

Study on the Civil Law Protection of Personal Biometric Information -- Focusing on the Construction of Rights and Remedy Mechanisms

Donghui Zhuo

Anhui University of Finance and Economics, Bengbu 233030, China

Email: zhuodonghui2022@163.com

How to cite this paper: Zhuo, D. H. (2025). Study on the civil law protection of personal biometric information -- Focusing on the construction of rights and remedy mechanisms. *Social Sciences and Humanities*, 1(1), 17–28. ISSN Print: 3104-4328, ISSN Online: 3104-4336.

<https://doi.org/10.63313/SSH.9003>

Published: 2025-07-16

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 the context of the fusion of information technology and biotechnology, personal biometric information is widely used but the risk of leakage and abuse is prominent. This study focuses on its civil law protection, with the construction of rights and relief mechanisms as the core. Personal biometric information has the attributes of basic human rights, personality rights, privacy rights, and property rights. In the current civil law system, privacy rights, general personality rights, and personal information rights and interests have problems such as limited scope of protection, ambiguous boundaries of rights, and insufficient positive power. As for the relief mechanism, the existing civil tort litigation and negotiation and mediation have such defects as unclear attribution principle, narrow scope of compensation, unreasonable burden of proof, and cumbersome procedures. The study proposes clarifying the presumption of fault, broadening the scope of damages, optimising the distribution of evidence, and simplifying litigation procedures to improve the protection system. It also emphasises the need to pay dynamic attention to new issues of technological development, balance the relationship between the protection of citizens' rights and interests and technological innovation, and provide systematic civil law protection for personal biometric information.

Keywords

Personal biological information; personality rights; protection of rights

1. Introduction

1.1. Background of the research

With the rapid development of information technology and biotechnology, personal biometric information has been widely used in people's daily life. From fingerprint unlocking and facial recognition payment in smartphones, to identity verification in security checks at airports and railway stations, to customer identification in finan-

cial institutions and identity confirmation in educational examination registration, biometrics have greatly changed people's lifestyles by virtue of its convenience and high efficiency, and brought a lot of convenience to the development and progress of the society. For example, in the financial field, the application of biometrics technology makes it possible for customers to perform online transactions, account login and other operations without the need for cumbersome password input, through fingerprint identification, facial recognition and other ways to quickly complete the identity verification, which not only improves the efficiency of the transaction, but also strengthens the security of the transaction. In terms of traffic and travel, passengers can quickly pass through the security channels of airports and railway stations through facial recognition technology, which greatly shortens the travelling time and enhances the travelling experience.

However, while personal biometric information is widely used, it also faces serious problems of being leaked, misused and other risks. Due to the uniqueness, immutability and high sensitivity of personal biometric information, once it is leaked or abused, it will cause irreparable damage to personal privacy, property security and even personal dignity. In recent years, there have been frequent incidents of personal biometric information leakage, such as the public sale of the full digital fingerprints of more than 60,000 users and the face data of 170,000 users, and the theft of property through WeChat authentication by voiceprint forgery. These incidents have not only brought huge losses to individuals, but also triggered public concern about personal biometric information security. In addition, some enterprises and organisations collect and use personal biometric information without users' consent, over-collection, and insufficient security measures for data storage, further exacerbating the security risks of personal biometric information.

1.2. significance of the research

The study of civil law protection of personal biometric information has important theoretical and practical significance. From the perspective of safeguarding citizens' rights and interests, personal biometric information is closely related to citizens' human dignity, privacy and property security. Through the protection of civil law, the rights of citizens to personal biometric information can be clarified, and when the rights are infringed upon, the citizens can obtain effective remedies according to the law, so as to effectively safeguard the legitimate rights and interests of citizens. For example, when a citizen's face information is illegally collected and used, the citizen can request the infringing party to stop the infringing behaviour and compensate for the loss according to the relevant provisions of the civil law, so as to safeguard his or her human dignity and privacy rights and interests.

From the perspective of promoting the healthy development of digital economy, personal biometric information is an important basic resource for the development of digital economy. Only by establishing a sound civil law protection mechanism can the public's trust in the use of personal biometric information be enhanced, the en-

thusiasm of market players to reasonably use personal biometric information for innovation and development be stimulated, and the healthy and sustainable development of the digital economy be promoted. Under a secure legal environment, enterprises can safely use personal biometric information to develop new products and services, such as intelligent security systems and personalised financial services, injecting new vitality into the development of the digital economy.

From the perspective of improving the legal system, at present, although China has made relevant provisions on personal information protection in laws and regulations such as the Civil Code, the Personal Information Protection Law, and the Cybersecurity Law, there are still some deficiencies in the civil law protection of personal biometric information, such as insufficiently clear definition of the attributes of the rights, insufficiently specific provisions on the content of the rights, and insufficiently perfect relief mechanisms. An in-depth study of the civil law protection of personal biometric information can help further improve China's legal system, fill the legal gaps, improve the adaptability and regulatory capacity of the law to the development of emerging technologies, and provide a more solid legal guarantee for the protection of personal biometric information.

2. Basic Theory of Personal Biometric Information

2.1. Concepts and Characteristics of Personal Biometric Information

2.1.1. Concept of Personal Biometric Information

In today's digital age, the definition of personal biometric information has been elaborated differently in domestic and international laws. Article 10134(2) of China's Civil Code clearly stipulates that personal information is all kinds of information recorded electronically or by other means that can identify a specific natural person individually or in combination with other information, which covers biometric information. Article 76(5) of the Cybersecurity Law also states that personal information includes a natural person's name, date of birth, identity document number, personal biometric information, address, telephone number, etc., which alone or in combination with other information can identify a natural person. And the EU General Data Protection Regulation stipulates that personal biometric information is personal information obtained through specific technical identification. Taken together, personal biometric information is a kind of information obtained by using modern biometric technology to digitally process a person's physical, physiological or behavioural characteristics, which can accurately identify the identity of a specific natural person and generally cannot be altered, and has a high degree of identifiability and irreplaceability.

Specifically, personal biometric information can be divided into body information and behavioural information. Physical information belongs to an individual's innate physiological information, such as facial images, fingerprints, palm veins, retina, iris and DNA samples, etc. Behavioural information is an individual's acquired behav-

journal information, such as handwriting, typing rhythms, gait and voice. In our daily life, we can see the application of personal biometric information everywhere. In the financial field, when handling banking, insurance and other businesses, face recognition links are used for identity verification; travelling by high-speed rail and train, the station needs to brush the ID card and carry out face recognition; the school credit network and various formal examination registration also rely on face recognition to verify the identity. Fingerprint information is also widely used, such as fingerprint card punching for time and attendance, fingerprint unlocking for smartphones and fingerprint door locks, and fingerprint payment for Alipay.

2.1.2. Characteristics of a person's biometric information

Personal biometric information has many unique characteristics. It has strong personal attributes, which every person possesses since birth, directly reflecting the unique and irreplaceable physical, physiological or behavioural characteristics of a natural person, and has a high degree of identifiability. Moreover, most personal biometric information cannot be changed, such as the fingerprints and iris of a natural person, which are unique, irreplaceable and lifelong. This higher identifiability and uniqueness enables personal biometric information to more accurately and quickly confirm the identity of a natural person and other relevant information, but once leaked or abused, it may cause more serious damage results, seriously infringing on the personal dignity and freedom of the subject of the information, or bringing huge property losses to the subject of the information. For example, the use of Internet technology to synthesise face and voiceprint information for fraud is more likely to succeed because it is easier to gain the trust of the victim.

2.2. The need for civil law protection of personal biometric information

At a time when information technology is developing rapidly, personal biometric information is widely collected, used and stored, but it is also facing serious security problems. It is not uncommon for a large amount of personal biometric information to be collected illegally, and some enterprises and organisations do not follow the principles of lawfulness, legitimacy and necessity when collecting information, and collect without the consent of the user, or even over-collect personal biometric information. In the use segment, there is also the phenomenon of improper use, using the collected personal biometric information for unauthorised purposes, or sharing or transferring it with a third party without informing the subject of the information. And in the storage process, personal biometric information is highly susceptible to leakage or illegal access once there is a security flaw in the protection technology. In addition, the case of voiceprint forgery to steal property through WeChat authentication also highlights the serious consequences of misuse of personal biometric information.

Personal biometric information is closely linked to the personal and property safety of citizens. Due to its uniqueness and immutability, once it is leaked, an individual's

identity is very easy to be used fraudulently, which in turn leads to property loss. By obtaining other people's fingerprint information, lawbreakers can unlock the fingerprint payment function and steal other people's account funds; using face information, they may break through the face recognition verification and log into other people's important accounts to steal privacy or carry out fraudulent activities. Moreover, the leakage of personal biometric information may also seriously damage the dignity and freedom of citizens, creating a sense of insecurity, as if living in a 'transparent' state, with no privacy to speak of.

Civil law protection of personal biometric information can help prevent the misuse of information and safeguard the legitimate rights and interests of the subject of the information. By clarifying the attribution of rights to personal biometric information and regulating the rules of information collection and use, civil law can effectively constrain the behaviour of information collectors and users, avoid their abuse of power, and safeguard the information subject's right to control and self-determination of his or her own biometric information. At the same time, a sound civil law protection mechanism can enhance public trust in the use of personal biometric information and promote the healthy development of biometric technology. Only in a secure legal environment will people feel more comfortable using biometric technology, and enterprises and organisations will be able to make better use of such information for innovation and development, promoting the rational application of biometric technology in various fields and creating greater value for society.

2.3. Theoretical foundations of civil law protection of personal biometric information

Personal biometric information has multifaceted attributes, which form the theoretical basis for civil law protection. It has the attribute of basic human rights, which covers both the digital presentation and protection of traditional human rights in the era of big data, as well as the rights and protection of new types of data and information that have emerged with the development of science and technology. In essence, the right to personal biometric information is a basic human right, which is the right that people should enjoy as human beings in the development of science and technology and information data. In modern society, an individual's control and protection of his or her own biometric information is an important manifestation of his or her basic human rights and concerns the dignity and freedom of the individual.

From the perspective of general personality rights, biometric information is unique to each individual, and its use and protection involves core issues such as equality, independence, freedom and dignity of personality. The subject of information enjoys the right to make independent decisions about his or her own biometric information, and others may not collect, use, store or disclose it without consent, or else the subject's personality rights will be violated. The privacy attributes of personal biometric

information are also very significant. In view of the importance of biometric information in consumer payment and traffic passage, most information subjects hope that their information will not be known by others, and have a strong expectation of privacy. Unlawful collection and use of personal biometric information is undoubtedly an infringement of informational privacy; if such information is used to track and monitor others and spy on their lives, it infringes on an individual's physical privacy.

From the perspective of property rights, in the era of big data, personal biometric information has a high degree of sensitivity and commercial utilisation value, and at the same time is extremely vulnerable. Once leaked or damaged, it is likely to bring huge property damage to the information subject. Some enterprises collect and analyse personal biometric information to carry out precise marketing and obtain commercial benefits, which also reflects the property value of personal biometric information from the side. Therefore, the protection of personal biometric information under civil law aims to safeguard the right to self-determination of personal information, protect the integrity of personality and property security, and comprehensively protect the legitimate rights and interests of the subject of information from multiple perspectives, so that he or she can better control his or her own biometric information in the digital age, and avoid being subjected to unnecessary infringement.

3. Rights-based construction of civil law protection of personal biometric Information

3.1. Inadequacies in the protection of biometric information of individuals under the existing rights system

Under the current civil law rights system, the protection of personal biometric information is mainly based on the right to privacy, general personality rights and personal information rights and interests. However, these rights have many limitations in dealing with the protection of personal biometric information.

From the perspective of the right to privacy, the traditional right to privacy emphasises the protection of the peace of private life and private space, focusing on passive defensive rights. Personal biometric information, although partially involving private attributes, is more often embodied in dynamic data that can be collected, used, stored and transmitted, and its protection needs go far beyond the scope of the traditional right to privacy. For example, when face recognition technology is widely used to monitor public places, it is difficult for information subjects to effectively control the collection of biometric information on the basis of the right to privacy, as the act does not directly invade the traditionally private space, but may cause potential damage to the personality and property interests of the information subject. Although the general personality right to protect personal biometric information has a certain degree of flexibility, the connotation and extension of the general per-

sonality right is relatively vague. In the specific judicial practice, the judge of the general personality rights of the application of greater discretion, difficult to form a unified, clear decision standard. This leads to uncertainty in the process of defending the rights of the subject of information, unable to accurately grasp the boundaries of the rights, and is not conducive to the provision of stable and reliable legal protection for personal biometric information.

As a newly established right in the Civil Code, although personal biometric information is included in the scope of protection, the nature and content of this right has not yet been fully clarified. At present, personal information rights and interests are more often reflected in practice as a less confrontational type of right and interest, lacking a clear positive power. For example, it is difficult for an information subject to actively request an information processor to delete collected biometric information on the basis of personal information rights and interests, and only after the information has been improperly processed can it provide relief, which is unable to safeguard the security and autonomy of personal biometric information from the source.

3.2. Construction of Exclusive Rights to Personal Biometric Information

In order to make up for the shortcomings of the existing rights system, it is of great significance to construct the exclusive right to personal biometric information. The exclusive right to personal biometric information should be a new type of independent civil right, with the personality and property interests of personal biometric information as the object of the right.

In terms of the content of the right, the exclusive right to personal biometric information shall include both positive and negative rights. Positive power covers the information subject's right to make independent decisions on its own biometric information, i.e. the right to decide whether to provide information, the purpose and scope of use of the information, etc.; the right to enquire information, the right to know the collection, storage and use of its own biometric information; the right to rectify information, the right to ask the information processor to rectify the information when the information is incorrect or inaccurate; the right to delete information, the right to request the deletion of the collected biometric information when the legal conditions are met. The right to request the deletion of collected biometric information under legal conditions. Negative power, on the other hand, is manifested in the right to exclude others from illegally collecting, using, storing, transmitting, disclosing and other infringing behaviours, and when the right is infringed upon, the subject of the information has the right to request the cessation of infringing behaviours, the elimination of impacts, and compensation for losses.

In the exercise of rights, the principles of lawfulness, legitimacy and necessity shall be followed, and the subject of information shall not harm the public interest and the lawful rights and interests of others when exercising its exclusive rights. At the same time, in order to balance the interests between the subject of information and

the information processor, for special scenarios involving the public interest, such as public security and public health, the exclusive rights of the subject of information shall be reasonably limited within the scope of the law. For example, during the period of epidemic prevention and control, the relevant departments collect personal biometric information in accordance with the law in order to track the spread of the epidemic, and the subject of the information should cooperate, but the information processor must also strictly follow the legal procedures and requirements to safeguard the safety and reasonable use of the information.

3.3. Coordination with other related rights

The exclusive right to personal biometric information is closely linked to, but distinctly different from, the right to privacy, the rights and interests in personal information and other related rights. In terms of coordination of rights, the boundaries and scope of application of each right should be clarified.

There is an intersection between the exclusive right to personal biometric information and the right to privacy, and when biometric information involves the private life and private space of an individual, it may be protected by both the exclusive right and the right to privacy at the same time. In this case, the priority application of the right should be judged according to the specific situation. If the infringement mainly infringes on the information subject's right to make autonomous decisions on biometric information, the protection should be based on the exclusive right to personal biometric information; if the infringement focuses on disrupting the peace and quiet of a person's life and infringing on the private attributes of the private sphere of private life, the right to privacy shall take precedence.

Compared with the rights and interests in personal information, the exclusive right to personal biometric information is more special and specific. Personal information rights and interests is a broader concept, covering all types of personal information, while the exclusive right to personal biometric information is constructed specifically for the characteristics of biometric information, and its right content and protection are more specific and strict. In practical application, for general personal information processing behaviours, it can be regulated according to the rights and interests of personal information; while for special processing behaviours involving personal biometric information, priority should be given to applying the exclusive right to personal biometric information, so as to give the information subject more adequate and effective protection. At the same time, in the application of both, duplication of rights and protection gaps should be avoided to ensure systematic and complete legal protection.

4. Status and Problems of Remedy Mechanisms for Civil Law Protection of Personal Biometric Information

4.1. Overview of available remedial mechanisms

China's current civil law protection and remedial mechanisms for personal biometric information mainly include civil tort litigation and negotiation and mediation. In terms of civil tort litigation, the subject of the information can, in accordance with the Civil Code, the Personal Information Protection Law and other relevant laws and regulations, file a lawsuit with the court on the grounds of a dispute over tort liability, and demand that the infringer assume civil liability for stopping the infringement, eliminating the impact, and compensating for the loss.

Negotiation and mediation, on the other hand, involves the information subject and the information processor reaching a settlement agreement and resolving the dispute through self-negotiation or mediation by a third-party mediation organisation after the dispute has arisen. In addition, some industry self-regulatory organisations also participate in the resolution of disputes over personal biometric information to a certain extent, and through the formulation of industry norms and standards, they guide information processors to handle information in a lawful and compliant manner and facilitate the resolution of disputes.

4.2. Problems with relief mechanisms

4.2.1. The principle of attribution is not clear

In personal biometric information infringement disputes, there is controversy over the fault determination standard of the infringer. As biometric information infringement behaviour is often hidden, technical and other characteristics, it is difficult for the subject of information to prove that the infringer is at fault, and the current law does not explicitly provide for the application of the principle of no-fault liability or the principle of presumption of liability, resulting in inconsistent adjudication standards in judicial practice, and it is difficult to effectively safeguard the legitimate rights and interests of the subject of information.

4.2.2. Excessively narrow scope of damages

At present, damages for infringement of personal biometric information are mainly limited to direct property losses and partial compensation for moral damages. However, once personal biometric information is leaked or misused, it may bring long-term and potential risks to the information subject, such as identity theft and fraud, etc., and it is often difficult to obtain compensation for these indirect losses and possible future losses. In addition, there is a lack of clear legal provisions to support the reasonable costs incurred by the subject of information in defending his or her rights and interests, such as the costs of investigating and obtaining evidence and attorney's fees.

4.2.3. Unreasonable distribution of burden of proof

In personal biometric information infringement litigation, the information subject, as a weaker party, faces many difficulties in collecting evidence. As the information

processor holds the technology and data for information processing, it is difficult for the information subject to obtain evidence of the infringement. The current law still follows the general principle of burden of proof of 'whoever claims, whoever proves', requiring the information subject to bear the main burden of proof, which puts the information subject in an unfavourable position in litigation, and the cost of defending rights is too high, leading many information subjects to give up defending their rights due to the difficulty of proving their rights.

4.2.4. Proceedings are cumbersome and inefficient

Infringement disputes over personal biometric information often involve complex technical issues and a large amount of evidentiary material, requiring professional identification and assessment. However, the existing civil litigation procedures are relatively cumbersome and the trial period is long, which cannot meet the needs of information subjects to defend their rights in a timely manner. At the same time, a single litigation method is also difficult to adapt to diversified dispute resolution needs, and the lack of a diversified dispute resolution mechanism makes the information subject lack more choices in the dispute resolution process.

5. Suggestions for Improving Remedial Mechanisms for Civil Law Protection of Personal Biometric Information

5.1. Clarification of principles of attribution

In order to better protect the legitimate rights and interests of information subjects, the principle of attribution of responsibility for personal biometric information infringement disputes should be clarified. In view of the special nature of personal biometric information infringement, it is recommended that the principle of presumption of fault liability be adopted. That is, once the information processor has committed the act of infringing personal biometric information, it is presumed to be at fault, and unless the information processor is able to prove that it is not at fault, it should bear the responsibility for the infringement. This can reduce the burden of proof on the subject of information and improve the enthusiasm of the subject of information in defending its rights, while also prompting the information processor to be more cautious in handling personal biometric information and enhancing its sense of responsibility.

5.2. Broadening the scope of damages

The scope of damages for infringement of personal biometric information should be broadened to include not only compensation for direct property losses and moral damages of the subject of information, but also indirect losses and reasonable losses that may occur in the future. For example, compensation should be provided for losses incurred by the subject of information as a result of fraud due to the leakage of biometric information, as well as for expenses incurred in taking the necessary

measures to prevent risks that may occur in the future. In addition, it is clearly stipulated that reasonable expenses incurred by the information subject in defending its rights and interests, such as investigation and evidence collection costs and attorney's fees, shall be borne by the infringer, in order to reduce the cost of defending the rights and interests of the information subject.

5.3. Optimising the allocation of burden of proof

In personal biometric information infringement litigation, the allocation of the burden of proof should be appropriately adjusted. On the basis of the principle of 'whoever claims, whoever proves', the burden of proof should be reversed for facts that are more specialised and difficult for the subject of the information to prove. For example, the burden of proof shall be borne by the information processor for facts such as whether the information processor has taken the necessary technical measures to safeguard information security and whether there is any illegal collection or use of information. At the same time, the subject of information is encouraged to actively collect evidence, and electronic evidence obtained by the subject of information through lawful means shall be admissible in accordance with the law, so as to improve the subject's ability to adduce evidence.

5.4. Simplification of proceedings

In view of the characteristics of personal biometric information infringement disputes, litigation procedures should be simplified and litigation efficiency improved. Special personal information infringement litigation procedures can be established, and for cases where the facts are clear and the relationship between rights and obligations is clear, simplified procedures or small litigation procedures should be applied to hear the case, so as to shorten the hearing cycle. At the same time, the examination and identification of electronic evidence should be strengthened, and modern information technology means should be fully utilised to achieve online submission, examination and review of evidence, so as to improve the convenience and efficiency of litigation.

6. Conclusion

The civil law protection of personal biometric information is an important topic for safeguarding the legitimate rights and interests of citizens and promoting the healthy development of digital economy in the digital era. By constructing the exclusive right to personal biometric information, clarifying its relationship with other related rights, and improving the relief mechanism of civil law protection, it can effectively fill the gaps and deficiencies of the existing legal protection, and provide comprehensive, systematic and effective legal protection for personal biometric information. However, the civil law protection of personal biometric information is a dynamic development process, with the continuous innovation of biometric tech-

nology and the increasing expansion of application scenarios, it is also necessary to continue to pay attention to the new problems and challenges in the protection of the law, and constantly improve the relevant legal system to meet the needs of the times, effectively safeguard the legitimate rights and interests of the information subject, and promote the healthy development of personal biometric technology on the track of lawfulness, compliance and safety. and promote the healthy development of personal biometrics in a lawful, compliant and safe track.

References

- [1] Ding YF, Shi XY. Research on consent and withdrawal of biometric information, *Journal of Weifang College*, Vol. 24 (2024) No. 6, p.64-72.
- [2] Lou Bingwen. The construction of reasonable use system of personal biometric information under the threshold of digital human rights, *Journal of Jiangsu University (Social Science Edition)*, Vol. 27 (2025) No. 2, p.83-93.
- [3] Zhu Peizhi. Study on the Tort Liability of Personal Biometric Information, *Journal of Gansu University of Political Science and Law*, 2024 No. 5, p.42-51.
- [4] Jingyi Chu. On the identification standard in the definition of biometric information and the construction of China, *Journal of Huazhong University of Science and Technology (Social Science Edition)*, Vol. 37 (2023) No. 4, p.85-97.
- [5] Gu Xiuwen. Research on restraint application of personal biometric information in the context of big data, *Journal of Hubei Engineering Institute*, Vol. 43 (2023) No. 1, p.95-101.
- [6] Song Yichen. Security risk and legal regulation of biometric information, *Journal of Henan College of Pastoral Economics*, Vol. 35 (2022) No. 3, p.56-61.
- [7] Gao Lifan, Yang Bo. Thoughts on Compliance in Biometrics Application, *Cyberspace Security*, Vol. 13 (2022) No. 2, p.79-83.