

On the tort liability of personal information

Ziqian Cheng

Anhui University of Finance and Economics, China

How to cite this paper: Cheng, Z. Q. (2025). On the tort liability of personal information. *Law and Humanities*, 1(3), 1 - 11. ISSN Print: 3079-5117; ISSN Online: 3079-5125.

<https://doi.org/10.63313/LH.9020>

Published: 2025-07-03

Copyright © 2025 by author(s) and Erytis Publishing Limited.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Abstract

In recent years, the development of big data and other technologies has brought many convenient services to people's lives. However, the advent of the era of big data has prompted the continuous change and expansion of the scope of the concept of personal information. The concept of personal information is no longer a "pre" precise definition, but a dynamic judgment process. China's legislation and practice integrate these ideas and reshape the definition of the concept of personal information. The theoretical basis of the legislative model of personal information is the theory of identification, combined with the way of summary and illustration. At the same time, the rapid development of science and technology has also subverted the social scene established by the traditional tort law. The infringement cases of personal information are becoming more and more frequent, but the single application of the principle of fault imputation and the principle of no fault liability can not complete the mission of personal information relief. The author believes that we should establish a system of imputation principle of damage compensation liability with the coexistence of fault liability and fault presumption on the basis of learning from and absorbing foreign laws and according to our national conditions. In terms of the liability effect of personal information infringement, we should recognize the diversified liability methods, improve the compensatory liability methods, and the punitive compensation system should be more future oriented, so as to make the personal information infringement relief system in line with the development trend of the times.

Keywords

Personal information right; Elements of tort liability; Imputation principle; Responsibility bearing mode

1. Introduction

Personal information security has always been a topic of concern for all sectors of society. Statistics show that more than 70% of netizens have had their personal identity information leaked, including various types of private and sensitive information such as name, education, and home address... In 2015 alone, netizens suffered a total loss of about 80.5 billion yuan due to personal information leakage, spam, fraud, and other phenomena, with an average of about 124 yuan per person. [1]As for the daily express delivery sent and received by residents, there is a blind spot in the real name supervision of express delivery, and over 70% of netizens'

personal life information has been leaked. As early as the introduction of the real name system for express delivery, this system has sparked heated discussions from all sectors of society: on the one hand, the tragic and real cases have made people urgently call on the government to further strengthen the supervision of personal information; On the other hand, in response to the serious situation of personal information leakage in the current society, people are becoming more concerned about the security of personal information under the real name system of express delivery.

A citizen in Qinghai, who had just purchased a new house, faced a barrage of harassing phone calls from various decoration companies, but did not know where those companies obtained his phone information from. In real life, it is not uncommon for people to face such troubles. According to relevant research results, the scope of personal information leaked by netizens is very wide, with nearly 80% of netizens' personal identity information being leaked, including personal information such as ID numbers, work units, and company addresses; About 60% of netizens' personal online activity information has been leaked, including sensitive information such as usage records, IP addresses, software usage traces, and geographic locations. Nearly 85% of surveyed netizens believe that personal information leakage has had a significant impact on their normal production and life, indicating that personal information infringement has become a normalized problem in current society.

2. Organization of the Text

2.1. The Evolution of Personal Information Infringement

2.1.1. Theoretical Development of the Concept of Personal Information

The implementation of the Personal Information Protection Law is based on evaluating whether specific types of information are personal information. Only when specific information is considered personal information, will it be subject to the supervision and protection of the Personal Information Protection Law, and information subjects can enjoy the rights stipulated by law. Information processors or infringers will assume legal obligations. Therefore, the different definitions of the concept of personal information will directly affect the scope of personal information protection and the value orientation of legislation. It is necessary to address practical issues with clearer theories.[2]

The premise of studying the liability for personal information infringement is the definition of the term 'personal information'. The theoretical theories that define the concept of personal information mainly include identification theory, association theory, abolition of static concept theory, and new knowledge theory.

Identification theory is the earliest theory to define the concept of personal information, which divides personal information into personal information and non per-

sonal information, and defines personal information based on whether there is an objective and identifiable possibility between the information and the subject. However, this theory is sometimes limited to the types of personal information listed in legislation, which makes personal information protection inadequate; Sometimes, overemphasizing the role of technology and neglecting the legal significance of "identification" leads to the static nature of the concept of personal information. These two levels of issues can provide reference for China's personal information legislation. The National Institute of Standards and Technology in the United States has proposed the "association theory" in addition to the "identification theory". The association theory advocates the identification from information to individuals, that is, knowing or collecting other information about a specific individual, emphasizing the dynamic nature of the definition of personal information. With the advent of the big data era, the application of traditional information protection laws is also constantly changing. Especially with the development of information recognition technology, non personal information is gradually being identified as personal information, indicating that the attributes of personal information are highly dynamic. Abolishing the static concept theory indicates that the definition of the concept of personal information should be approached from a broader perspective and advocates that it should not be limited to the concept of personal information in the legal system. However, its drawback is that it cannot determine the scope of personal information protection laws. The new identification theory is developed on the basis of traditional identification theory, understanding personal information as a "spectrum", with one end being unidentifiable information, followed by indirect identification of personal information, and then direct identification of personal information.

From the above theory, the rapid development of science and technology has promoted the continuous change and expansion of the scope of the concept of personal information. International legislation and practice tend to define relevant rights and obligations based on dynamic risks in the context rather than static information types. [3]The concept of personal information is no longer a precise definition in advance, but a dynamic evaluation process. Chinese legislation and practice need to integrate these concepts and redefine the concept of personal information.

2.1.2. The legislative model of the concept of personal information in China

There is no unified legislation on personal information in our country, and we only rely on other laws, regulations, and judicial interpretations. Article 76 of the Cybersecurity Law promulgated in 2016 stipulates that "personal information refers to various types of information recorded in electronic or other ways that can be used alone or in combination with other information to identify the personal identity of a natural person, including but not limited to the name, date of birth, identification number, personal biometric information, address, telephone number, etc." Article 1

of the "Interpretation on Several Issues Concerning the Application of Law in Handling Criminal Cases of Infringement of Citizens' Personal Information" promulgated by the Supreme People's Court and the Supreme People's Procuratorate in 2017 further clarifies that "citizens' personal information" includes identification information and activity information. The term "personal information" refers to various types of information recorded electronically or in other ways that can identify a specific natural person's identity or reflect their activities, including name, ID number, communication and contact information, address, account password, property status, and whereabouts. Article 1034 of the Civil Code of the People's Republic of China clearly stipulates that "personal information is various types of information recorded electronically or in other ways that can identify a specific natural person individually or in combination with other information, including the name, date of birth, ID number, biometric information, address, telephone number, email address, health information, whereabouts information, etc. of a natural person. Information Protection Law Article 4 stipulates that "personal information refers to various types of information related to identified or identifiable natural persons that are recorded in electronic or other forms, excluding information that has been anonymized." From this, it can be seen that the theoretical basis of China's personal information legislation model is the identification theory, combined with a summary and illustrative approach.

2.2. Principle of Attribution of Liability for Personal Information Infringement

The principle of attribution of liability for infringement refers to the criteria and principles used to determine the tortfeasor's liability for infringement when their actions cause harm to others. The principle of attribution of liability for infringement is the core of the Tort Law, which determines important elements such as the constituent elements of tort liability. Studying the principle of attribution for personal information infringement is an unavoidable part of solving the problem of personal information infringement. [4]The author will analyze and compare the differences in the principles of attribution for personal information infringement between other countries and China, in order to better understand the attribution principles established in the current applicable personal information protection laws in China.

2.2.1. Extraterritorial reference to liability for personal information infringement

The European Union and the United States have established relatively complete personal information protection systems as early as the last century. The EU follows the legislative tradition of the civil law system and adopts a centralized and unified legislative model; The United States follows the legislative tradition of the Anglo American legal system and adopts a decentralized legislative model.

The formation of the EU's personal information protection model stems from the long-standing commodity economy structure in Europe. Article 23 of the 1995 EU Directive stipulates that the EU adopts the principle of no fault liability for the protection of personal information. The most stringent General Data Protection Regulation (GDPR) internationally not only strictly regulates the allocation of burden of proof for personal information and the way in which liability for damages is borne, but also re-establishes more rigorous regulations on the scope of personal information protection. From the perspective of burden of proof, Article 5 of GDPR does not require the infringing party to demonstrate subjective fault, as long as the information subject proves that the infringing party's handling of information was illegal or improper, resulting in certain harmful consequences. From the perspective of liability for infringement, GDPR not only applies the principle of no fault, but also further extends the scope of data protection accountability, establishing that when there are two or more infringing parties, they should bear joint and several liability. The establishment of this joint liability system makes it easier for citizens to hold themselves accountable. [5] From the perspective of personal information infringement liability, GDPR also stipulates the liability for property damage compensation. Overall, the EU still adopts the four elements theory for the composition of personal information infringement, but designates information managers as specific compensation subjects, and the traditional subjective fault elements are also replaced by specific subjects.

The regulations on personal information protection in the United States are scattered among legal provisions such as the Privacy Act and the Electronic Communications Privacy Act. The Privacy Act stipulates that the government and public institutions should apply the principle of no fault liability. The Freedom of Information Law stipulates that "regardless of other legal provisions, the defendant must provide a substantive response within 30 days after receiving the plaintiff's appeal." The Freedom of Information Law also stipulates that the plaintiff's legal fees should be reasonably borne by the losing party to balance the natural imbalance of material possession between the two parties in infringement cases. From the perspective of maximizing the protection of citizens' personal information rights and interests, this bill supplements the unequal status of citizens in infringement cases by increasing the responsibility of infringing parties and reducing the cost of citizen litigation. In legal practice, for specific cases of infringement of personal information, the first thing to consider is whether there are specialized regulations in a specific field. If there are special regulations, they shall be followed. If there are no special regulations, the principle of fault liability shall be applied in accordance with the provisions of general infringement.

2.2.2. Principles and improvement opinions on the attribution of liability for personal information infringement stipulated by Chinese laws

The EU and the US have adopted different legislative models and attribution princi-

ples for the protection of personal information, as mentioned earlier. The principle of no fault attribution adopted by the European Union and the United States has a clear and concise logic, and adopts a uniform approach to the issue of compensation for personal information infringement damages. However, the application of compensation for damages is relatively single, without distinguishing between compensation for damages and non damages or distinguishing between the means of handling the subject. [6]Our country's legislation has taken into account the complexity of issues such as information network entities, rights holders, and attribution reasons, and has conducted a balance of interests to develop reasonable standards for classifying the principles of compensation for personal information infringement damages. The Personal Information Protection Law combines the advantages of uniformity in the European Union and the United States, and takes into account the difficulty for victims to prove the elements of fault. It incorporates the principle of presumption of fault and provides a single provision for the subjective attribution principle of compensation for personal information infringement.

Article 69, Paragraph 1 of the Personal Information Protection Law stipulates: "If the processing of personal information infringes upon the rights and interests of personal information and causes damage, and the personal information processor cannot prove that they are not at fault, they shall bear the liability for damages and other infringement liabilities." This provision clarifies the principle of presumption of fault for compensation for personal information infringement damages, but it still cannot exclude fault from the constituent elements of the claim for compensation for personal information infringement damages.

The liability for compensation for infringement of personal information is distinguished according to different types of personal information, and different attribution principles are established. This provision is undoubtedly more comprehensive and specific. Standardizing it as fault liability would be detrimental to the legitimate rights and interests of natural persons, as in cases of infringement of personal information rights, natural persons often find it difficult to prove the fault of the perpetrator, and even to determine the specific perpetrator. However, it is not appropriate to classify it as a presumption of fault liability, as it does not reflect special protection for sensitive personal information. The appropriate approach should be to apply no fault liability for infringement compensation arising from the handling of sensitive information; The liability for infringement compensation arising from the handling of non sensitive personal information shall be subject to the presumption of fault liability. The reason for this is that sensitive information is related to significant legal interests such as the dignity of natural persons, so its handling behavior itself is a highly dangerous behavior in law. In principle, the handling of sensitive information should be prohibited, but exceptions should be made based on various higher interest needs. In this situation, the responsibility of the processor is heavier. Secondly, the processing of sensitive information objectively opens up

Pandora's box, and processors have the ability to control their processing behavior. Therefore, according to the requirements of danger opening theory and danger control theory, processors of sensitive information should also bear fault liability. Once again, applying fault liability to sensitive information infringement liability will also increase the cost of processing sensitive personal information, making it difficult for general processors with insufficient capabilities to easily handle such information. This can better include personal information in the protection umbrella.[7]

2.3. Personal Information Infringement Liability Method

2.3.1. Preventive responsibility for diversity

In order to establish a more comprehensive and thorough relief system for personal information infringement, the liability for personal information infringement cannot be limited to one point. While considering compensating for the consequences of the infringement that has already occurred, it is also necessary to pay attention to the legal interests that may be infringed in the future. Among them, preventive liability is essential and can effectively provide prior protection for victims. When personal information is infringed, obstructed or threatened by criminals, whether the damage results or whether the information processor is at fault does not affect the victim's request for the information processor to assume preventive responsibility. Preventive liability can be summarized into three categories:

1. Common preventive liability for infringement of personality rights. There are mainly two types: one is the preventive liability for personality rights infringement stipulated in Article 995 of the Civil Code, such as the destruction and cancellation of books, periodicals, and documents that contain content that infringes on personal information; Secondly, Article 997 of the Civil Code stipulates that if a natural person has evidence to prove that the perpetrator is committing or about to commit a personality rights infringement, and failure to stop it in a timely manner will cause irreparable damage to the legitimate rights and interests of the natural person, the natural person has the right to apply to the court for an injunction. Issuing a ban may prompt information processors to promptly block and block information, preventing the spread of harmful consequences.[8]
2. The preventive liability for personal information infringement is reflected in the Civil Code. Article 1037 of the Civil Code clarifies the right to correct and delete personal information, and the anonymization measures stipulated in Article 1038 (1) can also serve as a way to assume liability for infringement when a natural person's personal information is being or will be infringed upon. If a natural person discovers that the personal information processed by an information processor is incorrect, they have the right to raise objections and request necessary measures such as timely correction; If a natural person discovers that an information processor has processed their personal information in violation of laws, administrative regulations, or the agreement between both parties, they have the right to request the infor-

mation processor to delete it in a timely manner

3. The preventive liability for personal information infringement is reflected in the Personal Information Protection Law. It mainly includes: firstly, the measures for suspending the provision of products and services as stipulated in Article 47 (2) of the Personal Information Protection Law. The main manifestation is that when the information processor improperly or violates the agreement of the parties to process personal information, and it is technically difficult to delete the personal information, the personal information processor should stop processing other than storage and take necessary security protection measures. The second is the encryption and de identification measures stipulated in Article 51 (3) of the Personal Information Protection Law.[9] When natural persons face specific risks of personal information leakage or abuse, they can request information processors to use pseudonyms or other technical means to replace the identification of personal information.

2.3.2. Dual compensatory liability approach preventive responsibility for diversity

If personal information is infringed upon by criminals and actual damage consequences have occurred, natural persons have the right to request information processors to bear some compensatory responsibilities. According to different protection purposes and compensation methods, the above liability bearing methods can be roughly divided into two categories:

1. Restore the original state. In a broad sense, restoration to the original state refers to timely remedial measures to restore the personal information rights and interests of natural persons to their pre injury state. It specifically includes restoration to the original state, elimination of impact, restoration of reputation, and apology in a narrow sense. There are several issues worth noting regarding this: firstly, when the victim requests compensatory liability, the scope of exposing personal information cannot be expanded to avoid secondary damage. Secondly, in a narrow sense, the restoration of the original state is not limited to the restoration of tangible damages. The technical measures mentioned above, such as correction, deletion, anonymization, and de identification, used to eliminate intangible damages, can also be used as specific methods for restoring the original state after the damage results occur. Thirdly, if the restoration of the original state still cannot restore the damaged personal information rights and interests to their original state, compensation for losses should be taken.

2. Compensation for losses. The damage results of personal information infringement include various types, including property damage and mental damage, thus giving rise to multiple methods for calculating the amount of compensation for damages. Firstly, for those who cause property damage, there are three main methods for calculating the compensation amount: firstly, compensation is based on actual losses, and the scope of compensation includes not only direct benefits such as

economic losses and reputation damage caused by information leakage, but also indirect benefits lost due to rights protection actions. [10]The second is to compensate for the improper benefits obtained by the tortfeasor through infringement, such as profits obtained through illegal sale or use of personal information. Thirdly, when it is impossible to accurately determine the actual losses and the scope of benefits obtained, the court can make a discretionary decision on the amount of damages compensation based on individual cases. Secondly, the Personal Information Protection Law does not provide clear provisions on the compensation system for mental damages caused by personal information infringement. According to Article 1183, Paragraph 1 of the Civil Code, if the personal rights and interests of a natural person are infringed upon, the victim has the right to request compensation for mental damages under the following two conditions: firstly, the object of infringement is the personal rights and interests of the natural person. Secondly, it must cause serious mental harm. The provision regarding "causing serious mental harm" as a necessary element is not entirely reasonable in my opinion. On the one hand, the damage to personal information has a latent effect, and victims have great difficulties in proving the severity of their mental damage, which has led to many courts rejecting victims' claims on the grounds that their lives are not seriously disturbed; On the other hand, both the EU's General Data Protection Regulation and Germany's Federal Data Protection Act have the requirement to remove the requirement of "causing serious mental harm" as a necessary element, reflecting the human rights supremacy tendency of contemporary personal information legislation that puts people first. The victim only needs to prove that they have suffered sufficient mental pain to request relief, and multiple factors are considered to determine the amount of compensation for mental damages, such as the subjective malice of the infringer, the mode and occasion of the infringement, and the severity of the damage caused.

2.3.3. A punitive damages system for the future

Due to the complex consequences of personal information infringement, it is necessary to introduce a punitive damages system to achieve the damage prevention function of infringement law, which is an inevitable development of the law. The reasons are as follows: firstly, to punish and deter information processors. In the era of big data, the interests carried by personal information are becoming increasingly significant. If we do not crack down severely on infringing personal information processors, there will be cases where information processors, due to the huge benefits brought by personal information, disregard legal punishment and take risks to commit infringement. At this point, information processors' pursuit of personal information interests will surpass their reverence for legal punishment mechanisms, making it impossible to achieve the goal of deterring and deterring those who intend to commit infringement but fail to do so.[11] But the punitive damages system can precisely suppress the improper information processing behavior of personal in-

formation processors, thus playing a preventive and deterrent role. Secondly, fill the compensation gap. Due to the complex nature of personal information infringement, victims often face objective difficulties in obtaining evidence. Under normal circumstances, victims who have suffered personal information infringement find it difficult to fully demonstrate the original state of the infringement after their personal information has been infringed, and some victims may not even realize that their personal information has been infringed, let alone collect and submit all the evidence of the infringement on their own. The punitive damages system can effectively remedy all losses suffered by the victim, making the infringer bear the full compensation obligation for the consequences caused by their harmful behavior, and can supplement the legislative deficiencies caused by the inability of the infringed to provide complete evidence. Thirdly, encourage victims to actively safeguard their personal information rights and interests. The property characteristics of personal information are often manifested in the storage of a large amount of information on relevant media. Given that the property characteristics of individual natural person information are relatively insignificant compared to a large amount of information, coupled with the high cost of seeking legal remedies for individuals who have infringed on personal information. [12] Faced with the asymmetry between the cost of safeguarding rights and the benefits of winning a lawsuit with relatively small property characteristics, most victims of infringement choose to silently bear the infringing behavior and not pursue the infringer's actions. The purpose of the punitive damages system is to improve this situation, advocating for the active exercise of relevant civil litigation rights by providing a benefit driven approach.

3. Conclusion

Personal information is a distinguishing feature in the era of big data, carrying various legal interests of different subjects. Due to the complexity of personal information and the blank of China's personal information protection law, various issues of personal information infringement have emerged one after another. For example, the app forcibly, frequently, and excessively requests permissions and collects personal information beyond its scope; Illegal dissemination of commercial information; Disregarding users' right to fair trade and using big data to 'kill' them; Abuse of facial recognition data; Monitor and monitor personal privacy, etc. Therefore, this article explores the definition of the concept of personal information rights and the principles of liability for personal information infringement. Based on the achievements of foreign legislation, it is believed that the scope of personal information is constantly changing with the development of technology. Only by establishing a system of liability for damages that combines fault liability and fault presumption can the mission of personal information relief be achieved. In this regard, China's Personal Information Protection Law should establish a responsibility system with preventive, compensatory, and punitive functions in order to fully utilize the remedial function of the Per-

sonal Information Protection Law and safeguard the personal information security of natural persons.

Acknowledgements

This article was finally finalized after four months, during which many difficulties were encountered and often stuck in bottleneck periods, but they were overcome with their own persistence. At the same time, I would like to express my gratitude to all the scholars whose works are cited in this paper. Only by studying your works can I have a deeper and more thorough understanding of the topic, and ultimately complete the writing of this paper.

References

- [1] Information on: https://www.cac.gov.cn/2015-07/22/c_1116002040.htm
- [2] Zhang Xinbao: Principles of Tort Liability Law (China Renmin University Press, China 2005) p. 33-35.
- [3] Hu Yan: Case Study of China's Tort Liability Law (Intellectual Property Press, China 2011)p. 205-206.
- [4] Xie Yuanyang: Private Law Protection of Personal Information (China Legal Publishing House, China 2016)p. 341-343.
- [5] Cai Yingwen: Research on Legal Issues Concerning the Determination of Infringement Fault (Law Press, China, 2016)p. 168.
- [6] Guo Minglong: Protection of Personal Information Rights through Infringement Law (China Legal Publishing House, 2012)p. 96-97.
- [7] Zhou Hanhua: Research Report on Personal Information Protection Law and Legislation (Beijing Publishing House, China 2006)p. 242.
- [8] Zhang Xinbao: Discussion on the main contradictions in the legislation of China's Personal Information Protection Law, Journal of Social Sciences, Jilin University, 2018 (05)p. 113-115.
- [9] Yang Lixin: Personal Information: Legal Interest or Civil Right - Interpretation of Article 111 of the General Principles of Civil Law on "Personal Information". Legal Forum, 2018 (01)p.25-27.
- [10] China Legal Publishing House: Civil Code of the People's Republic of China: Large Font Edition (China Legal Publishing House, China 2020)p.326-327.
- [11] Zhang Jianwen and Shi Cheng: New Forms of Personal Information Infringement and Their Remedies Journal of Law, April 15, 2021p.34-36.
- [12] Diao Shengxian: Research on Personal Information Network Infringement Issues (Shanghai Sanlian Bookstore, China 2016)p.175-177.