Inadequacy and Improvement of Legal Protection of Sensitive Personal Information

Zhangboyu Sun, Zixi Liu *

School of Law, Sichuan Agricultural University, Ya' an, 625014, China

Abstract. In the era of rapid development of big data, the problem of personal information leakage is widely concerned by the society. Among them, sensitive personal information related to the human dignity of natural persons or basic rights such as personal and property is more important. China introduced the Personal Information Protection Law in 2021 to improve the legal system of personal information protection in China, but due to the short development time of the relevant system for the protection of sensitive personal information, resulting in the legal protection of sensitive personal information faces serious challenges in practice, so it is especially important to improve the legal protection of sensitive personal information in China. Based on this, this paper firstly explains the concept and characteristics of sensitive personal information, then analyzes the shortcomings of the legal protection of sensitive personal information, and finally puts forward suggestions for improvement from different perspectives, including improving the principle of "informed consent", strengthening the supervision of industry self-regulation and improving the principle of imputation.

1 INTRODUCTION

With the booming development of the information age, big data technology has begun to penetrate into various industries, providing convenience to the development of various enterprises while there are also risks and loopholes. Then how to protect personal information, especially the more important and sensitive personal information has become a problem of this era. In order to solve this problem, China has introduced relevant laws to protect the personal information of citizens, the most representative of which is the Personal Information Protection Law, which came into effect on November 1, 2021. However, this law is only one year old, and the research on the legal protection of sensitive personal information in China is still in its initial stage.

In recent years, domestic scholars have conducted extensive research on the protection of sensitive personal information, and have achieved rich theoretical results. Wang Liming [1] believes that the handling of sensitive personal information should follow the rule of "specific purpose + separate consent", and also adopt the "scenario theory". Zhang Yong [2] believes that the protection of sensitive personal information should be strengthened and classified. He believes that the previous laws, such as the Personal Information Protection Law, should be used as a reference, and the acts, objects, scope and criminalization criteria of infringement of sensitive personal information should be specifically identified at the criminal law level. Xu Lei [3] and others analyzed the real problems of sensitive personal information protection by sorting out the current situation of sensitive personal information protection, and put forward reasonable suggestions for the improvement of sensitive personal information protection on this basis.

Based on this, this paper firstly elaborates the concept and characteristics of sensitive personal information, then analyzes the shortcomings of the current legal protection of sensitive personal information from three levels: the principle of "informed consent", industry self-regulation and the principle of imputation, and finally puts forward suggestions for improvement.

2 SENSITIVE PERSONAL INFORMATION

2.1 Concept

The concept of sensitive personal information first originated in Germany in the 1970s with the enactment of the Personal Information Protection Act. It defines it as "information that is subject to a risk of damage or discrimination against the individual concerned if it is disclosed." Our Civil Code only provides for private information and does not include the protection of sensitive personal information. However, as personal information leaks become more frequent, some scholars and legislators have found that certain unique personal information is highly sensitive to the information subject. Once leaked, such information can pose a great risk to the human dignity and property security of the information subject, and therefore needs to be treated differently from general personal information and also given stricter protection in legislation. Therefore the

* Corresponding author: 2225153328@qq.com

Personal Information Protection Law introduced in 2021 provides for them for the first time and sets out the rules for their handling in the form of a special chapter. The Personal Information Protection Law states that "Sensitive personal information is personal information that, if leaked or used illegally, could easily lead to the infringement of a natural person's human dignity or jeopardize the safety of his or her person or property, including biometric, religious beliefs, specific identity, medical and health, financial accounts, whereabouts and trajectories, as well as the personal information of minors under 14 years of age personal information."

2.2 Characteristics

First of all, sensitivity is the core characteristic of sensitive personal information, and the criteria for judging this characteristic are divided into the following two categories: "discrimination criteria" and "high risk to fundamental rights criteria". The "discrimination criterion" refers to sensitive personal information when the leakage or improper handling of the personal information of the information subject will lead to the unfair treatment of others. For example, the leakage of information on race and religion can lead to racial and religious discrimination, so this kind of information is listed as sensitive personal information in many countries. "High risk to basic rights" means that the illegal misuse of personal information will result in a high risk to basic rights such as personal and property rights of victims, for example, the leakage of financial account information of natural persons will lead to a great risk to citizens' property rights [4].

Second, sensitive personal information refers to the sensitive information of natural persons. From the perspective of comparative jurisprudence, the subjects protected by sensitive personal information in most countries are natural persons, and do not include legal persons or unincorporated organizations, and the same is stipulated in our country. This is also because the purpose of protecting sensitive personal information is to protect the human dignity and personal safety of natural persons, who are the only ones with human dignity and personal safety.

Finally, sensitive personal information must also be identifiable. Identifiability means that the personal information can be analyzed and processed to directly identify a specific natural person. The former means that the information can directly identify a specific natural person, such as biometric information; the latter means that the information cannot be directly identified and must be combined with other information to identify a specific natural person.

3 INADEQUACY OF LEGAL PROTECTION OF SENSITIVE PERSONAL INFORMATION

3.1 "Informed consent" principle

In practice, although the operators of many APPs will inform the right holder of the collection and processing of sensitive personal information, they do not give the user the right to choose. When users choose to refuse, the app will often be forced to quit, resulting in the inability to use. This shows that the principle of "informed consent" has failed to work, and in practice, this principle does not provide users with the right to know and the right to choose in the true sense, nor is it conducive to the reasonable and lawful collection and processing of users' personal information by enterprises [5]. For their part, users do not have the interest, time, or energy to understand the privacy policies provided by companies, and most of them do not have the ability to understand sensitive personal information. For the obscure privacy policies provided by companies, many users may not understand the legal implications even if they want to read them, so the right to know and the right to choose given by the "informed consent" principle is meaningless [6]. As far as enterprises are concerned, the "informed consent" principle may bring excessive warning to some users who value the protection of sensitive personal information and refuse to collect sensitive personal information from enterprises. Under normal circumstances, the collection of sensitive personal information will bring users a better service experience, such as personalized recommendations, without posing any risk to their rights and interests.

3.2 Industry Self-Regulation

The Personal Information Protection Law stipulates that before collecting users' personal information, organizations shall inform the information subject of the handling and use of their information, and requires that the consent of the person concerned be separately obtained and informed of the purpose and necessity when collecting sensitive personal information. The so-called separate consent, in addition to the relevant provisions of Article 14(1) of the Personal Information Protection Law, shall be voluntary and clearly made with full knowledge, which means that the processor must distinguish sensitive personal information from general personal information, and is also required to separately inform and obtain the consent of the user when handling sensitive personal information. However, this provision is null and void for some network operators, and it is not uncommon for some companies to sell sensitive personal information as a commodity in order to make profits. This shows that China's industry self-regulatory system on the protection of sensitive personal information has not developed mature, and the Internet industry has not played an internal regulatory role.

3.3 Principles of imputation

The principles of imputation of fault for torts in the Civil Code include the principle of fault, the principle of presumption of fault, and the principle of no-fault. The Personal Information Protection Law uses the principle of presumption of fault for the imputation of damages for general personal information and sensitive personal information, which makes it difficult to reflect the special protection for sensitive personal information [7]. The author believes that sensitive personal information should be treated differently and a more severe imputation method should be adopted to protect it.

4 IMPROVE THE LEGAL PROTECTION OF SENSITIVE PERSONAL INFORMATION

4.1 Improving the principle of "informed consent

As the sensitivity of sensitive personal information is related to the scenario of handling information in real time, the principle of "informed consent" for sensitive personal information should be specific to the specific scenario of handling information. The author believes that the principle of "informed consent" needs to break through the traditional static framework and adopt a scenario-based and dynamic model to strengthen the protection of sensitive personal information [8].

Although the Personal Information Protection Law establishes the obligation to inform information processors, under the traditional framework of "informed consent", the legislator does not pay enough attention to the disclosure of sensitive personal information in the process of processing, which results in the obligation to inform performed by information processors is usually one-time. The right holder is not informed of the handling of sensitive personal information in real time and is unable to know whether the handling of sensitive personal information is risky in the first place. Therefore, the legislator should strengthen the "notification" mode of sensitive personal information and establish a sustainable information disclosure system, requiring the information processor to continuously inform the information subject of the subsequent process of handling sensitive personal information and the possible risks after the first notification obligation has been fulfilled. In this way, we can fully guarantee the information subject's right to be highly informed of his or her sensitive personal information, and thus increase the information subject's control over his or her sensitive personal information [9]. In addition, privacy terms issued by information processors are wordy, complex, and not easy to understand, and terminology, such as user profiles and algorithmic procedures, are frequently found in their form terms. Therefore, when making information disclosure, information processors need to clearly inform information subjects which of their important information is handled, and use simple and easy-to-understand language, as well as special ways to make information subjects fully understand the handling of their sensitive personal information, such as informing rights holders by means of video explanations. For specialized terms or information that is prone to ambiguity, information processors should provide special links to explain them so that information subjects fully understand the purpose and meaning of the processing activities.

4.2 Strengthen the supervision of industry self-regulation

The healthy development of any industry is inseparable from supervision, and the supervision of the industry self-regulation model concerning sensitive personal information must be strengthened for its long-term development. First of all, the legislature should improve the industry self-regulation standards, and clarify the way of reward and punishment, so that the prior protection of sensitive personal information can be improved on the basis of clear rewards and punishments. Secondly, the internal supervision of industry self-regulation should be strengthened. The supervisory role played by the government is mainly to macro-regulate the market, and it is impossible to monitor the internal information of the industry in real time. Therefore, the establishment of a supervisory department within the industry self-regulatory organization can provide real-time supervision of enterprises in the industry, thus improving the overall quality of the industry and strengthening the protection of sensitive personal information. Finally, the government should encourage the people to monitor the illegal acts of enterprises infringing on sensitive personal information. The government can establish incentives for effective reporting, and after receiving reports from the public and verifying them correctly, give certain rewards to citizens, thus promoting the protection of sensitive personal information.

4.3 Improve the principle of attribution of responsibility

The author believes that the principle of no-fault should be applied when dealing with infringement cases concerning sensitive personal information, while the principle of presumption of fault should be applied when dealing with infringement cases concerning general personal information. The specific reasons are as follows. First, the handling of sensitive personal information is highly dangerous at the legal level, and due to the special nature of sensitive personal information, the legal interests involved are significant legal interests related to the human dignity, health, and property of natural persons, etc. The possibility of danger in handling sensitive personal information is significantly higher than that in handling general personal information, so in principle, it should be prohibited for those who handle sensitive personal information to handling, but exceptions are allowed for sensitive personal information in order to protect higher legal interests, such as public safety, medical safety, national security, and other legal interests, so the processor should be held more strictly

liable [10]. Second, the establishment of the principle of no-fault tort damage for sensitive personal information will greatly increase the possibility of winning lawsuits for sensitive information subjects, and will also increase the cost of illegal handling and collection of sensitive personal information by information handlers, forming an economic barrier, which makes information handlers dare not to easily infringe such information.

5 CONCLUSION

In the era of big data, the rapid development of information technology brings many risks to the protection of sensitive personal information, and the characteristics of sensitive personal information determine the necessity of its protection. 2021's Personal Information Protection Law established sensitive personal information for the first time at the legislative level and provided rules for its handling in a special section, which is undoubtedly a very milestone step, but its provisions on sensitive personal information However, the regulations on sensitive personal information are not perfect to deal with the risks arising from the handling of sensitive personal information by enterprises in practice. Although the construction of a legal system for sensitive personal information cannot abandon the framework of the legal system for general personal information, it is necessary to achieve legal protection that is different from that of general personal information. It is hoped that this paper can bring theoretical reference value for the subsequent research of scholars.

REFERENCES

1. Liming Wang. Basic Issues of Sensitive Personal Information Protection - Against the Background of the Interpretation of the Civil Code and the Personal Information Protection Act [J]. Contemporary Law Review, 2022,36(01):3-14.
2. Yong Zhang. Integrated Public-Private Law Protection of Sensitive Personal Information [J]. Oriental Law, 2022(01):66-78.
3. Lei Xu, Chun Liu. The practical dilemma of sensitive personal information protection and the way to break it [J]. Information Studies: Theory & Application, 2022, 45(03):42-49+41.
4. Ye Tian, Chenhui Zhang. On the Legal Protection of Sensitive Personal Information[J]. Henan Social Sciences, 2019,27(07):43-49.
5. Wei Fan. Reconstructing the path of personal information protection in the era of big data [J]. Global Law Review,2016,38(05):92-115.
6. Qing Lu. Normative structure of the "consent" rule in the protection of personal information[J].Wuhan University Journal(Philosophy & Social, 2019, 72(05): 119-129.
7. Dingyi Xiang. Typological analysis and differentiated protection of personal information [J]. Journal of Chongqing University of Posts and Telecommunications (Social Science Edition), 2017, 29(01):31-38.
8. Min Tang. The European and American experience of personal sensitive information protection and its inspiration[J]. Library Development,2018(02):41-47.
9. Xuzhi Han. Personal Information Typology Study[J]. Journal of Chongqing University of Posts and Telecommunications (Social Science Edition), 2017, 29(04): 64-70.
10. Yuan Ning.Legal Basis and Scope Definition of Sensitive Personal Information - Centered on Article 28(1) of the Personal Information Protection Law[J]. Journal of Comparative Law, 2021(05):33-49.