Science of Law Journal (2023)
Clausius Scientific Press, Canada

DOI: 10.23977/law.2023.020401
ISSN 2616-2296 Vol. 2 Num. 4

# *The Boundary and Protection Path of Personal Information and Privacy Right from the Perspective of Civil Code*

**Na Liang***

*Guangdong University of Finance & Economics, Guangzhou, 510320, China*
**Corresponding author*

***Keywords:*** Personal information, privacy, civil code, privateness

***Abstract:*** In the development of digital economy and intelligent governance, the promotion of universal informatization is inevitable, but it also brings about personal information protection issues. As the basic law of civil law, the Civil Code only establishes the basic principles and directions for the protection of personal information. Therefore, there is a need to refine "personal information", and then combine the experience of overseas personal information protection models to manage personal information in a hierarchical manner. Therefore, this paper suggests taking privacy as the judgment standard, distinguishing the boundary between privacy and personal information, further refining sensitive information and general information in personal information, applying different protection modes.

## 1. Introduction

In an era of data explosion, privacy and personal information are more easily compromised than ever before. We have given stricter protection to "privacy" and allowed "compliance use" for "personal information". Accordingly, some scholars suggest that the right to privacy should not be separated from the rights and interests of personal information, otherwise it will inevitably lead to the weakening of the protection of the latter, and personal information, like privacy, has the attribute of symbolizing the dignity of individuals, so that people cannot be treated as "cows" in the data era and disregard the dignity of human beings because of the resource attribute attached to personal information.[1] The author believes that some personal information is not related to dignity or personal image, but is only one of the links in the promotion of information technology to establish a better service system and communication system. If all personal information is raised to the same level of protection as privacy, it will stall the development of the Internet economy and the advancement of the smart governance model.

The question that arises is how to define the boundary between personal information rights and privacy? What is the best way to protect personal information in order not to hinder the process of economic and social development? This article will focus on these two questions, attempt to clarify the relationship between privacy rights and personal information protection in the context of the implementation of the Civil Code, and put forward relevant proposals for improving the personal information protection system.

## 2. The Boundary between Personal Information Interests and Privacy

### 2.1. Basic Attributes of Personal Information Interests and Privacy

First of all, privacy is an absolute right, and no one can violate the privacy of others. According to the expression of Chapter 6 "Privacy and Protection of Personal Information" of the Civil Code, personal information is not formally recognized as a right at the legal level in China. Secondly, privacy has a strong brand of personality rights and represents human dignity and freedom. In the process of collecting and utilizing personal information, property value is inevitably generated, so it has both personality and property attributes. Thirdly, in the implementation of the law, privacy is more of a negative right, the legislation does not make

Provisions on how to it. On the contrary, the exercise of personal information interests is more active. The subject has the right to inspect, copy, correct and delete. Finally, while privacy emphasizes undisclosed things, personal information interests has the additional property of public nature. For example, government departments can collect information on personal health status for public health needs.

### 2.2. Privateness is the Key Consideration in Distinguishing Personal Information from Privacy

The most critical factor in distinguishing personal information from privacy lies in determining whether the object is private or not. Other factors, such as whether it is a right or an interest, whether it is exercised in a positive or negative manner, and whether its protection is strict or lenient, are merely "acquired" differences arising from the different provisions of the law.

Whether there is privateness or not, the author thinks it should be judged from three aspects comprehensively: One is the attitude of the information subject. Second is the general public perception, customs and habits of the local community. The third is the possible adverse effects. The average person rarely voluntarily discloses his or her privacy to unspecified others, but the public is far less concerned about personal information than privacy. For example, only a small percentage of people will erase personal information after the delivery is received. All personality rights and interests cannot be separated from the influence of social perceptions, so whether they are private or not cannot be based on the subjective judgment of individuals alone, but must also be combined with the degree of awareness of the general public in society. We should learn from the experience of overseas legislation and exclude collection information, government public information, credit information, driver information, etc. from the protection of privacy. [2] People living in different countries and regions have different attitudes toward privacy due to historical traditions and customs. For those regions that are relatively conservative, the protection of privacy can be appropriately increased to meet the needs of the public. On the contrary, the requirements can be relaxed appropriately. Privacy is about secrets that the person does not want others to know, and these secrets may be different from public values, so if privacy is exposed, there is a high probability that it will cause serious damage to the person. And there are not many factors in personal information left for people to judge the value of, and the problems brought by information leakage are mostly the receipt of advertisements, fraudulent messages and so on.

## 3. Future Outlook of Personal Information Protection System

After distinguishing "personal information" from "privacy" by" Privateness", we are able to analyze the advantages, disadvantages and improvements of the existing personal information protection system in China.

Needless to say, with the introduction of the Civil Code and the Personal Information Protection

Law, China has made some improvements effective in protecting the information rights of natural persons and facilitating the digital economy. However, at the same time, there are still problems such as incomplete claims, unclear models of interest protection, difficulty in proving and difficult determination of damages. [3]

### 3.1. Privacy and Personal Information Interests in the Civil Code

Article 1034, paragraph 3 of the Civil Code stipulates that "private information" in personal information is in principle subject to the provisions of the right to privacy, and that the provisions on the protection of personal information are applicable only if the right to privacy is not provided for. However, the legislation does not give clear guidelines on the criteria for determining privacy.

Article 1035 of the Civil Code emphasizes the procedural rules that should be followed in handling personal information around the principles of legality, legitimacy, and necessity. The specific application of the principle of lawfulness and legitimacy is reflected in the law, while the principle of necessity needs further elaboration. The author believes that the principle of necessity is similar to the "principle of proportionality" in administrative law, that is, information should be handled in a way that achieves the purpose and has the least impact on the parties.[4]

Article 1038, paragraph 1 of the Civil Code implies that information processors may provide personal information of natural persons to others without the consent of the person concerned, after concealing key information. However, automated processing technology that can store a large amount of pre-collected personal information in a database, and identify and analyze individuals by integrating various pieces of personal information, thus creating an uncertain risk of infringement of their personal and property rights. [5] Therefore, the provision that "The use of personal information that cannot be identified after processing is permitted" needs to be expanded in the legislation or judicial interpretation to prevent significant leakage of personal information and privacy due to reverse identification technology.

### 3.2. Judicial STATUS of Personal Information Protection in China

The author concluded through case search analysis that the following problems exist in the current judicial cases of personal information protection in China: On the one hand, there are some deviations in the understanding and application of the law. Only acts reasonably performed in the public interest or in the legitimate interest of that natural person are exempt from liability in accordance with the circumstances covered by Article 1036, paragraph 3, of the Civil Code. For example, although extramarital affairs violate public order and morals, but the massive dissemination of the plaintiff's personal information on the network is also not reasonable, and therefore cannot be a cause of exclusion for the defendant. On the other hand, excessive emphasis is placed on the probative power of evidence, while ignoring the fact that in the protection of personal information, as the loss is usually intangible personality interest or the impact is long-term and latent, it is difficult for the plaintiff to provide corresponding evidence to prove the result of damage. If the plaintiff's burden of proof is not properly adjusted, it will be detrimental to the substantive fairness of the case. Last but not the least, the standard of adjudication is not uniform from one court to another. Some courts are very strict about the probative value of the evidence and will rule against the plaintiff's claim if the party cannot provide the appropriate evidence or the evidence provided is insufficient to prove the damages caused. And some courts will be in accordance with the specific circumstances of the case, combined with the actual, even if the plaintiff does not have sufficient evidence, will also support the plaintiff's request for compensation at their discretion.

### 3.3. Extraterritorial Experience in Personal Information Protection

On the above issues, countries such as Europe and the United States provide relevant legislation and judicial experience.

On May 25, 2018, the EU officially imposed its General Data Protection Regulation ("GDPR"). "Special categories of personal data" (private information) are explicitly listed in Article 9(1) of the GDPR. This includes data on individuals who indicate racial or ethnic background, political affiliation, religious or philosophical beliefs or trade union membership, genetic data, biometric data for the purpose of specifically identifying natural persons, and data relating to a natural person's health, personal sex life or sexual orientation.

Regarding the necessary limits for processing information, Article 11 of the European Convention on Human Rights and Fundamental Freedoms stipulates that data enterprises must clearly inform and justify the purpose, use, and necessity of the data flow, and are not allowed to arbitrarily change the original purpose or use, exceed their authority, or induce individuals to authorize the flow of data, except by regaining explicit permission.

In addition, regarding the problems of infringement determination, the GDPR strictly reinforces the relevant obligations of information processors, especially with regard to obtaining the consent of data subjects, requiring that such consent must be made of free will, specific, explicit and informed, and that data subjects have the right to withdraw their consent. At the same time, the GDPR requires data processors to be jointly and severally liable with data controllers, making it possible for information to be treated more carefully in the process of circulation. Given the insidious nature of personal information infringement and the difficulty of collecting evidence, data regulators in European countries also regularly check companies for data discrimination, algorithmic bias and other issues.

The California Consumer Privacy Act ("CCPA") adopts a new privacy framework and further refines the "scene rules" in light of the different reasonable expectations of privacy and personal information in different industries, geographies, and scenarios.[6] Under the thinking of "scene rules", there are two criteria for judging the reasonable use of privacy information: first, whether it meets the reasonable privacy expectations of users; second, whether it causes unreasonable privacy risks.[7]

To better address the difficulty of proving infringement due to unequal relationships in information processing, the Singapore Personal Data Protection Act ("PDPA ") provides that the Personal Data Commission may appoint a Data Protection Commissioner to assess data breaches and notify affected individuals. It may issue warnings and impose fines for violations such as unauthorized disclosure of personal data.

### 3.4. Improvement of the Path of Personal Information Protection in China

#### 3.4.1. Clarify the Protection Model Applicable to Personal Information and Privacy

The protection model applied to personal information and privacy includes two aspects, one is the delineation of the boundary between personal information and privacy, i.e., the issue of the determination of privacy. The second is the issue of regulating data that can be reverse-identified.

The latter of these objects is the gray area created by the impact of the digital revolution on the established public-private dichotomy of privacy protection mechanisms.

For the issue of privateness, it is possible to take the approach of GDPR and explicitly enumerate the cases that are private information in the judicial interpretation of the Civil Code. I tentatively drafted the article as follows: "The private information in Article 1033 of the Civil Code refers to information that directly reflects the dignity of the person concerned and does not want to be known

to others. This includes information related to physical health, sexual life, sexual orientation, marital history, family status, and education." In order to prevent the lag of the law and then add a bottom clause such as: "other information that is as private as the previous paragraph.

The regulation of the problem of reverse identification of information can be mainly focused on the following aspects: First of all, information processors should follow the principle of necessity at the source and collect as little identifiable information as possible. Secondly, enterprises shall not re-transfer data with the possibility of reverse identification, and shall not retain or reveal user data by re-identification or linking without authorization. Government agencies should clean up the collected data in a timely manner, except for the retention of data used for evidence collection and crime fighting.

### 3.4.2. Graded Management of Personal Information

There is a divergence in the sensitivity of the areas of privacy protection presented in different contexts such as education, healthcare, and social networking platforms. Therefore, specific guidelines can be given in the legislation and judicial discretion according to industry practices. Besides, in order to achieve a balance between personal information protection and industrial development, a graded and classified approach to personal information management should be implemented. The most strictly protected level is "private information". Moreover, those sensitive information in personal information such as ID numbers, which is second only to private information in importance, their protection should be strict too. The use of such information requires the prior consent of the person concerned, which can be withdrawn at any time, as well as the purpose and manner of using the information, and the information cannot be re-licensed to other parties without permission. In the event of disclosure of this information, the person handling and controlling the information is jointly and severally liable. For general information other than sensitive information, such as phone numbers, almost all APPs in daily life them, and the level of protection required for them is weaker than the first two. For the sake of efficiency, the information can be applied to the areas related to this service by means of a web-based form contract that allows people to check whether or not they agree to the terms of service by means of a notification.

### 3.4.3. Improve the Personal Information Infringement Recognition System

The following solutions can be adopted to address the difficulty of proving personal information cases: At first, the obligation to report infringer information should be added to the platform. Judicial organs, administrative organs and rights holders who provide relevant identification are entitled to request the platform to disclose information such as the name and network address of the infringer. Next, since it is impossible for users to propose amendments and changes to the Privacy Policy and User Agreement when they download the APP, they can only express their acceptance or non-acceptance in general, and there are indeed many unreasonable and unequal contents interspersed in these format terms. [8] Therefore, in order to prevent "informed consent" from becoming an excuse for abuse, there should be greater oversight of information processors, and companies should be required to reduce their reliance on the informed consent rule. Then, given that internet platforms manipulate individuals' privacy choices through a highly asymmetric information environment, and individuals are now not just being mined for data by the platforms, but are also incentivized and competing with each other to disclose privacy in exchange for various bonuses or to avoid disadvantages. [9] It is very necessary for companies to regularly conduct ethical assessments of their algorithms and report them to the authorities. Furthermore, it is possible to refer to the Singaporean practice of introducing third-party regulation and setting up organizations such as the Personal Data Protection Committee to collect evidence related to information leakage incidents, make timely

assessments of the resulting damage, and provide consulting services to relevant rights holders. At last, in order to achieve case-by-case balance and practical fairness in infringement cases, the requirement of the burden of proof on the right holder should be appropriately relaxed in cases where evidence is really difficult to collect.

Regarding the principle of attribution of liability for infringement of personal information and privacy, the author believes that it can be divided into two cases: For one thing, the principle of no-fault imputation should be applied to the situation where personal information is handled without the consent of the person concerned. This is because the handling of personal information without the consent of the natural person is extremely bad in nature, regardless of whether perpetrators is at fault or not. For another, the principle of presumption of fault should be adopted when an authorized information processor fails to fulfill its security obligations resulting in information leakage. Since the information processor is usually an Internet company with certain qualifications, it should have the corresponding information processing technology and understand the corresponding legal regulations. Therefore, except for the information processor who can prove that it is not at fault, it should bear the corresponding responsibility.

Regarding the scope of compensation for infringement of the rights and interests of personal information, in accordance with Article 69, paragraph 2 of the Personal Information Protection Law, the scope of compensation shall be determined in accordance with the loss of the person concerned or the benefit obtained by the information processor as a result, and other cases shall be determined in accordance with the actual situation. The author believes that this provision should be applied together with other provisions of the Civil Code. Since personal information interests belong to the category of personality rights, the person concerned may request for moral damages from the information processor in accordance with the provisions of Article 1083 of the Civil Code. For the sake of fairness, the principle of offsetting fault should also be applied to the damages suffered by the parties. If the party is also responsible for the information leakage, the responsibility of the information processor can be reduced accordingly. In addition, the "predictability principle" of Article 584 of the Civil Code may be applied: the information processor is liable for damages up to the amount that it foresaw or should have foreseen at the time of the conclusion of the contract as a possible result of the breach. In case of fraud due to the leakage of telephone numbers, the information processor can hardly foresee this loss at the time of contracting and should not be liable. In order to maximize the compensation for the loss of the parties and increase the cost of violation, in addition to filling the losses of the parties, a punitive compensation system should be implemented for cases with particularly serious circumstances (wide dissemination and serious mental damage to the victims).

## 4. Conclusion

With the development of the digital economy, personal information is no longer just a derivative of personality, but has become an active factor of production with more and more property content attached to it. But at the same time, the need to protect personal information for the sake of a peaceful life is increasing day by day. Then, in order to balance both, it is necessary to achieve graded and precise protection of personal information based on the application of a differentiated approach. It is high time to use "privacy" as the standard to classify privacy and personal information, and then refine the distinction between "sensitive information" and "general information". It is also necessary to apply the principle of balance of interests in justice, and reasonably allocate the burden of proof and the scope of compensation to protect the relatively vulnerable information right holders. If we can take into account the dual needs of data circulation and information protection, then we can improve our country's governance capacity in the new development of the information age and manifest the

Chinese characteristics of common governance and sharing!

## References


*[1] J. W Zhang. (2021) Between Dignity and Resource, the Difficulty of Personal Information Privacy Test in the Age of China's Civil Code. Journal of Soochow University (Philosophy and Social Science Edition), 01, 62-72.*

*[2] Y Ren. (2021) Legal Structure and Rule Reconstruction of Privacy Protection in the Digital Age. Oriental Law, 02,188-200.*

*[3] Y. B Cai. (2021) Understanding and Judicial Response to Provisions on Personal Information under the Implementation of the Civil Code. Journal of Law Application, 03, 88-98.*

*[4] H Zhang. (2019) Frontier Research on the Right of Privacy Legislation. Social Scientist, 02, 7-21.*

*[5] J. W Zhang. S, Cheng. (2022). The Relationship between the Right of Privacy and Right of Interest of Personal Information under the Perspective of Personal Information Protection Law: with a focus on the Legal Application of Private Information. Journal of Soochow University (Philosophy and Social Science Edition) 01, 101-108.*

*[6] Daniel. J. Solove., A. Taxonomy of Privacy, (2006)154 University of Pennsylvania Review, 03, 477-564.*

*[7] S. K Fang, X. J Cao, (2019) On the Private Nature of Personality Interests under Personal Information. Law and Social Development, 04, 46-57.*

*[8] L. M Wang. X. D Ding. (2023) The Development and Improvement of Civil Law in Digital Age, Journal of the East China University of Politics & Law, 02, 6-21.*

*[9] C. F Yu. (2023) Reconstructing Social Theory of Privacy in the Digital Age, China Legal Science, 02, 169-188.*