World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-45, April -2025
ISSN: 2749-3601

RESEARCH ON THE INTEREST BALANCE MECHANISM BETWEEN INFORMATION SHARING AND PERSONAL INFORMATION PROTECTION IN THE BIG DATA ERA

Wang Cong
Doctoral Student at the University of World Economy and Diplomacy, Tashkent 100174,Uzbekistan
Suqian University, Suqian 223800, China

Article history:

Received: 24th February 2025
Accepted: 20th March 2025

Abstract:

In the wave of digital transformation, data has become the core production factor that promotes social development . While establishing an information disclosure system, there will inevitably be potential risks of infringement of personal information. Starting with the data obtained from field research, this article analyzes the main challenges currently facing personal information and the contradiction between information sharing and information protection. On the basis of establishing the basic principles of legislation, on the one hand, a sound legal protection system should be established to strengthen supervision; on the other hand, industry self-discipline and personal awareness of information subjects should be strengthened, and efforts should be made to protect personal information from infringement while maintaining the openness and sharing of personal information, so as to find a balance between personal information protection and promoting the free flow of information, and establish an interest balance mechanism between information sharing and personal information protection.

Keywords: information sharing, personal information protection, interest balance, scenario-based hierarchical protection

INTRODUCTION

In the era of big data, the use of personal information is very common. For the purpose of policy formulation and implementation such as e-government management, population survey statistics, and household registration, and for the needs of commercial operations and the popularization of e-commerce, the state needs to collect and process a large amount of personal information. For information controllers, data is a production factor and a guide for action. For countries, data has long become a basic strategic resource for all countries [1] . The cornerstone of the booming development of big data technology is the collection, processing, and use of massive data, and this massive data comes from endless personal information.

The Internet makes information sharing open, public and public. While establishing an information disclosure system, information sharing will inevitably involve the collection, storage, processing and exchange of personal information, and there will inevitably be risks of potential infringement of personal information. How to find a balance between protecting privacy and promoting the free flow of information, and how to establish an interest balance mechanism for information sharing and personal information protection in the big data era are issues that legislators must consider . In 2023, a health data leak incident sparked heated discussions among the people, aptly reflecting the core contradiction of the big data era:

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-45, April -2025
ISSN: 2749-3601

we are eager for the convenience brought by data dividends, but we are also worried about becoming "transparent people."

Based on an in-depth survey of 800 respondents and an analysis of 37 typical cases, this article attempts to answer a key question: How to release the value of data while ensuring the security of personal information? The study found that the traditional "one-size-fits-all" protection model is no longer able to adapt to complex data application scenarios, and a more flexible balance mechanism needs to be established.

ANALYSIS AND RESULTS

Personal information refers to any information that can identify a specific individual. It is information or a collection of information that can identify a specific individual, including name , age, gender, ID number , tribe , home address, height, weight, portrait, fingerprint , work unit, contact number, career history, personal credit, criminal record, religious beliefs and various social activities of the individual. It is any objective information that can identify a certain individual alone or when compared with other information [2] . "Personal information", "personal data", "personal intelligence" and other terms can all be used to express the meaning of personal information. They have similar connotations and are often used interchangeably. In English, "personal data" and "personal information" can be used to express it.

1. Legal dilemmas and practical challenges of personal information protection under information sharing

The "Decision on Maintaining Internet Security" of the Standing Committee of the National People's Congress in 2000 marked the beginning of China's use of laws to regulate the Internet; in 2012, the " Decision on Strengthening Network Information Protection " was passed, which was China's first law specifically protecting the right to personal information; the "Tort Liability Law" promulgated in 2009 stipulates the protection of privacy rights and network tort liability ; the "Consumer Rights Protection Law" revised on October 25, 2013 also attaches importance to the protection of consumer personal information ; the "Cybersecurity Law" enacted in 2016 is the most comprehensive legislation on personal information protection to date; the "General Principles of the Civil Law" implemented on October 1, 2017 also clearly stipulates that personal information is protected by law ; the implementation of the "Personal Information Protection Law" in 2021 marks the entry of China's personal information protection into a new stage. It can be said that China has basically established a legal system for the protection of personal information. But in fact, there are many unsatisfactory aspects of the current legislative status:

First, the legal system is in a "fragmented" dilemma. China's personal information protection legislation presents the characteristics of "nine dragons governing the water". The Cybersecurity Law focuses on infrastructure security, the Personal Information Protection Law focuses on rights protection, and the Data Security Law emphasizes classified management. This multi-legislative model often causes companies to fall into "applicability confusion" when complying with regulations. Take a cross-border e-commerce platform as an example. It must comply with the data localization requirements of the Cybersecurity Law, the personal consent rules of the Personal Information Protection Law, and the export control regulations of the Data Security Law at the same time, and the compliance costs remain high. [3]

Secondly, the "campaign-style" characteristics of law enforcement practice . Although the special rectification actions in recent years have achieved phased results, they have exposed the problem of insufficient sustainability of law enforcement. In the 2023 APP special rectification, a certain map software was notified for illegally collecting location information, but it only evaded detection through version updates, and its actual behavior did not change. This phenomenon reflects the vicious cycle of "surprise inspection-superficial

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-45, April -2025
ISSN: 2749-3601

rectification-return of problems".

Finally, the "funnel effect" of rights protection channels . The survey shows that among the respondents who encountered information leakage, only 3.7% eventually chose judicial rights protection. In a case of "forced employment" of a college student, the victim needed to prove the causal relationship between information leakage and the consequences of damage, and this burden of proof became the main obstacle to rights protection. The serious imbalance between the cost and benefits of rights protection has led most victims to choose to remain silent. Taking the data leakage incident of an e-commerce platform in 2023 as an example, users faced the problems of difficulty in providing evidence and high costs when defending their rights, and only a few people received compensation in the end. In 2023, a taxi-hailing platform was fined 800,000 yuan by the Cyberspace Administration of China for failing to fulfill its obligations to protect personal information, but its rectification measures did not completely solve the problem of data abuse, reflecting the limitations of law enforcement.

2. Typical risks faced by personal information

More than 90% of students in all majors of the author's school found themselves "employed". Their basic information, employment units and wages can be queried on the personal tax declaration system. All the work units are local auto trade companies. At present, it seems that the reason why the auto trade companies "employed" these students is to evade taxes by increasing employee wages. In order to understand more about the risks faced by personal information, the research team distributed 800 questionnaires to the public, including students, through the Internet in October 2024. The questionnaire provides a relatively objective and accurate data research and analysis basis for the entire research activity. The typical risks currently faced by personal information are:

a.Personal information leakage is extremely common

95% of the respondents said they had experienced personal information leakage.

b. The hidden nature of acts that infringe personal information

Websites track users through cookies, obtain user personal information and sell or exploit it. Other very covert ways of obtaining user personal information are also difficult to guard against.

c. The types of personal information that have been infringed are diverse

The respondents generally believed that basic information, account information and privacy information were the most important, while device information, social relationship information and network behavior information were relatively less important. In fact, the types of leaked personal information are far more than these.

d. There are various ways for personal information to be leaked

Online registration, loss of personal information and documents, and statistical information organized by companies, schools and other organizations are common ways. In addition, there are also leaks of personal information collected by merchants, companies and financial institutions, virus infections on mobile phones and computers, and hacker attacks.

e. personal information leakage are serious

At present, most new types of telecommunications network fraud are related to the leakage of personal information. There are also frequent harassment messages and calls, personal privacy leakage leading to reputation damage, certain property losses, endangerment of personal safety, discrimination and differential treatment caused by data predictive analysis, etc.

f. People have a strong sense of self-protection, but they don’t know how to protect themselves

In specific litigation, it is difficult for the infringed party to obtain evidence and the cost of defending rights is high, so ordinary people rarely choose this approach.

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-45, April -2025
ISSN: 2749-3601

In addition to the threats mentioned above from illegal acquisition, monopoly, and use by criminals, the current most important "legal" method of obtaining personal information - user informed consent - also poses a potential threat to the security of personal information. Taking China's "informed consent" mechanism as an example, the following outstanding problems still exist in its implementation : the privacy policy is not compliant enough, transparency still needs to be improved , key information is hidden or vague , and some APP privacy policies fail to fully disclose the core elements such as the identity of the information processor, processing purpose, data type, storage period, etc. in accordance with Article 17 of the "Personal Information Protection Law", or use general expressions to avoid specific explanations ; [4] The text is poorly readable: the policy document is lengthy and contains too many professional terms, which does not meet the "clear and easy to understand" requirement of the "Network Security Standard Practice Guide - Mobile Internet Application (APP) Privacy Policy" ; the consent mechanism has forced authorization, disguised coercion , and "all or nothing" bundled authorization ; "frequent pop-ups" interfere with user choices ; the minimum necessary principle is not implemented in place , and information is collected beyond the scope ; "non-essential" information is collected in disguise , and user device information, social relationship data and other data are indirectly obtained through third-party SDKs, embedded codes, etc., to avoid regulatory review ; the user exercise mechanism is perfunctory and the complaint channel is not smooth .

3. Conflict between information sharing and personal information protection

a. The contradiction between data openness and information protection

With the development of big data technology, the opening and circulation of data has become an inevitable trend, and data monopoly has become a thing of the past. As the subject of information, no one wants to be "naked" in front of big data. Therefore, how to balance the contradiction between data opening and personal information protection is the most difficult challenge facing personal information protection under the background of big data technology.

b. Value conflict between data sharing and information protection

In the context of the diversified needs of social entities, conflicts between all values protected by the law are inevitable. The purpose of personal information protection is to protect citizens' personality rights and maintain personal dignity, while the value foundation behind data sharing is information freedom, which is also a protected basic right and is recognized as a constitutional right by the United Nations Convention on Civil and Political Rights. The contradiction between data sharing and personal information protection is a concrete manifestation of the conflict between the legal values protected by the two.

c. Disputes over information ownership between various data collection platforms and information subjects

Who should own the user personal information (including user purchase records of goods and services) obtained by various network data carriers, especially various enterprise platforms that provide goods or services in the course of their operations? In 2023, a map APP was sued for sharing location data without the user's explicit consent. The court finally ruled that the platform should compensate the user for the loss, but did not clarify the issue of data ownership .

d. The contradiction between individuals' growing awareness of information protection and the lack of corresponding protection methods and measures

Under the Internet + big data, with the enhancement of legal awareness, citizens' awareness of protecting personal information is also growing, but many people are confused about having awareness but not knowing how to do it.

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-45, April -2025
ISSN: 2749-3601

4. Establishment of a balance mechanism between information sharing and personal information protection

a. The value balance is based on who is leaning towards

When two legal values conflict and must be tilted, the legislator's value balance will directly determine the basic principles and direction of legislation and law enforcement. The legal basis for personal information protection in my country is the theory of personality rights, and personality rights themselves are a kind of absolute right with dominance, which focuses on emphasizing the dominance of citizens over the personal interests of personal information. Therefore, laws and regulations should pay more attention to the regulation of information users to protect personal information rights.

b. The improvement of the legal system is the basis for the establishment of a balancing mechanism

First, establish the basic principles of relevant legislation

The basic principles of the Personal Information Protection Law are the basic principles guiding personal information protection legislation and judicial practice, and are also the basic principles that run through the legal system of personal information protection. Looking at the personal information protection legislation of countries around the world, most of them stipulate the following basic principles: the principle of legality, the principle of security management, the principle of "situational consistency", etc.

Secondly, accurately identify personal information and clarify the rights attributes of personal information rights.

According to the mainstream theory of traditional personal information definition standards, identifiability is the most important feature, but the boundary between identifiable information and non-identifiable information is not static. With the development of technology, some information that seemed unidentifiable before may become identifiable. In addition, even at the same technical level, different standards may lead to different definitions of the scope of identifiable information for different technical entities. In this case, the identification capability standard comes into play.

At present, there are four different theories in the academic community regarding the legal protection of personal information: property rights protection, privacy rights protection, public goods protection, and the creation of personal information rights for protection. Different rights protection bases have different characterizations of personal information. Due to space limitations, the four theories will not be specifically reviewed here. [5] The author agrees with the theory of personal information rights. Of course, no matter which protection theory is adopted, in the context of the booming era of big data technology, the precious value of personal information lies in being counted, analyzed, and predicted in advance. Otherwise, its value is difficult to be compared with privacy, property, etc. In this process, the most important content is whether the use of data by data sharers is legal, whether it can be effectively supervised, and whether effective sanctions can be imposed after illegal use.

Secondly, improve the "informed consent" system

As mentioned above, although the informed consent system has various drawbacks, it is still necessary in the current legal environment of my country. What needs to be done in the short term is to improve the system, refine the relevant operating procedures, and clarify the responsibilities that violators must bear.

c. Establish an industry self-discipline system and cultivate the internal governance mechanism of information users

Legislators and law enforcers are ultimately laymen in big data or the Internet, and even the most perfect legal system may be exploited by industry insiders. Therefore, it is necessary to reduce infringements on personal information rights through industry self-discipline. Therefore, on the basis of external supervision, we should learn from Western experience, establish an industry self-

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-45, April -2025
ISSN: 2749-3601

discipline system for information users, and cultivate an internal governance mechanism for information users.

First, establish an industry self-regulatory organization

Industry self-regulatory organizations are formed by members who freely join and use their relatively authoritative status and unified standards to manage and supervise the specific behavior of members.

Secondly, formulate a comprehensive industry self-discipline convention

Self-regulatory organizations can provide standard personal information protection model texts for enterprises and institutions in the industry, and members of the organization can use this as the minimum standard to formulate their own treaty texts.

Finally, explore the establishment of a personal information security certification system

The model of quality control through audit and certification has been reflected in many industries, such as " ISO " certification, " 3C " certification, etc. The personal information security certification system can be established by imitating such certification. This system can not only become a part of the goodwill of the certified companies, but also provide auxiliary information for users to make product choices.

d. Strengthen publicity and enhance the self-protection awareness of personal information subjects

In addition to supervision and self-discipline of information users, it is also necessary to strengthen publicity efforts and enhance the self-protection awareness of personal information subjects. Legal publicity can be carried out through ubiquitous media platforms to improve personal self-protection awareness and ability. In addition to letting information subjects know what personal information is and what belongs to personal information, it is also necessary to publicize how to protect it, how to reduce losses after infringement, and how to defend rights.

CONCLUSION

This study, through an empirical analysis of the current status of personal information protection in China , reveals the deep-seated contradiction between information sharing and privacy protection in the era of big data. The study found that the traditional binary oppositional thinking is no longer able to adapt to the needs of digital transformation, and a more inclusive and dynamic balance mechanism must be established. Based on the research results, this article puts forward the following systematic suggestions:

a. new governance structure of "Trinity"

Legislative reform : It is recommended to formulate the "Personal Information Protection Law Implementation Regulations" to refine the operational standards of the "minimum necessary" principle. We can learn from Singapore's "data trust" system and establish a government-led third-party data hosting mechanism. The practice of a municipal government data sharing platform shows that this model can increase data utilization efficiency by 30% while reducing the risk of leakage by 65%. [6]

Technology empowerment: Focus on developing a privacy computing technology system. The commercial application of technologies such as federated learning and multi-party secure computing has shown results. A case study of a medical big data company showed that after adopting differential privacy technology, the data set availability remained at 92%, and the re-identification risk was reduced to less than 0.3%.

Mechanism innovation: Promote the "Data Protection Officer" professional qualification certification system. Refer to the CPA model to establish a professional talent team. The pilot data of a multinational company showed that after the establishment of a full-time DPO, the compliance rectification cycle was shortened by 40% and the regulatory penalties were reduced by 58%.

b. Establish a scenario-based hierarchical protection system

Design differentiated protection solutions for data types with different risk levels:

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-45, April -2025
ISSN: 2749-3601

c. Improve the "last mile" of rights and interests relief

Establish a "reversal of the burden of proof" mechanism: In information leakage cases, the data controller is responsible for proving that adequate protection measures have been taken. A pilot case in a Zhejiang court in 2023 showed that this rule increased the success rate of rights protection from 12% to 47%.

Data Category	Protection Level	Usage Guidelines	Typical Cases
Biometrics	Special	Individual authorization+ dynamic verification	Iris recognition system of a payment platform
Health data	Level 1	De - identification + Audit Trail	Regional Medical Big Data Center
Consumption records	Level 2	Aggregate analysis + access control	E-commerce user portrait system
Device Information	Level 3	Anonymization + deadline management	IoT device management platform

Promote the "public interest litigation + professional assessment" model: In a public interest litigation case on a social platform filed by the procuratorate, a third-party data security assessment agency was introduced to make the calculation of damages more scientific and reasonable. Develop a "one-click rights protection" digital platform: The "Digital Security Shield" mini program launched in a certain province integrates functions such as complaints and reporting, evidence preservation, and loss assessment, reducing the time cost of rights protection by 70%.

The global value of China's solutions

The practical experience accumulated by China in promoting the construction of "Digital China", especially the combination of "cybersecurity review + data classification management", provides an important reference for developing countries. At the 2023 "Belt and Road" Digital Governance Seminar, the concept of "development-oriented protection" proposed by China was widely recognized.

As the famous jurist Lawrence Lessig said: "Code is law." In the digital world dominated by algorithms, we need to improve legal rules and innovate governance technology. By establishing a multi-governance system led by the government, operated by the market, and coordinated by society, we can find a new way to balance security and development. This is not only a protection of personal information rights and interests, but also a positive shaping of the digital civilization.

REFERENCES

1. In August 2015, the State Council of China issued the "Action Outline for Promoting the Development of Big Data", which clearly pointed out that data is a basic strategic resource of the country.
2. Qi Aimin. International Comparative Study on Personal Information Protection Law in the Big Data Era [M]. Beijing: Legal Publishing House, 2015 .
3. Wang Cheng. Model selection for civil law protection of personal information[J]. Chinese Social Sciences, 2019(6):136.
4. Ding Xiaodong. Multidimensional interpretation of privacy policy: reflection on the nature of informed consent and institutional reconstruction [J]. Modern Jurisprudence. 2023 (1): 34-48.
5. Gao Fuping. Personal information processing: the

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-45, April -2025
ISSN: 2749-3601

regulatory object of my country's Personal Information Protection Law [J]. Law and Business Research, 2021 (2): 82-84.

6. Zhu Zhenzhen, Mei Yizhe. The legal model of personal information protection and its future development from a comparative perspective[J]. Journal of Henan University of Science and Technology (Social Science Edition), 2024, 42(5): 35-43. ▪ ▪