Economics, Law and Policy
ISSN 2576-2060 (Print) ISSN 2576-2052 (Online)
Vol. 7, No. 3, 2024
www.scholink.org/ojs/index.php/elp

Original Paper

Civil Law Protection of Personal Information in the Digital Age

Yi Zhang[1]

[1] Dalian Ocean University, Dalian 116023, Liaoning, China

Received: December 10, 2024 Accepted: December 30, 2024 Online Published: December 31, 2024

doi:10.22158/elp.v7n3p206 URL: http://dx.doi.org/10.22158/elp.v7n3p206

Abstract

With the advent of the digital age, the collection, use, and dissemination of personal information have undergone profound changes, while also giving rise to increasingly serious security issues. Emerging digital and information technologies not only bring convenience to life but also pose new challenges to the security of citizens' personal information. The phenomenon of excessive collection and abuse of personal information occurs frequently in reality. Although our country has regulated this through legislation in various aspects, the public's awareness of the protection of personal information under private law has not yet fully awakened. The introduction of the Civil Code of the People's Republic of China signifies a new height of emphasis on the protection of personal information at the legal level in our country. Taking this as an opportunity, this article focuses on the Personal Information Protection Law, discusses the current situation of personal information protection under the existing legal framework in our country, analyzes the various difficulties faced in current judicial practice, and proposes suggestions and paths for improvement. This not only helps to enhance the public's understanding of personal information rights but also provides theoretical support for building a more sound legal protection system.

Keywords

personal information, Civil law protection, digital age

1. Definition and Classification of Personal Information

Article 4 of the Personal Information Protection Law of our country stipulates that personal information refers to all kinds of information related to identified or identifiable natural persons recorded in electronic or other forms, excluding information that has been anonymized. It can be seen from the legal provision that personal information possesses the characteristics of identifiability and recordability.

According to Article 27 of the Personal Information Protection Law, personal information processors may process personal information that individuals have voluntarily disclosed or has already been legally disclosed within a reasonable scope; except when individuals explicitly refuse. When personal information processors process publicly disclosed personal information and it has a significant impact on individual rights and interests, they shall obtain individual consent in accordance with this law. Personal information can be categorized into publicly disclosed personal information and non-publicly disclosed personal information. Publicly disclosed personal information should possess stronger public nature and stronger attributes of public interest compared to non-publicly disclosed personal information.

According to Article 28 of the Personal Information Protection Law, "sensitive personal information" refers to the information that is likely to lead to the natural person once it is leaked or illegally used dignity of human personality. Those who have been harmed or whose personal or property safety has been endangered personal information, include Biometrics, religion Specific identity, health care, financial account, location tracking and other information, as well as those under the age of 14 juveniles Personal information is also subject to stricter rules for processing sensitive personal information, which can be classified as sensitive personal information and general personal information.

2. The Legal Nature of Personal Information

Regarding the attributes of personal information in civil law, there are two main perspectives: the civil rights theory and the civil interests theory. Concerning the legal attributes of personal information, there are two primary viewpoints: one posits that personal information constitutes an independent civil right, emphasizing that individuals have direct control over their information akin to property or personality rights; the other viewpoint views it as a civil interest, arguing that personal information itself does not constitute a specific right but is protected through a series of related interests (such as the right to informed consent, access, correction, deletion, etc.), which are regulated by laws and regulations such as the Civil Code of the People's Republic of China and the Personal Information Protection Law of the People's Republic of China. Despite these differences, the current legal framework tends to regard personal information as a civil interest requiring special protection rather than an independent specific civil right.

Personal information is an entitlement that should be protected. Although there has been a dispute between rights and entitlements over the legal attributes of personal information, both the right theory and the entitlement theory undoubtedly believe that personal information should be protected.

3. Legal Provisions on the Protection of Personal Information

The process of bringing “personal information” into the legal protection framework in our country has been a long one. Before the promulgation of the Personal Information Protection Law, the protection of personal information was scattered across various laws, involving both public law and private law. Regulations concerning personal information were found in multiple laws, but there was no specific and detailed provision. Since 2017, our country has continuously explored and successively enacted the Cyber security Law, the Civil Code, the Data Security Law, and the Personal Information Protection Law, gradually forming a relatively complete legal system for personal information protection, basically achieving that personal information protection is now supported by law.

The Criminal Law Amendment (V) enacted in 2005 added the crime of “stealing, purchasing, or illegally providing credit card information”, which clearly categorizes credit card information as a type of personal information. The Criminal Law Amendment (VII) was the first to explicitly stipulate the crimes of infringing on citizens personal information and selling or illegally providing citizens personal information, specifying that acts of obtaining personal information through theft or other means would be subject to criminal punishment. However, the regulation did not clearly define how to determine personal information.

The Civil Code, which came into effect on January 1, 2021, for the first time dedicated a chapter and section to personal information, stipulating in Article 1034 that personal information of natural persons is protected by law; Article 1034s definition of personal information adds content such as “email addresses, health information, location tracking information” based on the Cyber security Law. The Civil Code further standardizes the definition of “personal information”.

According to the provisions of Consumer Rights Protection Law, operators who cause damage to individuals information rights due to their own faults must bear corresponding legal responsibilities, which include but are not limited to making an apology, restoring the victims reputation, eliminating related negative impacts, and providing material compensation for losses. Based on the specific content of this provision, it stipulates the civil liability for personal rights violations suffered by consumers, where civil liability can be understood as tort liability.

The Data Security Law of the People’s Republic of China emphasizes the overall security concept and provides comprehensive protection for national interests, public interests and the legitimate rights and interests of individuals and organizations. The Data Security Law of the People’s Republic of China and other laws have adopted a protective attitude towards data, but most of them are designed with individuals as the radiation center.

The “Cyber security Law of the People’s Republic of China” is a foundational law primarily addressing comprehensive norms for network information at the network level and issues concerning cyber security management in cyberspace. It also dedicates a special chapter to network information security, which is mainly manifested as personal information security. Chapter Three of Cyber security Law stipulates the obligations of network operators (especially those operating critical infrastructure).

Articles 41-45 of the "Cyber Security Law" specify the protection of citizens (consumers) personal information. Before the Personal Information Protection Law was enacted, the actions of network operators were mainly guided by the provisions of the "Cyber Security Law".

Personal Information Protection Law provides comprehensive regulations on the protection of personal information specifying the rights enjoyed by information subjects the obligations that information processors should abide by and the responsibilities that information processors should bear in case of infringement.

4. The Current Situation of Civil Law Protection of Personal Information

Searching for documents on the China Judgments Online with keywords such as "personal information", "civil cases", and "judgments", a total of 125, 050 documents were retrieved. From the data of cases related to personal information, it is evident that the number of documents concerning personal information has generally remained at a high level. Further organization of the documents reveals that the types of information infringed upon are diverse, covering extensive personal information such as names, phone numbers, and travel trajectories. The infringing entities include both natural persons and non-natural persons, such as legal entities or unincorporated organizations. Compared to non-natural person infringement cases, natural person infringement cases are fewer in number. Additionally, personal information civil disputes exhibit a characteristic where very few cases involve the full support of all information subjects. The Personal Information Protection Law, enacted in 2021, is first specialized law to systematically regulate personal information protection, providing clear guidelines for personal information protection and offering a basis for personal information processors. This law promotes the protection of personal information while also ensuring its reasonable use, responding to the needs of people's better lives in the digital age and providing legal guarantees for the healthy development of the digital economy. Since its implementation over a year ago, the Peoples Courts have increasingly emphasized the protection of personal information in civil judicial decisions. The rules of the protection of the judges are also increasingly clear, fully reflecting the characteristics of protecting the legitimate rights and interests of the people in the digital era and taking into account the healthy development of the digital economy.

5. The Dilemma of Civil Law Protection of Personal Information

5.1 The "Informed Consent" Rule Is a Formality

The "Informed Consent" principle is one of the core principles in personal information processing and also an important barrier for protecting personal information security. According to Article 14 of Personal Information Protection Law, processing personal information must be based on the individuals consent, and such consent should be voluntarily and explicitly given by the individual after fully understanding the specific circumstances of information processing. In practical applications, this principle is mainly reflected in the user agreements and privacy policies of internet services and

applications (APPs).

However, in practice, many user agreements and privacy policies are often lengthy and complex in language, failing to provide prominent prompts or simplified explanations for key clauses involving personal information. This makes it difficult for ordinary users to fully understand their content within a short period, leading them to potentially not read these terms carefully. Moreover, in many cases, users cannot use the application if they do not accept the privacy policy. This results in situations where information subjects are forced to agree to use the software. The ubiquitous “agree” button clearly does not necessarily mean meaningful consent, as few people read the terms before reflexively “agreeing” to them, yet courts still enforce these terms. To ensure the autonomous choice of information subjects and achieve substantive justice, it is necessary to provide more effective institutional safeguards.

5.2 The Dilemma of Information Subjects Personal Information Protection Awareness

The difficulties in improving citizen’s awareness of personal information protection mainly include the following aspects:

Many citizens lack sufficient understanding of the definition, value, and potential risks associated with the leakage of personal information. They may not know which information qualifies as sensitive personal information or the consequences that could arise if such information is misused. With the advancement of information technology, the technical means for protecting personal information have become increasingly sophisticated. Common citizens struggle to comprehend specialized terms and technical measures such as encryption and anonymization, making it difficult for them to implement effective self-protection measures in their daily lives. Although countries have enacted relevant laws and regulations to protect personal information, ordinary citizens often have limited knowledge about these laws and their own rights, and are unsure how to assert their interests when faced with personal information violations. Some citizens may overlook the importance of personal information protection due to trust in the government or businesses. For example, when online service providers request excessive personal information from users, users may not question its necessity and security.

In order to obtain a more convenient service experience, some citizens are willing to sacrifice a certain amount of privacy. For example, they agree to the application to obtain location information in order to enjoy personalized recommendations, but they do not fully consider the potential security risks.

Although efforts are being made across society to strengthen the promotion and education of personal information protection, there are still shortcomings in terms of breadth and depth. Especially in rural areas and among the elderly population, the dissemination of relevant information is more limited. In some cases, social trends can also influence individual behavioral choices. If those around do not prioritize personal information protection, individuals may also be affected and become complacent. In the face of rapidly evolving information technology, existing protective measures and strategies sometimes appear outdated and unable to promptly address new threats and challenges.

To overcome the above difficulties, it is necessary for the government, enterprises and all sectors of society to make joint efforts to improve citizens awareness of personal information protection through legislation improvement, technological innovation, public education and other ways.

5.3 The Relief of Personal Information Protection Is Not Perfect

In our country, civil compensation has always adopted the principle of making up for losses. When protecting against group personal information infringement cases under the Civil Code, the traditional principle of "compensatory damages" is still applied. Article 1182 of the Civil Code stipulates that if an act infringes upon another persons personal rights and causes property loss, compensation shall be provided according to the loss suffered by the victim or the profit gained by the infringer; if it is difficult to determine the loss suffered by the victim or the profit gained by the infringer, and if the victim and the infringer fail to reach an agreement on the compensation amount, the Peoples Court shall determine the compensation amount based on the actual circumstances when the case is brought to court.

Article 69 of the Personal Information Protection Law stipulates that when processing personal information, if there is an infringement of personal information rights and the processor of such information fails to prove its innocence, it shall bear civil liabilities such as compensation for damages. The amount of compensation shall be determined based on the losses suffered by the victim and the benefits gained by the infringer. Overall, there are indeed specific provisions for tortious acts in the field of personal information to ensure the protection of personal information rights. Of course, the amount of compensation for damages is determined according to actual losses or the benefits obtained by the tortfeasor. However, in practice, due to the concealment and complexity of personal information infringement acts, as well as the difficulty in quantifying losses, the existing civil liability compensation system may not be sufficient to effectively curb the increase in such infringements. With the development of big data and technological advancements, the number and complexity of personal information infringement cases are increasing, and the existing compensation system may need further improvement to better adapt to new challenges and provide more effective legal protection.

6. Improvement of Civil Law Protection of Personal Information

6.1 The "Informed Consent" Rule Is Refined

Faced with the challenges posed by the rapid development of data technology to personal data protection, the limitations of the traditional informed consent model are becoming increasingly evident, primarily manifested in the one-time and broad consent authorization made by information subjects before the start of information processing activities, which makes it difficult to adapt to the diversity and dynamic changes in information processing activities. To address this issue, a multi-level and dynamic consent system should be established to balance the protection of personal information rights with the need for the reasonable use of personal data to promote social development.

In the Internet era, how to identify unauthorized and beyond authorization determines the scope of control and utilization of data by information processors. The traditional informed consent model involves the information subject expressing their intention before the information processing activity begins, with the scope of authorization often limited to the processing purposes predefined by the information processor before the activity starts, making it difficult to cover various future information processing activities. In practice, the privacy policies provided by information processors are often overly lengthy and obscure, leaving users with little patience for a thorough read. Instead, users tend to simply click the agree button to quickly obtain the desired services, leading to relatively weak practical effectiveness of privacy policies. This phenomenon makes privacy policies seem more about meeting legal requirements rather than being genuinely designed for human users. For users, they often lack comprehensive understanding of personal information processing and true control over how their information is collected, used, and shared. This model struggles to adapt to the characteristics of multiple and multi-platform information processing activities, thus requiring the establishment of a continuous dynamic consent mechanism that allows data subjects consent to be extended within a certain time frame, thereby reducing the burden on both information processors and users. To address the varying levels of personal information privacy, a differentiated processing and authorization mechanism should be implemented based on the sensitivity of the information. For highly sensitive personal information, the validity period of consent authorization should be relatively shortened to ensure that users can more frequently review and control the use of their data. The existence of one-time consent authorization often stems from the asymmetry of understanding between the information subject and the processor regarding information processing activities. To address this issue, it is necessary to strengthen the information subjects right to know. Information processors should notify users of any changes in data processing methods or scope in a reasonable and clear manner during the processing, allowing users to track the use of their data throughout the process. At the same time, the notification method should focus on effectiveness, avoiding overly frequent or complex content, instead providing users with a selectable and customizable range of options through simplification and filtering, enabling users to independently decide which data changes and processing activities they are concerned about. This dynamic and hierarchical consent mechanism not only enhances user control but also promotes transparency and trust in information processing.

For the content and form of information disclosure, methods that sufficiently attract the attention of the subject and are convenient for viewing at any time should be adopted. For key and less understandable clauses, the information should be conveyed using language that is easy for the information subject to understand and in simple terms. The privacy policy should be presented in a user-centered manner, adopting more concise and easily understandable formats. The privacy policy should focus on user experience, using clear and straightforward language to avoid the use of professional or legal jargon, ensuring that users can fully understand the personal information processing matters involved.

In addition, to increase users' attention to privacy policies, some recommendations include providing summaries or key points, as well as using charts or images to present information. Information subjects have the right to real-time updates of their personal information data, and information processors should provide adequate technical means for real-time management of personal data, updating authorization scopes and times, withdrawal, and deletion of personal data. Whether it is continuous data disclosure or the practical application of dynamic consent, a platform that facilitates good communication is required. Information processors should establish communication platforms for implementing the above information subject rights, promoting continuous interaction between information processors and information subjects, to achieve a dynamically designed consent mechanism with hierarchical design, strengthening the legal responsibility of information processors. Improving the design of privacy policies is a complex task that requires balancing legal requirements, user expectations, and the actual operations of information processors. Future development requires joint efforts from all parties to continuously explore more humane and effective privacy policy models to ensure better protection of users' personal information.

Improving the traditional informed consent model and shifting towards a more flexible, user-friendly multi-level dynamic consent system not only helps enhance the level of personal information protection but also promotes the rational use of data and social progress. This requires the joint efforts of legislative bodies, regulatory agencies, information processors, and technology developers to explore a new path that aligns with contemporary characteristics while balancing the interests of all parties. Through such reforms, we can look forward to a safer, more transparent, and more personalized digital world.

6.2 Improve the Information Protection Awareness of Information Subjects

To enhance public awareness of personal information protection the key lies in strengthening individuals understanding of the importance of information protection and ensuring they are aware of and can utilize relevant laws and regulations. By consciously taking protective measures in daily life the risk of personal information leakage can be effectively prevented. Strengthening information protection education and management at the individual level not only helps reduce the exposure of personal information on big data platforms but also improves the overall efficiency of information protection thereby achieving comprehensive information management.

Strengthen the promotion of laws and regulations such as the Personal Information Protection Law to ensure that the public understands their rights and knows how to legally protect their interests. By releasing typical cases, especially those involving personal information leaks, remind the public to be aware of potential risks and enhance legal awareness. Encourage the public to form good information security habits in daily life, such as setting strong passwords, not clicking on suspicious links at will, and regularly updating software. Educate the public to carefully decide which information can be shared and which should be kept confidential in social networks, job applications, and other situations. Integrate personal information protection into school curricula to cultivate students' digital literacy and

personal information security awareness from a young age. Conduct various forms of training activities, including lectures, workshops, and online courses, tailored to different age groups and social populations, to help the public acquire necessary information security knowledge and skills. Urge enterprises and organizations to comply with personal information protection regulations, establish and improve internal management systems, and ensure the security of user data.

Require enterprises to maintain transparency when collecting and using personal information provide users with clear privacy policy explanations respect users right to know and choice Promote the use of secure and reliable technical tools such as authentication applications to offer the public more convenient and effective protection methods Utilize artificial intelligence and machine learning technologies to develop systems that can automatically detect and warn of personal information leakage risks helping users take timely response measures Continuously optimize and improve laws and regulations related to personal information protection clarify the responsibilities and obligations of all parties provide a solid legal foundation for personal information protection

Through the above measures, we can comprehensively improve people's awareness of personal information protection, so that everyone can become the first guardian of their own information, and at the same time promote the whole society to form a good atmosphere of paying attention to personal information protection, and finally realize the effective protection of personal information in the era of big data.

6.3 We Will Improve Remedies for the Protection of Personal Information

In cases where personal information has been significantly damaged, relying solely on protective laws for compensatory damages is no longer sufficient to meet current needs, and the most effective control measure is to avoid disclosing ones personal information without hindering normal behavior. Therefore, our country can introduce punitive damages to increase the cost of violations, making it an effective deterrent. Punitive damages refer to situations where the court determines that the compensation amount exceeds the actual harm caused by the infringement, serving as a form of punishment for the infringer. Punitive damages aim to compensate both the damages suffered by the victim and their property, thereby punishing malicious infringements and serving as a warning and educational tool. However, in civil matters, the compensation scope that information processors owe to individuals is limited to compensatory damages. Although Chinese law has not yet recognized punitive damages for personal information infringement, punitive damages are not a static or closed system, nor do they hinder discussions on the necessity, feasibility, and specific construction content and pathways of establishing a punitive damages system for personal information infringement from a legislative perspective. The punitive damages system for personal information infringement is an effective means to strengthen civil liability for personal information infringement, which helps to adjust the relationship between the victimized group and the infringer. The imbalance of public interest, the prevention of damage to personality rights, and the inhibition of large-scale infringement of personal information by victims "free-riding" are issues. Punitive damages originate from the United States and are mainly

applicable to intentional torts, aggravated negligence (gross negligence or recklessness), and strict liability. In addition, Article 69, Paragraph 2 of the Personal Information Protection Law itself implicitly includes the application of punitive damages, as the benefits obtained by personal information processors may exceed the property loss and mental distress suffered by the information subjects, with the excess being considered as punitive damages. Introducing a punitive damages system in personal information protection has the following reasons: First, punitive damages have a deterrent and punishing effect. When the cost of illegal acts is significantly higher than the benefits gained from such acts, the violators will consider whether to commit illegal acts. Second, punitive damages can fill the compensation gap in damage claims. Not only do punitive damages not require proof of actual damage, but they also have the function of covering all amages caused by the infringement, effectively addressing the compensation gap in personal information infringement cases where damage is difficult to prove. In short, the punitive compensation system has the functions of compensation, punishment and education. It is necessary to expand its application to the field of personal credit information infringement. China should establish a punitive compensation system for personal information infringement.

7. Conclusions

In today's era of booming big data and internet economy, emerging digital and information technologies have brought convenience but also pose challenges to citizens' personal information security. In reality, situations where personal information is excessively collected and improperly used frequently occur. To address this issue, strengthening personal information protection in the field of civil law is particularly important.

The current Civil Code of the People's Republic of China and the Personal Information Protection Law, although providing a legal framework for personal information, may not be sufficiently detailed in specific provisions, leading to some ambiguity in practical application. Therefore, it is necessary for the legislative body to further refine relevant regulations to ensure that the law can more accurately guide practice, effectively protect personal information rights, and promote the healthy development of cyberspace.

Looking to the future, legislators and technical experts should attach importance to the protection of personal information and continuously optimize and improve laws and regulations. At the same time, with the advancement of technology, it is necessary to develop and apply more advanced technical means to strengthen the security protection of personal information. Through dual guarantees from law and technology, we can build a more robust and effective personal information protection system, thereby better serving the interests of the public.

References

Aaron, P., & Jason, S. (2022). *The End of Ownership: Property Rights Protection in the Digital Age* (J. W. Zhao, Tran.). Beijing: Peking University Press.

Gerhard, W. (2012). *The Future of Damages Law: Commercialization, Punitive Damages and Collective Damage* (C. F. Wang, Tran., p. 137). Beijing: China Legal Publishing House.

Zhang, H. R. (2022). Overlap and Coordination of Data Property and Data Security Law Protection. *Legal Application, 2022*(9), 83-95.

Zhu, G. X. (2022). An Investigation of the Punitive Damages System in the United States. *Comparative Law Research, 2022*(3), 152-168.