Legal Regulation and Path Improvement of Face Recognition Information Protection from the Perspective of Comparative Law

Kexin Zhou

School of Political science and Law, Northeast Teachers University, Changchun, China

zhoukx383@nenu.edu.cn

Abstract.: With the increasing popularity of artificial intelligence technology, face recognition technology has shown explosive growth, but high speed and risk coexist. In recent years, the number of cases caused by face recognition has been increasing at home and abroad. The civil law system has paid attention to the protection of face information, a particular type of personal information. However, whether the existing law can fully deal with the face recognition technology under the new technology development situation and whether it can effectively protect it still needs further demonstration and analysis. From many face recognition infringement cases, we can see that the abuse of face recognition technology and the infringement of face information have caused severe violations of personal rights and even endanger public security. With the introduction of the Personal Information Protection Law and Civil Code, information subjects obligations and legal consequences are stipulated, which better meets the practical needs of face recognition information protection. However, there are still some problems in practice, such as imperfect standards of face recognition information obligations, unclear definition of the 'safety, legality, legitimacy and necessity' principle, poor protection of sensitive personal information, complex relief of data space infringement, and unclear connection with criminal law. Therefore, based on the analysis of extraterritorial experience and domestic legislation and judicial practice, we can further improve the problems above and optimize the path of legal protection.

Keywords: Face recognition information, Comparative law, Civil code, Personal information protection law.

1. Introduction

Face biological information collected by face recognition technology belongs to face recognition information[1], which is identifiable, unchangeable, relevant, and easy to obtain. In recent years, we has widely use face recognition in residential access control, payment transfer, real-name registration, unlocking and decryption, company attendance, and other scenarios. Tianyancha data shows that there are more than 6,500 face recognition-related enterprises in China. China is the largest consumer of face recognition equipment and is expected to account for 44.59 percent of the world in 2023, according to the China Personal Information Security and Privacy Protection Report. Face recognition is everywhere.

The wide application of artificial intelligence and big data technology undoubtedly provides technical support for face recognition, and face recognition technology also brings many conveniences to people. For example, in the context of the new coronavirus, many public places, such as large shopping malls and schools, adopt face recognition technology to prevent and control the epidemic. Thus, face recognition technology is developing rapidly in the digital age.

Although face recognition technology brings convenience to our lives and social governance, the abuse of face recognition technology will bring comprehensive risks and challenges to personal information protection and privacy security. The promulgation of the Personal Information Protection Law in August 2022 has great practical significance, which responds to the current situation that personal information needs legal protection in big data. At the same time, the ‘Civil Code’ separates the ‘right to personality’ into separate parts and regulates personal information as personal rights. Some new provisions on privacy and personal information protection are included in the law, such as the principle of dealing with personal information, namely, impartiality and necessity, which made

significant progress in the legal regulation of personal information protection. However, how should the existing legal norms ensure that don't abuse face recognition technology? Can the existing laws fully deal with face recognition technology under the new technology development situation? The above issues pose new challenges to the current legal norms and need further exploration. Based on these, this paper will deeply analyze the path and shortcomings of the protection and application of face information under the existing legal norms, and combine comparative law with China's national conditions to analyze and improve the path.

2. Face Recognition Information and The Necessity of Its Protection

2.1 Characterization of Face Recognition Information

2.1.1 Face recognition information belongs to sensitive personal information

The Civil Code defines personal information as a variety of recorded electronically or otherwise that can be used to identify a particular natural person individually or in combination with other information. Academic circles generally believe that personal information can be divided into sensitive information and non-sensitive information [2]. Biometric information is closely related to personal property, so it belongs to sensitive personal information.

Face recognition information belongs to biological data, which is closely related to the position of facial shape and size. Biological data is unique, such as fingerprints, irises, genes, and faces. Thus, it is more explicit than ordinary personal information. When mastering the data, it can identify people's identities and then associated with other information in big data to obtain the personal family address, telephone number, payment account, and so on, so that individuals become ' transparent. 'Therefore, it is closely related to personal identity and property rights.

As a sub-item of sensitive personal information, face recognition information applies to the relevant norms of personal information. Therefore, if the face recognition information is caused by infringement, we can seek the personal information law.

2.1.2 Face Recognition Information and Privacy

On the current legal norms, the private information in personal information also can be divided into privacy, so there is a close relationship between personal data and privacy. However, the differences can't be confused. From the perspective of an attribute, personal information emphasizes identification and is closely related to personal identity, while privacy emphasizes secrets[3]. From the content of rights, personal information rights mainly refer to the control of personal information and independent decision, which is the right of initiative. The focus of privacy is to prevent personal secrets from being illegally disclosed rather than to protect the control and use of such information. It is a hostile and defensive right[4].

Therefore, in practice, it is necessary to grasp the situation of concurrence in their legal protection. In the case of concurrence, according to Paragraph 3 of Article 1034 of the Civil Code, the protection method of privacy for private information is stipulated. When recognition information can be defined as confidential information, it applies to the right to privacy protection. In the case of difference, personal information protection provisions are applicable to separate security.

In conclusion, the protection of personal information needs to be regulated according to the proper application of the law.

2.2 Necessity Analysis of Face Recognition Information Protection

Based on an objective and comprehensive investigation and analysis of the current situation of face recognition information security, the report reflects that although face recognition technology in China has developed rapidly, it also brings us many security challenges. Information security risks such as personal privacy data leakage, technology abuse, and other issues need to be solved urgently. The lack of network and data security guarantee mechanisms can easily cause face data leakage. At

the same time, the application of face recognition technology is not standardized and may lead to the abuse of face data, threatening user property and even personal safety.

On the one hand, face recognition information with uniqueness, immutability, and personal attributes belong to sensitive personal information for individual rights and interests. Once disclosed, it may become a 'transparent person' immediately, which may cause irreversible damage seriously. It may endanger individuals' privacy rights and interests and even the right to reputation, causing severe harm to the body and spirit. On the other hand, for public safety, although the application of face recognition can track down fugitives and carry out social management, such as during the epidemic era can effectively track close and sub-close groups to prevent and control effectively. These will facilitate the public, but immature technology also brings many hidden dangers to public safety. There are many irregularities in the management of face recognition technology, leading to information leakage. Criminals also use personal information to engage in telecommunications fraud, and in-depth forgery technology is becoming active, negatively influencing the face recognition system. Illegally stealing other people's payment accounts or obtaining other people's personal information is an endless stream that threatens public security and causes social anxiety and a trust crisis.

It is not difficult to see above that in the context of big data in the Internet era, and it is necessary to protect human face information. However, for a long time, the cost of personal information protection has been high, the effect of administrative means is limited, and the ability of personal prevention is low, resulting in the 'difficult rights protection' phenomenon. With the introduction of the 'Personal Information Protection Law ' and the ' Civil Code ', the protection of personal information is better than before. The obligations of information subjects and legal consequences are stipulated. At this time, the security of personal data is becoming more and more mature. With the rapid development of face recognition technology, the protection of face recognition information has increasingly become the focus of social governance modernization. It is urgent to improve its technical application limit and legal regulation. How to systematically regulate face recognition technology has become the focus of its protection and regulation. Therefore, it is necessary to explore further whether the introduction of the Civil Code and the Personal Information Protection Law has completed the security of face recognition information and whether the current legal regulation is insufficient and how to improve it further.

3. Legal regulation analysis of face recognition information protection

3.1 Legislative Status of Face Recognition Information Protection in China

3.1.1 Norms of the Civil Code

The provisions of the Civil Code ‘Personality Rights’

The right to personality is independent, and the right to personality has an independent right system, so its relief can be guaranteed by the right to claim personality, which has made a major breakthrough with the traditional protection of personality rights that must rely on the right to claim creditor’s rights. It undoubtedly reflects the importance of personal dignity and freedom.

The personality rights section provides the rational use of personal information and the correction and collection of data. It makes detailed provisions on the collection, use, deletion, modification, and protection of personal information. At this time, the subject of obligation is more stringent than the previous legislation. However, in this section, there are no further provisions on civil liability for infringement of personal information,but in China's Personal Information Protection Law for other provisions, which reflects the combination of general law and particular law. Besides, the infringement of personal information is also applicable to the general provisions of the personality right relief in the personality right and can use the right to claim personality rights for relief[5].

The right to claim personality rights pays attention to prevention in advance, and adding the pre-litigation injunction of personality rights in the 'Civil Code' is beneficial to prevent the occurrence or expansion of damage. The Civil Code makes specific provisions on the pre-litigation injunction in

article 997. When more urgent violations occur, we can take this temporary measure to prevent them in advance. .

Therefore, it can be seen that China's Civil Code 'Personality Rights' provides for the relief of personal information protection, which is undoubtedly a new way of comfort and ideas for personal information. Face recognition information as a sub-item of confidential information also applies to relevant norms.

Norms of Civil Code 'Tort Liability '

The protection of tort liability is another important way to protect personal information. In the general provisions of tort liability, face recognition information as a sub-item of personal information is a basic civil right. The principle of fault liability applies to tort liability.'Tort Liability' in Chapter III of the special provisions of the subject of responsibility and face information protection of particular subjects of responsibility, namely network users and network service providers[5], and provides specific provisions on the way of its responsibility. For example, when the network service provider knows that the network user uses its network to implement the infringement, and does not take the necessary measures to delete, block or disconnect the link[6], the network user is allowed to use the network platform provided by it to implement the infringement, causing damage to the infringed person. Among the consequences of the violation, there is the responsibility share by the network service provider, and it should bear joint and several responsibilities[7].The above cannot simply apply the principle of fault liability, let alone the doctrine of no-fault liability[8].

For damages, generally speaking, in tort damages, when there is no violation of the victim's rights, property rights, intellectual property rights, and other rights, but only a pure loss of money, it can't claim tort damages except when the infringer is intentional. What's more, it is stipulated in the Civil Code of Tort Liability that the infringer may request compensation for mental damage. Therefore, mental damage compensation can be advocated when the violation of face recognition information causes severe mental harm to the victim.

The Civil Code regulates the protection of face recognition information in the personality rights section and tort liability section, which is conducive to protecting the legitimate personal information rights and interests. Of course, the Civil Code also provides for acts committed within the consent of natural persons or their guardians, or acts to safeguard the public interest or the persons' legitimate rights and interests. The people don't need to bear civil liability. Only when the exemptions are met, the case of infringement of face recognition information can not accept civil liability.

3.1.2 Norms of Personal Information Protection Law

With the progress of technology, personal information security has been paid more and more attention, and now all countries in the world attach great importance to information and data. Whoever masters the data will master the password of the powerful government. The status and role of information data were further highlighted in the report of the Nineteenth Congress. At the same time, before introducing the Personal Information Protection Law, China's information protection has gone through three stages: criminal law first, multi-pronged administrative field, and civil law complement. The time of separate legislation on personal information protection is also increasingly mature, so Personal Information Protection Law arises at the historic moment.

Personal Information Protection Law realizes the balance of interests among information subject, information industry, and state organs by using general personal information and strengthening the protection of personally sensitive information. The single section of diplomatic personal information processing rules highlights the security of personal biometric data such as face recognition information[9]. Therefore, although face recognition information is not protected separately in the Personal Information Protection Law, it is personal biometric information belonging to sensitive personal information to be applied to the provisions on the protection of sensitive personal information.

In the section of Personal Information Protection Law, Article 28 defines the basic principles of sensitive personal information processing. Sensitive personal information has a broader range of notification matters, which increases the notification obligation of individual information processors,

makes special provisions on minors' information rights and interests, and further limits the collection of sensitive personal information. Therefore, in obtaining the consent of the information subject, face recognition information should obtain individual consent and hand over the decision-making power to the information subject. At the same time, the information processor should adopt different ways of obtaining consent for other information subjects.

The personal information protection law embodies the combination of administrative, civil, and criminal responsibility in legal liability, and connects with the civil code in civil liability, forming a more comprehensive legal protection framework for face recognition information, which is beneficial to make up for the problems of limited scope and relatively low effectiveness of the Personal Information Protection Law, and then further protect people's rights and interests.

3.2 Protection of Face Recognition Information in Chinese Judicial Practice

The first case of face recognition has a milestone significance. In this case, the court of the first instance found the facts of the case mainly from the point of view of the conclusion of the contract. During the performance of the contract, the defendant sent two messages to the plaintiff, which were equivalent to a new offer, but the plaintiff disagreed. As a result, face recognition did not become a contract clause and did not have effect on the plaintiff, and the defendant required that it must be entered into the garden through face recognition, which was contrary to the contract and thus the defendant was liable for breach of contract. At the same time, the court identified the behavior of face recognition information collection in the case from the perspective of 'legitimate, legitimate and necessary principles'. The behavior of the plaintiff and his wife agree to take pictures is not equal to the consent of face recognition. Therefore, the plaintiff requires the defendant to delete its face recognition information. The reason is legitimate and should be supported. The judgment of the second instance also held that the determination of face recognition in the first instance was not inappropriate.

The case does not further explain some of core issues in face recognition, such as principles, and therefore requires further interpretation of ' legitimate, legitimate and necessary principles' in judicial practice. Besides, the case mainly presupposes that the plaintiff and the defendant are in an equal position to judge. But as a fact, the defendant is a strong party, which is not conducive to the protection of the weak. However the case is in the Civil Code and Personal Information Protection Law issued before the decision, reflecting the concept and spirit of the law on personal information protection, such as the use of ' legitimate, legitimate, necessary principles ', and both the court's decisions have recognized the right to delete information subject. This has great practical significance, which has aroused people's attention to face recognition protection and the use of judicial relief to protect face recognition information and safeguard personal rights.

4. Protection and Experience Reference of Face Recognition in Foreign Countries from the Perspective of Comparative Law

4.1 USA

4.1.1 U.S. existing legislation and legislative recommendations on the legal regulation of government departments mainly prohibit the use of special licensing systems.

In May 2019, San Francisco passed the 'Stop Secret Surveillance Ordinance' to ban all government departments from using face recognition technology. The legal regulation of face information protection in the United States mainly takes this form. The special licensing system means that the investigation and law enforcement departments can only use or resort to face recognition technology when obtaining court permission to compare the ID card photo database. And even with permission, audits should be conducted annually to ensure that the system is not abused.

4.1.2 The path of non-governmental protection is represented by Illinois 'Biological Information Privacy Act' and the 'Commercial Face Recognition Privacy Act' under consideration by the United States Parliament, which are more stringent and more memorable than the general personal information protection.

BIPA is the first law in the United States to protect personal biological information at the state level, which establishes two equally important security protection requirements,one is reasonable attention standards and second, biometric identifiers and biological information must be protected in the same or higher way for ' confidential or sensitive information '. At this point, the victim was also granted private prosecution[10].

4.2 European Union

The EU's General Data Protection Regulation applies to the public and private sectors. GDPR's biological data handling follows in principle the 'principle prohibits, with special exceptions', but data controllers may use the 'consent of the data subject' provision exceptionally. But the consent must be ' free to give, clear, specific, unambiguous ', any passive consent does not conform to the provisions. The EU's General Data Protection Regulations clearly stipulates the processing behavior of information processors. One of the sources of legitimacy is to obtain the consent of information subjects, which information processors must prove. If the consent is made in the form of a written statement, the law stipulate that the consent should also be significantly different from other matters requiring consent. In addition, the information processor should also inform the information subject that it has the right to withdraw consent at any time. It should be as easy as making consent, because consent is the embodiment of the autonomy of the information subject and can dispose of personal information independently.

4.3 Experience of European Union and USA Regulation on Face Recognition

4.3.1 Strengthening Special Legal Regulation on Face Recognition Information.

In all states of the United States, laws related to biometric data, including face recognition technology, are enacted for the protection of face information. Although there is no specific legal regulation in the Federation, some existing laws can also be invoked to regulate face recognition information. Therefore, China can further highlight the legal regulation and protection of special personal information based on personal information protection, such as sensitive personal information protection.

4.3.2 To some extent, private litigation can be limited by public power.

In the protection of face recognition information, the status of information collectors and rights subjects is unequal, and the cost of relief difficulties is high, which is not conducive to the protection of rights and the improvement of enterprise efficiency. Therefore, private relief is limited abroad, which can alleviate the burden of litigation to some extent. Individuals have limited ability to collect evidence in personal information protection. Appropriate intervention in public relief in the need for comfort can improve efficiency and reduce litigation costs.

4.3.3 Make technical specification requirements from the operational level clear.

At the level of technical risk regulation, Europe and the United States have issued relevant legislation to put forward the corresponding technical application norms, engaged in the prevention of technical risks in the pre-and mid-stage, such as the Washington State's Face Recognition Service Law to regulate the use of face recognition services from accountability, manual review, testing, and other mechanisms. EU's 3/2019 Guidelines on Processing Personal Data through Video Devices provide measures to reduce the risk of face recognition, such as encrypting biometric data and formulating key management policies and legal regulation at the technical level.

5. The challenges and difficulties of the existing legal norms on the protection of human face information and the improvement of its path

5.1 The Judgement Standard of Face Recognition Information Obligation Is Not Perfect

Firstly, the Personal Information Protection Law only specifies the obligations of personal information processors and the responsibilities of personal information protection departments. What's more, the Civil Code only stipulates the information security obligations of information processors and the confidentiality obligations of state organs, statutory bodies, and their staff who undertake administrative functions. However, natural persons such as trustees entrusted to handle personal information also have responsibilities in personal information protection, but the law does not specify their obligations. At the same time, whether the obligee subjects such as network users and network information service providers fulfill their duties is also connected with the technical standards of face recognition. There are deficiencies in operational normative documents such as technical security standards.

Therefore, it is necessary to strengthen the evaluation of the impact of face recognition technology on personal information security, including the compliance evaluation of face big data construction, the safety evaluation of face recognition technology update, the update and the maintenance evaluation of face recognition information and its database. Further clarifying the relevant technical standards is conducive to promoting the close connection between the technical application and legal regulation to protect face recognition information better.

5.2 The protection of face recognition information is not perfect

Although China has made special protection requirements and enforcement norms in the collection, storage, and sharing of sensitive personal information in the Personal Information Protection Law, the relevant concepts are not unified with the concepts of civil law, criminal law and administrative law, and the legal system of personal information protection is still relatively imperfect. Therefore, biometric information's importance and unique legal status have not been fully recognized under the private information protection system. This has a negative impact on the protection of face recognition information.

Therefore, it is necessary to pay attention to the protection of sensitive personal information such as biometric information, but from the perspective of legislative and judicial costs, special legislation on biometric information is high, and it is not feasible in China at present. Therefore, according to its particularity, it can be regulated, such as in torts from the special nature of face recognition information to set special rules and compensation standards. It can also increase the protection of sensitive personal information in higher-level laws. The concept of sensitive personal information needs to be unified in civil law, criminal law, and administrative law so that biometric information's importance and special legal status are fully recognized under the personal information protection system.

5.3 Further definition of the basic principles of ' safety, legality, legitimacy and necessity '

The principle is stipulated in the ' Civil Code ' and ' Personal Information Protection Law '. As the basic concept of personal information protection, the principle runs through the relevant rules. However, it is not limited to the current judicial practice. The legitimacy and necessity of collecting and using face information by different subjects are unclear.

Therefore, the basic principle of 'safe, legal, legitimate, and necessary ' for the protection of personal information needs to be further explained in judicial practice. For example, in the first case of face recognition, although the court proposed that 'the collection of face recognition information by Guo and his wife in the wild animal world exceeded the requirements of the necessary principle and was not justified', the principle was not further explained. Therefore, the principle should be further explained and defined through judicial precedents, laws and regulations and judicial

interpretations in individual cases, which is conducive to realizing the legitimacy and rationality of judicial decisions.

5.4 Difficulties in remedying infringement in data space

The face recognition information will be difficult to query and track after the information subject agrees to the information processor to obtain face recognition information. Because in the network space, face recognition information is transformed into network code and cross with other data, it is challenging to identify infringement. It is difficult to locate the actual damage degree, which is often a measure of the game between the two parties. Due to the high imbalance between the data controller and the personal information subject, in the infringement cases involving the use of personal data, users often lose their ability to protect their rights because of the difficulty of proof and the litigation cost of face recognition information infringement is high for all parties.

Therefore, we can pay attention to the combination of public relief and private relief of face recognition information and consider the application of public prosecution to face recognition infringement which seriously endangers the public interest. In addition, according to the characteristics of biometric information protection, we should strengthen the prevention in advance, and the relief afterward often has caused irreparable losses. Therefore, it is necessary to effectively use the ‘pre-litigation injunction ‘system, which is closely integrated with civil litigation and criminal law.

5.5 The connection between legal protection of face recognition information and criminal law is unclear

As for the biometric information of face recognition, the concept category of personal information is not unified, the legal attribute is not clear, and the lack of cohesion in civil law, administrative law and criminal law. Moreover, criminal regulations are often afterwards relief in the protection of personal information[11].As for the general application of personal information crime in different forms of biometric information leakage, forgery, abuse, trading and other acts by using biometrics as the core technology, it is actually unable to play the role of relief, prevention and protection. In fact, the criminal law is absent.China’s Criminal Law does not provide special protection for sensitive personal information such as face recognition information.Thus it can increase for sensitive personal information crime related charges, making criminal law this public remedy more powerful.

References

[1] Wang Xinyuan: ' Risk and Legal Regulation of Face Recognition Technology Application, 'contained in ' Science and Technology and Law (Chinese and English) ' No. 05,2021, p.93-101.

[2] Yang Lixin and Hu Yan: ' Personality Rights of the Interpretation and Case Commentary of the Civil Code of the People's Republic of China, 'China Legal Press 2020 Edition, p.353.

[3] Lu Qinzhong: ' Criminal Law Protection of Credit Card Information Security - - An Analysis of the Crime of Stealing, Purchase and Illegally Providing Credit Card Information, 'Published in Zhongzhou Academic Journal No.03,2013, p.55-62.

[4] Wang Liming: ' Redefinition of the concept of privacy, " Jurists ' 2012 No. 1, p.1005-0221.

[5] Zhang Xiaolei 1, Pang Xueguang 2: ' College students ' personality rights violations and rights relief related issues, 'containing ' learning and practice, ' No. 08,2017, p.90-97.

[6] Yang Lixin : ' Understanding and Interpretation of the Internet Tort Liability ', ' Journal of the State Prosecutor ' s College ' February 18,2010, No.03.

[7] Hao Zhixin : ' Tort Law Protection of Network Privacy ', Jilin University Master thesis, 2011.

[8] Yan Jun: ' Research on the Fault of Internet Service Providers ' Infringement ' Master's Thesis of Shanghai Jiaotong University, 2011.

[9] Zhou Hanhua: ' Research on Xi Jinping's Internet Rule of Law Thought, 'No. 03,2017, p.5-21.

[10] Guan Zheng: Research on Civil Law Protection of Face Recognition Information, Master' s thesis of Beijing Jiaotong University, 2021.

[11] Zhang Xinbao: ' Personal information collection: restrictions on applying the principle of informed consent, 'published in the ' comparative law study ' No. 06,2019, p. 1-20.

[12] Wang Xiuzhe: ' Reconstruction of the legal protection system of personal information in the era of big data ', published in ' Law Forum ' No. 06,2018, p. 115-125.