Science of Law Journal (2025)
Clausius Scientific Press, Canada

DOI: 10.23977/law.2025.040219
ISSN 2616-2296 Vol. 4 Num. 2

Legal regulation of personal information protection under the big data environment

Wang Qianying

Krirk University, Bangkok, Thailand

Keywords: Big Data; Personal Information; Legal Protection; Privacy

Abstract: With the rapid development of Internet technology, big data technology is widely used in all walks of life, and the collection, use and analysis of personal information has become more and more convenient. However, the protection of personal information faces unprecedented challenges in the big data environment. Criminals use technological means to illegally obtain, sell and use personal information, which seriously infringes on citizens' right to privacy and information self-determination. This paper aims to discuss the legal regulation of personal information protection under the big data environment, analyze the shortcomings of the current legal system, and put forward suggestions to improve the legal system of personal information protection. By drawing on the advanced experience at home and abroad, this paper proposes that the scope and level of personal information should be refined, the protection of criminal law should be strengthened, and the civil relief channels should be improved, in order to promote the healthy development of personal information while protecting the rights and interests of big data technology.

1. Foreword

With the rapid progress of information technology, big data technology has become a new engine for promoting economic and social development. Big data, with its massive, high-speed and diverse characteristics, provides unprecedented data processing and analysis capabilities for all walks of life. However, the development of big data technology has also brought new challenges in personal information protection. As an important part of data, personal information is at risk of leakage in its collection, storage, use and disclosure. Once personal information is illegally obtained or abused, it will seriously threaten the security of personal privacy, and even cause a crisis of social trust. Therefore, discussing the legal regulation of personal information protection in the environment of big data is not only related to the protection of personal privacy rights and interests, but also an important measure to maintain social stability, fairness and justice. [1]

The purpose of this study is to deeply explore the legal regulation of personal information protection in the big data environment, in order to provide a useful reference for the construction of a perfect legal system of personal information protection. The research methods mainly include literature analysis, case study and comparative analysis. By systematically reviewing domestic and international literature, this study illuminates the contemporary landscape and evolutionary trajectory of personal information protection legislation. Through meticulous case analyses, it examines the root causes, cascading impacts, and regulatory efficacy of data breaches. Building

upon exemplary practices from global jurisdictions, the research synthesizes actionable recommendations to refine China's legal framework for safeguarding personal information in the digital age.

2. Basic concept of personal information protection in the big data environment

Big data, with its five significant features, huge data volume (Volume), diverse data types (Variety), low value density (Value), fast processing speed (Velocity) and high data accuracy (Veracity), is profoundly changing our daily life and business operations. These features not only provide rich resources for data analysis, but also put higher requirements for the protection of personal information.[2]

First of all, the huge volume of data is the primary feature of big data. With the popularity of the Internet of Things, social media and e-commerce, the amount of data generated has grown exponentially. The accumulation of such massive data provides a valuable resource for data analysis, but it also brings great challenges to the storage, management and security protection of personal information. How to ensure that personal information is properly protected in such a large data set has become an urgent problem to be solved. Secondly, the diversity of data types and sources increases the difficulty of personal information protection. Big data contains not only traditional structured data, but also semi-structured data and unstructured data. This diversity of data types blurs the boundaries of personal information, increasing the complexity of conservation. Moreover, the relatively sparse data value density is another big challenge for personal information protection in the big data environment. In huge amounts of data, the proportion of valuable information is often extremely low. How to accurately mine out valuable information from these data on the premise of not violating personal privacy has become an important topic. At the same time, the high speed of data processing and response requires big data systems to respond quickly and analyze data in real time [3]. However, this pursuit of speed often conflicts with the prudent principles of personal information protection, increasing the risk of personal information leakage. In addition, although the high accuracy and reliability of data are the core value of big data, it is often difficult to guarantee the authenticity, integrity and timeliness of data in the big data environment, especially when the data comes from multiple uncontrollable external channels. This uncertainty poses an additional challenge for personal information protection.

Personal information, as the information that can directly or indirectly identify a specific natural person, including the name, date of birth, ID card number, address, telephone number, etc. In the environment of big data, the scope of personal information is constantly expanding, and dynamic behavioral data and social relationship data have also become an important part. Although these information may not be able to directly identify individuals alone, it can often outline detailed portraits of individuals through big data analysis technology, which poses a potential threat to personal privacy. The challenge of personal information protection in the environment of big data is mainly reflected in the rising risk of personal information leakage and the contradiction between personal information protection and data utilization. How to promote the reasonable and effective use of data while maintaining personal privacy rights and interests has become a key problem to be solved in the current legal regulation. Excessive data protection may inhibit technological innovation and economic development, while the lack of effective protection may lead to serious infringement of personal privacy. Therefore, it is crucial to find the balance between personal information protection and data utilization.

3. The legal system and current situation of personal information protection in China

The legal system of personal information protection in China is mainly composed of the

Constitution, civil law, criminal law and a series of administrative regulations and departmental rules. As a fundamental law, the Constitution has established the principles of citizens' basic rights and freedoms, and provided constitutional support for the protection of personal information. It guarantees the personal dignity of citizens from infringement, ensures the freedom of communication and the security of secrets, and lays a foundation for the protection of personal information. In the field of civil law, the Civil Code establishes a legal framework for the right to personal information. It defines the scope of personal information, such as name, date of birth, id number, etc., and stipulates that the processing of personal information must follow the principles of legality, legitimacy and necessity. A natural person has the right to consult, copy, correct and delete his personal information, and the information processor shall bear the responsibility of protecting the information security. This provision provides a comprehensive legal protection for the protection of personal information. In terms of criminal law, China has taken a severe crackdown on the crime of infringing on citizens 'personal information, clearly stipulating the legal responsibility of illegally obtaining, selling or providing citizens' personal information, and setting corresponding penalties.[4]

In addition, administrative regulations and departmental rules have also supplemented and improved the protection of personal information. For example, the Cyber Security Law and other laws and regulations are closely linked with the Civil Code to jointly build a legal network for personal information protection. However, although the legal system is relatively perfect, there are still deficiencies in practice. First of all, there are vague areas in the scope of personal information protection, especially for new personal information, such as network behavior data and biometric information, and the legal provisions have not been clearly defined. Secondly, the protection of criminal law needs to be strengthened. The concealment and complexity of personal information crimes bring challenges to the investigation and evidence collection work, and the intensity of punishment is relatively low, so it is difficult to form sufficient legal deterrence. The unimpeded flow of civil relief channels is also an urgent problem to be solved. Personal information leakage involves many links and liability subjects, and the victims are faced with difficulties such as difficult proof and vague compensation standards when seeking civil relief. At the same time, the legal system is so complex that the victims feel confused and confused when seeking legal aid. In terms of supervision mechanism, the supervision system of personal information protection still needs to be improved. The unclear division of regulatory responsibilities leads to duplication and overlapping of regulatory work, which affects efficiency. Regulatory means and technology lag behind, and it is difficult to deal with the risk of new personal information leakage. In addition, the legal system is complex, and the regulatory authorities face difficulties in the process of law enforcement, which affects the regulatory effect.[5]

Case analysis shows that legal regulation plays a certain role in the protection of personal information, but it also exposes problems such as unclear application of law, unclear compensation standards, and inadequate supervision and law enforcement. In order to strengthen the protection of personal information, we need to further improve the legal system, clarify the application of the law and the compensation standards, strengthen the supervision and law enforcement, and strengthen the public's awareness and education on the protection of personal information. Through these measures, we can better protect our personal information and safeguard the privacy rights of our citizens.

4. Suggestions on the legal regulation of personal information protection under the big data environment

In the environment of big data, the protection of personal information is facing unprecedented

challenges. In order to cope with these challenges more effectively, we need to put forward a series of targeted and operational suggestions from the perspective of legal regulation.

4.1 Refine the scope and level of personal information

Establish comprehensive and unified standards for defining personal information, categorizing it into distinct types such as direct and indirect identification data to ensure systematic classification. Direct identification information, such as name and ID number, should be strictly protected; appropriate measures shall be taken. Clearly differentiate between sensitive information (such as health data and religious beliefs) and general information (including names and contact details), enforcing more stringent safeguards for sensitive categories. For routine personal information, proportional handling should be applied with greater flexibility in accordance with the principles of legality, legitimacy, and necessity. Establish a tiered classification framework for personal data protection, implementing tailored security protocols based on information sensitivity, criticality, and potential impact.

4.2 Strengthening the protection of the criminal law

Enhance and refine the legal framework governing personal information crimes, enshrining the illegal acquisition, sale, and provision of personal data as unequivocally punishable offenses under criminal law. Establish detailed tiers for criminal liability and sentencing criteria, holistically evaluating the gravity, context, and societal harm of such acts to ensure precise and proportional penalties. The punishment for the negligent disclosure of personal information should be increased, which should be included in the protection scope of the criminal law, and the legal responsibility and punishment measures should be clarified.

4.3 Improve civil remedies

The independent status of personal information right is established in the civil code to provide legal support and relief ways for the rights and interests of personal information. The scope of the subject of responsibility and the principle of attribution will be clarified, the direct and indirect violators will be severely punished in accordance with the law, and the burden of proof of the victims will be appropriately reduced. If the compensation system for personal information infringement should be improved, the amount of compensation should be determined by considering various factors, and punitive damages should be applied to malicious violators.

4.4 Strengthen industry self-discipline and supervision

Establish comprehensive industry behavior regulations, explicitly define the responsibilities and obligations of data processors throughout all stages of personal information handling, and safeguard the legality and security of data processing operations.The government should strengthen the supervision of the big data industry, build a sound supervision system, conduct regular supervision and inspection, and detect and correct illegal behaviors in time. Establish a robust social co-governance mechanism for safeguarding personal information, engaging governments, enterprises, social organizations, and the public to forge a collaborative alliance that collectively shields personal data through unified efforts.

4.5 Enhance public awareness of personal information protection

Intensify public awareness campaigns and educational initiatives on personal information protection, disseminating legal knowledge and preventive strategies through diverse channels to elevate the public's capacity for self-protection. Guide individuals in the rational and lawful use of personal data, emphasizing adherence to regulations and confining information utilization to legally permitted, necessary, and ethically sound boundaries. Foster a collaborative social oversight mechanism, engaging citizens, media, and various sectors in joint supervision, while ensuring seamless accessibility to complaint and reporting platforms for strengthened accountability.[6]

To sum up, the legal regulation of personal information protection in the environment of big data needs to start from many aspects, including refining the scope and level of personal information, strengthening the protection of criminal law, improving civil relief channels, strengthening industry self-discipline and supervision, and enhancing the public's awareness of personal information protection. These proposals aim to build a more comprehensive and effective legal system for personal information protection and provide a strong legal guarantee for the security of public personal information. At the same time, these suggestions also need the joint efforts and cooperation of the government, enterprises, social organizations and the public, in order to truly achieve the goal of personal information protection. By constantly improving legal regulations and enhancing public awareness, we can more effectively deal with the challenges of personal information protection in the big data environment, and lay a solid foundation for the healthy development of the big data industry.

5. Foreign legal regulation experience of personal information protection for reference

5.1 Legal regulations on the protection of personal information in the United States

The protection system of personal information privacy in the United States is sound, and the core lies in the development of privacy legislation. Although the Constitution does not directly stipulate the right to privacy, the Federal Supreme Court has established its legal status through precedents. To this end, the United States has promulgated the Privacy Act and the Electronic Communications Privacy Law and other special laws, which strictly restrict the collection, use and disclosure of personal information by government agencies, and give information subjects the right to know, choose, access and correct. In addition, the United States advocates industry self-discipline, encourages enterprises to formulate and disclose privacy policies, and improves the level of privacy protection through third-party authentication. Regulators such as the Federal Trade Commission (FTC) supervise and impose severe penalties for violations. Legal relief channels include civil litigation and administrative complaints, which provide a strong guarantee for the information subject.

5.2 The legal regulation of personal information protection in Germany

Germany regards the right to personal information as the basic human right, namely the right of personality, and clearly defines its legal status in the Basic Law of Germany. In order to refine the protection, Germany has formulated the Federal Data Protection Law, which specifies the requirements of each link of personal information processing. German laws strictly restrict data processing, requiring explicit consent from the information subject in advance and following the principle of purpose restriction. Restrictions on cross-border transmission to ensure global information security. Germany has set up a special data protection regulatory agency, with the power of independent investigation, punishment and law enforcement, to effectively supervise

information processing activities. Those who violate the regulations will face strict legal responsibilities to provide a solid guarantee for the right to personal information.

5.3 Comparative analysis of legal regulations at home and abroad

The United States and Germany have demonstrated different legislative concepts and protection models in the protection of personal information. The United States focuses on privacy protection to ensure personal control of information; Germany emphasizes the protection of personal information rights as the basic human rights. In terms of protection mode, the United States combines legislation with industry self-discipline, while Germany relies more on legislative protection. In terms of protection, American law covers both traditional and emerging types of information, and German law is rigorous and focuses on information directly related to personal identity. In terms of legal remedies, both countries provide civil litigation and administrative complaints, but the United States is flexible and can safeguard rights and interests through class action; Germany emphasizes administrative relief, strict legal liability and punishment measures to enhance authority and effectiveness.

To sum up, the United States and Germany have their own characteristics in the field of personal information protection, and show unique advantages in the legislative concept, protection mode, protection scope and legal relief channels. By learning from the experience of the two countries, China can further improve the legal system of personal information protection, improve the level of protection, and protect the legitimate rights and interests of citizens. The model of both self-regulation and strict regulation in the American industry, as well as the legislative concept that Germany regards the right to personal information as the basic human rights, have all provided valuable inspiration for China. In the future, China should take comprehensive measures in legislation, supervision, industry self-discipline and legal relief to build a comprehensive and effective personal information protection system.

6. Future outlook of personal information protection in the big data environment

6.1 The application of technical means in personal information protection

Encryption technology and anonymization processing have become the key to personal information protection. Encryption technology can ensure the security of information in the transmission and storage, and prevent illegal access and leakage. Anonymization reduces the risk of information leakage by removing or replacing identifiers. Big data analysis technology can deeply mine data, find potential leakage risks, provide early warning signals, and help formulate protection measures. In the future, stricter technical standards and certification systems should be established, covering all links of information processing, to ensure the legal compliance of the activities, and improve the overall protection efficiency.

6.2 The combination of legal regulation and technical means

Legal regulation is crucial in the protection of personal information. In the future, it needs to clarify the protection principles and requirements to provide the legal basis for the application of technology; meanwhile, it needs to follow the technology development and flexibly adjust the legal provisions to ensure the legal and compliant technology. Technical means can play an auxiliary role within the legal framework, realize automatic processing and real-time monitoring, improve the execution efficiency and supervision accuracy, provide data support and scientific basis for legal regulation, and help to formulate accurate protection strategies.

6.3 International cooperation and coordination of personal information protection

Under the background of globalization, personal information protection is facing the challenge of transnational legal conflict. Strengthening international cooperation and coordination and promoting legal unification and mutual recognition have become the countermeasures. By signing agreements and building mechanisms, we will strengthen cooperation and exchanges, jointly deal with legal problems, and ensure the global safe circulation of information. Establish comprehensive international protection standards that seamlessly integrate guiding principles, technical specifications, and legal accountability, forging a cohesive framework to dismantle jurisdictional obstacles and reduce implementation expenses while propelling the unfettered circulation of global data. Constructing robust international cooperation mechanisms emerges as a strategic imperative—manifested through systematically orchestrated multilateral forums, specialized task forces, and unified digital interfaces for transnational expertise sharing. These dynamic conduits empower nations to collaboratively calibrate safeguarding protocols by exchanging field-tested methodologies and aligning implementation blueprints. Moreover, instituting agile consultation channels and adaptive dispute-resolution circuits will enable stakeholders to swiftly navigate conflicts, thereby fortifying the resilient equilibrium of our interdependent digital infrastructure.

To sum up, technical means are combined with legal regulation to build a strict protection system; international cooperation and coordination to meet transnational challenges. Encryption, anonymity and big data analysis technology, build information security barrier; legal regulation of clear principles, guide technology development; international cooperation to formulate unified standards and promote the free flow of information. In the future, it is necessary to continuously optimize technical means, improve legal regulations, strengthen international cooperation, jointly enhance the level of personal information protection, ensure the security and free circulation of information, and maintain the good order of global personal information protection. Through comprehensive measures, we will contribute to the protection of personal information and protect the rights and interests of the public.

7. Conclusion

In the environment of big data, the importance of personal information protection is becoming increasingly prominent. Personal information is not only an important part of personal privacy, but also an important resource in the era of digital economy. However, with the rapid development and application of big data technology, the risks of personal information leakage and abuse have also increased, bringing severe challenges to the security of personal information. Although some progress has been made in the regulation of personal information protection in China, there are still shortcomings. At present, the legal system of personal information protection is not perfect, and the means of legal regulation are relatively lagging behind, so it is difficult to effectively deal with the new challenges of personal information protection in the environment of big data. In addition, the awareness of personal information protection is insufficient, and the legal responsibilities and obligations of enterprises and individuals in the protection of personal information still need to be further clarified. In order to improve the legal system of personal information protection, it is suggested to strengthen the legislative work and formulate stricter and more comprehensive laws and regulations on the protection of personal information. At the same time, we should improve the application level of technical means in the protection of personal information, strengthen international cooperation and coordination, and jointly deal with the legal challenges of transnational personal information protection. Looking forward to the future, China's personal information protection legal system will continue to improve, to provide a more solid legal guarantee for personal information security.

References

[1] Huang Henglin. The establishment of civil public interest litigation [J]. Legal system and Social Development, 2024,30 (02): 104-124.
[2] Dou Xiaodong. Risk and Control: On personal Information protection for generative AI applications [J]. Political and Legal Theory Series, 2023, (04): 59-68.
[3] Zhao Peng. "Risk-based" personal information protection?[J]. The Law Review, 2023,41(04):123-136. DOI:10.13415/j.cnki.fxpl. 2023.04.010.
[4] Wang Yan, Duan Chengge. Research on privacy data protection of users' personal information based on big data technology [J]. Intelligence Science, 2023,41(07):100-105.DOI:10.13833/j.issn.1007-7634.2023.07.012.
[5] Meng Xiaoyang, Feng Bobo. On personal information protection in the information society: dilemma and failure [J]. Technology and Law (Chinese and English), 2022,(05):27-34.DOI:10.19685/j.cnki.cn11-2922/n. 2022.05. 004.
[6] He Wei. Research on the Challenges and Countermeasures of Personal Information Protection in the Era of Big Data [J]. Intelligence Science, 2022,40(06):132-140.DOI:10.13833/j.issn.1007-7634.2022.06.017.