, coupled with a variety of simulations on the Internet to open source implementation, many people are doing is to adjust the parameters and optimize the deep learning framework of the work, like engineers building blocks: first of all, the best few models to restore the model, in the model around the parameter modification, add a little attention to the mechanism or change the order of the experiments suddenly found that the experiment can be run, then a success. This "trial and error" is in accordance with the experimental science of the proposed conjecture → design program → experimental verification → proposed new conjecture… path of operation, the lack of basic theory support, most of the effective program is through intuition and Most effective programs are generated through intuition and constantly verified by experiments. Therefore, no matter from the perspective of efficiency or effectiveness, the optimization of deep learning is very difficult to achieve.

Because of the poor interpretability, it creates another potential security problem, the results are not fully controllable, blurring the specific controllable risks. Ideal algorithmic models need to satisfy specific very hypothetical conditions, such as pictures requiring a certain resolution, speech requiring correctness without accent, etc. However, the actual application scenarios are variable and complex, and idealized algorithmic models are difficult to cover all types of situ-

ations. Taking the existing neural network model as an example, due to the dynamic and flexible data processing activities of the real human brain, which are mutually cooperative and difficult to exhaust, the current neural network model is slow to learn, lacks the corresponding theoretical guidance, and is difficult to cover the real operation pattern of the human brain. Since the input is unpredictable and the process is uncontrollable, there is no way to know whether the output data is true and reliable and meets the expectation, so it is difficult for privacy computing to realize the utility of a wider range of fields. A model of expected benefits and expected costs is introduced, where expected benefits refer to the benefits predicted based on known information in the absence of unforeseen circumstances, and expected costs refer to the most likely attainable costs expected to be incurred in the future. For privacy computing technology to be practical, it needs to satisfy that the expected benefit is greater than the expected cost. However, the scenario of privacy computing is more complex than that of artificial intelligence in general: the latter involves only one participant, whereas the former may involve multiple data processors due to its characteristics, and the expected benefits and expected costs of each data processor are associated with the other in a given situation, so that each party's behavioral choices are not the same.

Take a simple application scenario as an example, two data processors each have different data sources, one of them wants to utilize the other data processor's data to obtain certain outputs and is willing to pay a certain amount of money, for the data user, its expected benefits by obtaining each other's data are calculable and fixed, and its expected cost consists of the communication cost and the expenditure cost, which is also controllable. The fixed and controllable expected benefits and expected costs determine that there is no incentive for data counterfeiting, in other words, it is not difficult to understand that for the data user, who wants to obtain the real computing results, in the black-box algorithmic environment, he/she has to provide his/her own real and reliable data. The biggest difference between privacy computing and usual data processing is that neither party can see the other party's data, which makes it impossible for the participants to determine the authenticity of the other party's data. Based on this, it is difficult to distinguish the risk of normal operation of the model from the risk of human falsification in the unique operating environment of the black box, which on one hand blurs the cost of controllable risks, and on the other hand the motivational drive for falsification affects the expected cost, i.e., for the latter uncertainty needs to be included in the consideration of the cost. Thus, the expected benefit for the data user is the remuneration paid by the other party, which can be fixed, and the expected cost consists of the cost of communication and the cost due to the risk of data leakage, which, obviously, can be fluctuating and variable, and the party being used has the full choice to enter partially or fully incorrect data in order to reduce the cost, and if he/she enters false data to minimize his/her own cost, because by not entering real data There would never

be a risk of information leakage, and thus the data-used party has a strong incentive to falsify.

4. Reflections on and Responses to Legal Issues of Privacy Computing in China

Based on the limitations of the traditional risk regulation approach in the legal issues of privacy computing, the author believes that it is not appropriate to push back the construction of a new system during the mature transition period of the technology, which is time-consuming and laborious, and it is even still necessary to consider the additional risks brought about by its own applicability. Instead of eliminating risks with new algorithmic technology, the author believes that it is more expedient to take the traditional risk regulation approach as the basis and make appropriate adjustments in the original technical structure to regulate the secondary risks induced by the application of technology.

4.1. Building a Dynamic Framework for Informed Consent throughout the Process

Although the application of the rule of informed consent in the context of privacy computing has some limitations, such as those described above, it is undeniable that it plays an important role as the first gateway for the collection, utilization, transformation and exchange of information. Rather than reconstructing a new system, reasonable improvements can be made to the existing rules to consolidate their status as the first "gate" of risk regulation.

Existing privacy computing technology for the use of data processing is not a one-time or one-way, but multi-stage, chained, for the same set of data may need to go through a number of different standards of analysis and processing, the upper and middle reaches of the application of technology to the middle and lower reaches of the data processing as the basis of the change in any one of the subtle links, may be "pulling a start the entire body Any change in the smallest link may 'unleash the whole body'". Therefore, in privacy computing, the traditional static informed consent rules should be improved and modified to develop into a dynamic risk notification model for the whole process, so as to adapt to the current flexible and different application scenarios of privacy computing.

By informing users of the risks associated with data processing throughout the entire process, and by developing a dynamic structure of prior notification to one of prior notification, monitoring and evaluation, users will have the opportunity to know the stakes of data utilization in all aspects, and, to a certain extent, rid themselves of dependence on algorithmic technology, activate their autonomy, and, on that basis, make choices that are truly in line with their intentions. In addition, repeated notification of the whole process also has a warning effect, and the possibility of users understanding the relevant risks is also improved, even after the initial authorization of processing, there is an opportunity to stop losses in time, control subsequent risks, in order to avoid the "blanket

agreement" type of uncontrollable losses. Thus, a dynamic informed consent structure is of great importance in ensuring user autonomy by specifying and limiting risks both ex ante and ex post. In addition, the dynamic informed consent rules also form a reverse pushback effect on data processors, which, precisely because of the possibility of predicting the stage of user authorization, will carefully assess the risks and inform them in real time, and proactively take measures to control the risks rather than just letting them happen, so as to ensure the consistency of user authorization.

Theoretically, in the static structure of informed consent, the risk of "user unawareness" is the main object of regulation, and for this purpose, data processors can be considered to have formally fulfilled the obligation as long as they inform the operation effects and generalized risks of privacy computing technology. The problem is that the formal prior risk notification cannot cover the subsequent dynamic risk development, and some hidden risks and secondary risks will only be exposed in the subsequent modeling and computational processing. Relying only on the generalized risk prevention responsibility is a way to ensure that data processors are active and proactive in implementing the whole process of safety and security obligations, while the dynamic informed consent model can prompt data processors to actively explore the risks and prudently process and utilize the data to ensure the security, accuracy and privacy of the data, and to reduce the number of users choosing to "jump off the train" when they find out that the risks are unknowable and uncontrollable. Reduce the possibility of users choosing to "jump off the train" when they realize that the risks are unknown and uncontrollable.

It is undeniable that the dynamic risk regulation construct chooses to tilt towards the latter in the value trade-off between efficiency and security, which inevitably sacrifices the guarantee of efficiency to a certain extent, resulting in unfavorable conditions such as increased regulation costs and prolonged data utilization cycle. In the author's view, the technical original intention of privacy computing is to solve the contradictory problems of data utilization and privacy protection, and from the perspective of teleology, only after the prerequisite problem of privacy protection is solved can further circulation and utilization of data be possible, implying that the data processors can voluntarily provide the data without any worries.

4.2. Introducing a Socially Oriented Data Protection Model

"Personal information is not only about the interests of individuals, but also about the interests of others and society as a whole, and is public and social in nature." From the point of view of ownership, individuals do not fully own personal information, personal information is not entirely the product of individuals, in other words, "personal information is in fact an ecology", it is our activities in society, the natural formation of an ecosystem, which is not created by the individual alone, and naturally not controlled by the individual alone. From the

point of view of utilization, individuals also cannot fully control personal data, as a necessary medium of social communication, personal information is inevitably known to a certain extent to others and society, and it naturally carries the attribute of "sociality". Recognizing the social and public nature of personal information, the traditional data protection model based on the individual should be revised to adapt to the current transition from "data use" to "data governance". In recent times, Western personal data protection legislation has shown a general trend of individualism, taking the Uniform Data Protection Act as an example, which is a system based on individual control of personal information, and the integration of data rights into the framework of individual rights, with individualism as the basis. Paradoxically, the emphasis on the circulation and use of personal data in society and the extraction of value from collective data has been a major trend in the development of data technology, and the developmental aspects of technology clearly run counter to the current state of Western legislation.

At present, the basis of data protection lies primarily in the contractual relationship between the data owner and the data processor. However, with the application of algorithmic technologies such as big data, the contractualized and equal exchange model has gradually been broken, and the data processor is naturally in a superior position, both in terms of access to information and risk control. On the contrary, the harm suffered by the user is generally difficult to be perceived, and the uncertainty of the damage result causes difficulties in locating the subject of specific damages. In addition, in terms of burden of proof, due to the complexity of the privacy computer system and its "black box" attribute, the damaged group usually does not have the ability to enjoy the evidence. Compared with the damage caused by personal privacy leakage, data analysis technology often causes hidden and long-term damage to the group.

In terms of the current situation of localized personal data protection, unlike the West, which has already established a whole set of personal data protection concepts based on individualism, China's Data Security Law, Personal Information Protection Law, and Cybersecurity Law have just been introduced, and a mature personal information protection system has not yet been established, and it can still be said to be a blank sheet of paper in terms of the refinement of the relevant contents and the improvement of the remedies, which is highly accommodating to the adoption of the social-oriented data protection The model of social-based data protection has a high degree of tolerance and will not produce a large reaction of exclusion, coupled with China's traditional social concept of prioritizing public interests, the acceptance of the data protection model in the field of privacy computing is relatively smooth.

At the same time, the introduction of a social model of data protection does not imply a weakening of the protection of the rights of personal information. The public nature of personal data reveals that it has an independent legal benefit of protection when it is utilized socially, which is not in conflict with the pro-

tection of individual's legal interest in terms of value. Even under certain circumstances, the protection of public attributes of personal data can give new ways of relief for the protection of individual rights and interests, because in the ocean of big data, the value of individual data is very small, so that the control of individual data is extremely weak, through the radiation effect of macro data governance model, can make a large portion of the individual interests of micro balanced, and at the same time improve the efficiency of the protection of private interests.

4.3. Establishing an Externally Neutral Regulatory Review Mechanism

In response to the previously discussed risk of the existence of data processor fakery, to avoid ambiguity in the outcome of the risk, it is possible to think in terms of increasing the cost, i.e., making the cost on the side of the data processor increase as the probability of inputting true data decreases. This can be achieved either through endogenous mechanisms (e.g., steganographic queries) or additional mechanisms (e.g., regulatory mechanisms) can be implemented. In the field of privacy computing, in the absence of mature endogenous constraint mechanisms, forming a mandatory supervision through external neutral regulatory mechanisms or a more effective transition method to avoid backdoor operations and realize win-win situation for collaborators. Through strong external regulation, the joint supervision of multiple data processors can be formed to detect the hidden risks of black-box computing. The external regulatory body should be a neutral third-party government agency or organization that has no interest in the participants (Tang, 2022). In addition to the mandatory administrative means, or through the establishment of mutual constraints mechanism, the open source code, artificial intelligence to combat attacks, zero-knowledge proof and other cryptographic tools can be used to "fight fire with fire", to ensure the neutrality of the regulatory body and weaken the black-box operation. The neutrality of the main body can be ensured to weaken the characteristics of the black box. Some scholars advocate that external review should focus on whether the technical side is doing its best to reduce algorithmic discrimination. It is because of the flaws in the data and models themselves that confrontation and games between data processors become more pronounced, and the problem of algorithmic discrimination is particularly pronounced in privacy computing scenarios. Since the original algorithmic discrimination lies in the discriminatory nature of data, before the construction of the algorithmic model, the collection and cleaning of data should be regulated, and at the same time, a complete set of "default data screening mechanism" can be established, so as to prompt the data processors to take the initiative in reviewing the data and removing the unqualified, unclear and redundant data, so as to improve the efficiency of supervision and review, and to solve the problem of algorithmic discrimination at the source.

4.4. Establishing a Risk-Proof Data Governance Compliance System

With the rapid development of the digital economy, the data security protection and compliance risks faced by privacy computing are gradually increasing. To realize sustainable digital transformation and move from "data management" to "data governance", it is still not enough to rely solely on the above dimensions. Lack of refined top-level legal guidelines, enterprise competition is often prone to disorder and confusion, the veil of "surface compliance" hides the nature of capital for profit and the potential risks of data technology, some data compliance technology to a certain extent also induces the risk of non-compliance; the lack of a sound industry management system, cross-platform, cross-departmental, cross system communication costs are large, and the data governance system has to be improved to ensure that it can meet the needs of the industry (Zhao & Zhou, 2021). In the absence of a sound industry management system, cross-platform, cross-departmental, and cross-system communication costs are large, and the possibility of coordination and cooperation is problematic in the context of potential gaming and confrontation among enterprises, and in the absence of institutional constraints, one major department often takes the lead and other departments lack the motivation to participate. Thus, based on the principle of systematization of data governance, linking the various dimensions of governance together to form a top-to-bottom, inside-out governance system framework is necessary and essential for preventing and governing compliance risks in the context of the rapid development of data compliance technology represented by privacy computing.

At the level of legal regulation, the security obligations of data processors should be strengthened, and the corresponding legal responsibilities should be realized, so as to form a substantive binding force on data processors. In other words, on the basis of the informed consent rule, the law puts forward higher compliance requirements for data processors in the process of data circulation and use, which is also in line with the purpose of the creation of privacy computing, namely, to ensure that the data is "available but not visible", "the right of use is separated from the right of ownership", and the output of data processors is the result of the privacy computing model. This is also in line with the purpose of the creation of privacy computing, which is to ensure that data is "available and invisible" and "the right of use is separated from the right of ownership", and that data processors output the results of the privacy computing model to the outside world and comply with the relevant legal requirements. Article 21 of the Cybersecurity Law stipulates the network security level protection system, and network operators shall fulfill security obligations such as "adopting technical measures to prevent computer viruses and network attacks, network intrusion and other acts that jeopardize network security," "adopting measures such as data classification, important data backup and encryption," etc.; and the data processor shall adopt measures such as "available and visible," and "separation

of use and ownership". Similarly, Article 51 of the Personal Information Protection Law puts forward similar requirements on the obligations of personal information processors to "adopt corresponding encryption, de-identification and other security technology measures". In the author's opinion, the legal responsibility for violating security protection obligations and the punishment for corresponding illegal acts should be further clarified, so as to prompt data processors to strengthen their initiative and enthusiasm in taking protection measures for user data and prevent the occurrence of potential risks.

At the level of technical application, data processors should expand their exploration of scenario applications in the Internet and other fields under the guidance of industry standards, emphasizing the systematic adjustment of data security standards and technical applications. It is necessary to utilize the platform to encourage the creation of more communication opportunities and openly publicize more cases of data sharing. For example, in the network wind control scenario in the financial field, privacy computing technology can realize the safe fusion of the financial institutions' own data network and the data network of external institutions, and jointly establish a digital risk credit rating model to realize real-time prediction and improve the quality of wind control under the premise that the original data of all parties are not out of the domain. In response to the inherent characteristics of poor interpretability of privacy computing, at the industry level, the latent risks of algorithmic technology are examined in depth through the industry review system, i.e., the introduction of a neutral industry review mechanism.

Based on this, it is a general trend in the development of data science and technology to establish a sound data compliance system at the national, social, enterprise and even individual levels to reduce data risks and promote the effective circulation and use of data.

5. Conclusion

Privacy computing technology can cover a wide range of fields such as finance, healthcare, education, government affairs, etc., and has a wide range of application prospects. As an emerging algorithmic technology, it still has a lot of defects in China's current application scenarios, on the one hand, there are still deficiencies in the concept of technical foundation, on the other hand, legal regulations are also lagging behind, and there is still a long way to go to realize the technology on the ground. When the technical development of the principle layer enters a bottleneck, and accelerates the practicalization of privacy computing technology in a wider range of scenarios, the existing risk regulation method does not ipso facto lose its legitimacy, and still has the potential to continue to be applied, and it should be improved and amended according to the existing deficiencies, and amended by new means and new ways to cope with the new risks and challenges brought by the privacy computing: one of the following is to change the structure of ex-ante examination from static to dynamic information

regulation: to change the structure of ex-post examination to dynamic information regulation. First, shift from a static prior review structure to a dynamic informed consent framework to strengthen the autonomy of the whole process of data utilization; second, introduce the concept of "social cybernetics" on the basis of a single individual-based data protection model, and establish a data security protection system that adapts to the urgent needs of the era of algorithmic technology application; and third, propose a set of independent external review system to realize the protection of the hidden risks of privacy computing. Only in this way can we alleviate the contradiction between data utilization and data protection in the current technological applications, so as to solve the current dilemma of "wide application prospects, but difficult to implement in practice".

Unfortunately, this article still has some shortcomings. Firstly, the article mentions a number of examples of privacy computing, but may not go into enough depth about the failures of the risk-prevention approach to regulation in those examples and the specifics of the response. Secondly, this may make it difficult for readers to understand how the regulation performs in practice. The article focuses mainly on the technical aspects, but may not provide sufficient information on the legal and policy context. This may make it difficult for readers to understand the relevant legal and policy frameworks and how they affect the choice and application of risk prevention regulation.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

Tang, L.-Y. (2021). Legal Regulation of Privacy Computing. *Social Science, No. 12,* 117-125.

Tang, L.-Y. (2022). Risk Regulation and Jurisprudence of Data Compliance Technology. *Oriental Law, No. 1,* 79.

Zhao, J. W. (2022). Dispelling the Myth of Privacy Computing: Security Risks and Regulatory Logic of Governance Technology. *Journal of East China University of Politics and Law, 25,* 35-49.

Zhao, J. W., & Zhou, R. J. (2021). Privacy Computing Technology: Construction of Cooperative Protection Rules for Data Flow and Data Security. *Telecommunication Network Technology, No. 7,* 53-58.