ISSN 2616-7433 Vol. 5, Issue 15: 63-72, DOI: 10.25236/FSST.2023.051512

Protection of personal information in the application environment of face recognition technology

Liangliang Wang[1,*]

[1]*Anhui University of Finance and Economics, Bengbu, China*
[*]*Corresponding author*

Abstract: *In recent years, with the wide application of face recognition technology, the improper disclosure and illegal trading of face recognition data occur frequently. While citizens enjoy convenience, personal information, personal and property security are also facing severe risks. However, the data security risks brought by face recognition technology have not been paid enough attention by the public. The promulgation of China's personal information protection law on November 1, 2021 provides effective legal protection in the protection of personal information. Although most scholars focus on the data collection and processing process of face recognition technology at the technical level, so as to regulate the abuse of technology, the research on the security of data collected from the application of face recognition technology and its related legal protection is relatively rare. As the application product of face recognition technology, face recognition data has broken through the boundary of traditional legal protection, so it should be substantially recognized and protected. By analyzing face recognition technology and its characteristics, aiming at the current situation and existing problems of face recognition information protection, as well as the comparison of relevant legislative provisions abroad, this paper intends to explore the improvement suggestions of personal information protection law under the application environment of face recognition technology.*

Keywords: *Face recognition technology; Individual information protection; Comparison of legislation inside and outside the domain; Face information; Legal protection; Personal information*

1. Introduction

In the context of the increasing maturity of artificial intelligence and big data technology, the potential value of personal information has never attracted such high attention from society. Face recognition technology, as a representative of it, has been deeply integrated into various fields of society, and plays an important role in the process of social governance modernization, meeting the diversified needs of individual users in different scenarios. However, while this revolutionary technology brings convenience to our daily lives, it also exposes the thorny problems that exist in many applications. Specifically, face recognition technology has the risk of technology abuse and information disclosure, if not regulated, it will lead to a series of problems such as infringement of citizens' personal privacy, threat to property security, and infringement of personal dignity. At present, the current legal provisions on face recognition technology in China are decentralized, especially for sensitive personal information represented by face information, there is insufficient protection.

In the application of face recognition technology, the legal protection of personal information mainly faces the following difficulties: the principle of informed consent is difficult to effectively implement; The statutory grounds for processing sensitive personal information are to be clarified; The administrative supervision of personal information protection is absent; It is difficult to identify the damage and prove the causality of the infringement of personal information rights and interests. In response to the above dilemma, China can refer to the foreign legislative norms on face recognition technology, and according to the actual situation in China, the interests between technological development and personal information protection are measured, according to the scene theory to make detailed provisions on the application of face recognition technology, and prudently use face recognition technology in the case of protecting the rights and interests of personal information[1-3].

By combing and studying the different regulations of the European Union and the United States on the application of face recognition technology and face information protection, it can provide new ideas and reference significance for the improvement of relevant legislation in China. In terms of legislative improvement, the statutory reasons for processing sensitive personal information can be further

ISSN 2616-7433 Vol. 5, Issue 15: 63-72, DOI: 10.25236/FSST.2023.051512

clarified through legislation. In terms of administrative supervision, a special information regulatory body should be set up, and complementary preventive measures and in-process supervision measures should be improved. In terms of judicial relief, the identification of damage caused by facial information should consider relevant factors according to the characteristics of sensitive personal information, and the proof of causality can be selected according to different standards of proof in specific scenarios. Diversified protection should be carried out from the perspectives of legislation, administration, and justice to build a comprehensive and multi-level protection mechanism for citizens' face information, and defend the information rights and interests of every citizen in the era of big data.

2. Current situation of personal information protection under the application environment of face recognition technology

Face recognition technology through the collection, classification and recognition of the character's facial biometric characteristics to realize the identity of the identity of the person, its application is extensive, convenient and efficient, in the modern science and technology social life is widely used. Face recognition information is unique, privacy and high sensitivity, the application of face recognition technology for face recognition information collection, face recognition information once leaked, personal privacy security, personal information security, property security and even personality rights will be more than ever a threat.

2.1. Face recognition technology application environment caused by the difficulty of personal information protection

In modern society, the development of science and technology to keep pace with The Times is an irreversible trend of society, face recognition technology began to be widely used in all aspects of life and work, bringing convenience to citizens' social life at the same time, the public discussion of face recognition technology has not stopped. The application of face recognition technology is related to the vital interests of every information collector, careful use is always good, but in daily life, some places require face recognition is unavoidable, such as banks, schools, communities and so on. In this way, the information subject for the collection of personal information does not have the initiative, some information collectors for personal gain and sell a lot of face information, the information subject to protect personal information there are great difficulties, the reasons can be divided into the following:

1) Automaticity of face recognition technology

In daily life, face recognition technology is widely used in identity verification, security monitoring, health care, public administration, precision marketing and other fields, people from monitoring, cameras and other equipment will be collected face images. However, when these devices collect face images, they do not need to be deliberately catered to, and will automatically collect portraits without the consent of the collected person, and even collect information when the parties inadvertently, the automaticity of this collection method increases the difficulty of personal information protection.

2) The non-contact of face recognition technology

Face recognition is different from fingerprint recognition and iris recognition, fingerprint recognition needs to press the fingerprint several times to collect fingerprint information, and the collected person has the initiative to stop the loss in time. Iris recognition has higher requirements for technology. Iris recognition is to determine people's identity by comparing the similarity between the features of the iris image. Face recognition is a biometric recognition technology that analyzes and compares people's facial feature information. It collects images or video streams containing faces through camera equipment, and automatically detects and tracks faces in the images, and then compares the detected faces with the face database. Therefore, people can be collected face information without touching the collection device[4-8].

3) Parallelism of face recognition technology

When the face recognition technology is applied, it can collect the face image information of most people at the same time and identify and proofread, for example, the shopping mall surveillance camera can collect multiple face information through the monitoring area at the same time. In addition, face recognition equipment may also parallel multiple devices at the same time, so that multiple devices will collect multiple information subjects face information at the same time.

4) The sensitivity of face recognition information

In China's new Personal Information Protection Law, there are many kinds of personal information,

ISSN 2616-7433 Vol. 5, Issue 15: 63-72, DOI: 10.25236/FSST.2023.051512

and its value and sensitivity are different. According to Article 28, sensitive personal information is personal information that, once leaked or illegally used, could easily lead to the violation of the human dignity of natural persons or harm to the safety of person or property, including biometric information, religious beliefs, specific identities, medical and health information, financial accounts, whereabouts and tracks, as well as personal information of minors under the age of 14. Only when there is a specific purpose and sufficient necessity, and strict protection measures are taken, can the processing of sensitive personal information be carried out by the personal information processor. Face recognition information, as a kind of biometric information, once it is leaked or improperly used in any link of the information processing process, it will cause serious damage to the personal dignity or personal property safety of the information subject, especially spiritual damage. The greater the damage caused to the information subject, the higher the sensitivity of face recognition information. The more difficult it is to protect personal information[9-12].

5) The risk of facial recognition information

First, face recognition technology can obtain more comprehensive information about people. According to the operating principle of face recognition technology, face recognition technology to obtain the facial biometric information of the collected person is not only convenient and accurate, the application of face recognition technology seems to collect the facial information of the collected person, but in fact, the powerful information integration function of face recognition technology makes the personal information of the collected person bear a huge risk. Face recognition technology can be combined with cloud computing, Internet and other technologies to integrate with other data of the collector, so as to depict a complete facial portrait of the collector. According to the past, a single artificial intelligence technology can only collect a certain aspect of the personal information of the collected person, but with the progress of modern social technology, a number of face recognition technology advances lead to a variety of data information aggregation, which can depict the comprehensive facial features of the collected person, such as emotional interaction technology, The technology can be explored from the aspects of facial expression interaction, voice emotion interaction, body behavior emotion interaction, physiological signal emotion recognition, text information emotion interaction and so on. The facial expression interaction is based on the analysis of the facial movements of the interviewees, combined with other information of the interviewees and generated a report, so as to obtain the emotional fluctuations of the interviewees. This means that the inner emotional activities of the interviewees will also be analyzed and integrated into public information, and the autonomy of the interviewees to protect the traditional personal information may gradually lose its effect.

Second, the subject of infringement is uncertain. On the one hand, face recognition technology and artificial intelligence technology complement each other, if the face recognition is implemented by a highly intelligent robot, then the infringing subject will be disputed. The academic circle has been disputing whether intelligent robot has the civil subject qualification and should bear the tort liability. According to the rapid development of current intelligent technology, with the continuous progress of low intelligent robots to high intelligent robots, artificial intelligence will have the possibility of obtaining the restrictive subject status in the future, and the subject of personal information infringement liability caused by the independent face recognition of high intelligent robots will become a problem. On the other hand, face recognition technology has a wide range of applications, cameras, monitors and other facial biological information recognition machines all over the streets, and the facial information of people coming and going is collected and recorded by face recognition devices inadvertently. In addition, the collected face information will be collected after a number of links will be analyzed and processed, and in each link there are a number of information users, both may be the developer of face recognition technology, may also be the monitor image recorder, and may even be a profit-oriented villain. Therefore, when the face information of the collector is exposed and violated, it is difficult for the information subject to find the responsible person to bear the responsibility of violating the right to privacy.

Third, the infringement is more hidden. Usually the behavior of infringing face information is indirect behavior, in most cases, the application of face recognition technology will face information disclosure and other problems are attributed to the face recognition equipment's own failure to shirk the responsibility of the actual infringer, but people can do nothing about the failure of electronic equipment, and the responsible people can only bear to eat dumb. In addition, face information as a kind of intangible property, the information subject is collected facial information after facial information is lack of initiative for facial information, so it is difficult to detect hidden infringed behavior in the first time, it is difficult to investigate responsibility in the first time, get compensation. Fourth, the consequences of infringement have irreversibility. The facial information collected by face

ISSN 2616-7433 Vol. 5, Issue 15: 63-72, DOI: 10.25236/FSST.2023.051512

recognition technology equipment belongs to biometric information, which is unique. With the application of facial payment becoming more and more common, face information has become a new and more convenient mobile password. Because of the uniqueness of facial information, it is difficult to modify and save after exposure. The traditional digital password, pattern password can be modified and replaced, the lost mobile phone, bank card can also be reported lost remedy, and the face information leakage after there is nothing to do, the traditional means of protection often do not have a perfect effect, and even the leaked facial information is different information users flow in a variety of procedures, occasions, the damage caused by the consequences are difficult to eradicate, Has a very serious harm and irreversibility, in the long run, the infringed will not only have a strong trouble, the loss may also far exceed the ability of the expected.

2.2. The legislative status of personal information protection under the application environment of face recognition technology

with the rapid development of information technology, face recognition technology has gradually penetrated into all aspects of people's lives. While face recognition technology plays a huge role in many fields, there are also cases of abuse. Since the emergence of artificial intelligence, The State Council and the Supreme People's Court have issued a series of policy documents and judicial interpretations to standardize the application of face recognition technology.

1) Civil and commercial matters

The Guide to the Protection of Personal Information of Information Security Technology Public Commercial Service Information System, promulgated by the State Administration for Market Regulation and the Standardization Committee in 2013, is China's first national standard on the protection of personal information. In 2017, the Cybersecurity Law listed personal information as the object of protection, emphasized the autonomy of information subjects over personal information and stipulated the principles of the collection, storage and use of personal information. The Civil Code, adopted on May 28, 2020, added the content of personal information protection to the Code of personality rights, and included biometric information into personal information, clarifying the principles of "legality, necessity and legitimacy" that should be adhered to in handling personal information. In 2020, the newly revised Code for the Security of Personal Information in Information Security Technology distinguishes between personal information and sensitive personal information for the first time, and lists personal biometric information, including facial recognition features, as sensitive personal information. On August 20, 2021, the 30th session of the Standing Committee of the 13th National People's Congress voted to adopt the Personal Information Protection Law of the People's Republic of China, which will come into force on November 1, 2021. In response to the abuse of facial recognition technology, this Law requires that in public places where image acquisition and personal identification equipment are installed, prominent prompt signs should be set up; The personal images and identification information collected can only be used for the purpose of maintaining public security[13-14].

2) Criminal aspects

The ninth Amendment to the Criminal Law aims to better deal with the increasing theft and sale of personal information in society by relaxing restrictions on criminal subjects and increasing penalties.

3) Judicial interpretation

On July 28, 2021, the Provisions of the Supreme People's Court on Several Issues Concerning the Application of Law to Civil Cases Involving the Use of facial Recognition Technology to process Personal Information were officially released. The Provisions clearly state: "Property service enterprises or other building managers use face recognition as the only verification method for owners or property users to enter the property service area. If the owners or property users do not agree with the request to provide other reasonable verification methods, the people's court will support it according to law." According to this provision, when the property of the community uses the face recognition access control system to enter the face information, it should obtain the consent of the owner or the property user, and for the owner or the property user who does not agree, the property of the community should provide an alternative verification method, which shall not infringe on the personality rights and other legitimate rights and interests of the owner or the property user.

In August 2021, with the widespread use of face recognition technology in real life, citizens' concerns about the abuse of personal face recognition information are also increasing, and the call to strengthen the protection of face information is rising. The Supreme People's Court issued the

ISSN 2616-7433 Vol. 5, Issue 15: 63-72, DOI: 10.25236/FSST.2023.051512

Provisions on Several Issues Concerning the Application of Law in Civil Cases Related to the Processing of Personal Information Using face Recognition Technology, which clearly defined the collection of face information without the individual consent of natural persons or their guardians as "infringement", which not only responded to the legitimate demands of the public for the protection of face information, but also provided a legal basis for judicial departments to handle such disputes. It also enhances citizens' legal confidence in the protection of their personal rights and interests.

2.3. The law enforcement status of personal information protection under the application environment of face recognition technology

Based on real cases, the domestic supervision of face recognition is becoming more and more standardized. The first case of face recognition in China started the first shot of the country's war to strengthen personal information protection. On June 15, 2020, the Fuyang District People's Court of Hangzhou publicly heard the case of Guo Bing v. Hangzhou Wildlife Park service contract dispute. The case is a dispute caused by the upgrade of the entry method of Hangzhou Wildlife Park in 2019. After the admission method was upgraded, the annual pass purchased by plaintiff Guo Bing using fingerprint verification to enter the park was changed to face recognition. The original told that face information, as sensitive personal information, has a major impact on the information subject, and the defendant's short messages and announcements on changing the entrance method are invalid, and forced to collect face information in disguised form, in violation of the Law on the Protection of Consumer Rights and Interests, requiring the zoo to refund the card purchase fee, compensate for related transportation costs and delete the collected information. In the end, the court ruled that Wild Animals World should compensate Guo Bing for the loss of contract interests and transportation expenses, and delete the fingerprint identification information Guo submitted when applying for the annual fingerprint card.

On July 30, 2021, two of the four typical cases of personal information protection procuratorial public interest litigation announced by the Guangdong Provincial People's Procuratorate are related to face recognition, one is to deal with the illegal setting of "face information recognition" access control system in residential areas, and the other is to urge the rectification of illegal capturing of faces in sales venues. The unauthorized installation and use of "face information recognition" access control system in residential communities is easy to lead to the owner's personal information being collected and used by people with ulterior motives, infringing on citizens' personal and property interests, and infringing on social public interests. Jianghai District People's Procuratorate of Jiangmen City, Guangdong Province investigated the communities within the jurisdiction and conducted administrative public interest litigation investigation, held a public hearing, and urged the residential communities, shopping malls, schools and real estate sales departments that set up "face information recognition" access control system in violation of the jurisdiction to perform their duties according to law, rectification of the places with hidden risks and access to the public security network management system within a limited time. The illegal installation of places to be dismantled and cleared of all data processing. Another case is an administrative public interest lawsuit brought by the People's Procuratorate of Hui zhou City in Guangdong Province against the installation of facial recognition cameras in sales offices. Sales office installed face recognition camera is to calculate the performance of sales staff and housing sales, but without the same consumer and unauthorized installation, collection, storage and use of consumer face information behavior caused consumers to panic, so that some consumers wear helmets into the sales department to look at the house. Hui zhou City People's Procuratorate set up a task force to carry out an investigation of the sales department within the city, and eventually urge all the sales offices involved in the investigation to completely rectify and delete the illegal collection of information, and adopt a "look back" policy of timely supervision and urge the illegal departments to rectify.

3. The problems of personal information protection in the application environment of face recognition technology

3.1. The complexity of personal information protection cases

1) The boundaries of personal information that facial recognition technology can collect are unclear

As a private law related to the daily life of citizens, the Civil Code stipulates the protection of privacy rights and personal information in the series of Personality rights, dividing personal information into private information and non-private information. Among them, private information shall first be subject to the provisions of privacy rights, while non-private information and private information not stipulated by privacy rights shall be subject to the provisions of personal information

ISSN 2616-7433 Vol. 5, Issue 15: 63-72, DOI: 10.25236/FSST.2023.051512

protection. The Personal Information Protection Law, which will come into effect on November 1, 2021, classifies personal information into sensitive information and non-sensitive information. As a special law in the field of personal information protection, the Personal Information Protection Law is not related to the Civil Code as a special law and a general law. So whether private information and sensitive information belong to the equivalent relationship, whether non-private information overlaps with non-sensitive information, and how the Civil Code and Personal Information Protection Law are applied in different scenarios has become ambiguous.

2) The authority configuration of the personal information collection system in face recognition technology is unclear

The principle of informed consent is the most important basic principle of the "Personal Information Protection Law" on the processing of personal information activities, and whether the "informed consent" in the application environment of face recognition technology has the scope of definition? In public places, how can the information subject achieve informed consent to the processing of the collected personal information, whether it is partial consent or overall consent, temporary consent or indefinite consent, whether it is a single collection and use consent or repeated consent, these issues need to be specific and clear in specific circumstances. As the application of face recognition technology is more and more extensive, and the connection with daily life is more and more close, such as face payment, face sign, etc., under different social circumstances, different life scenarios, the scope and field of informed consent of the information subject, the content of the rights and obligations of the information collector also need to be clarified in the future more specific provisions.

3) The responsibility of the use of face recognition technology in business venues is unclear

The application of face recognition technology is more and more extensive, not only in the scope of public places, more and more private, business places are also widely used, such as Internet cafes, hotels, small shops and so on. So the "Personal Information Protection Law" for the installation of image equipment in the scope of public places, personal identification provisions are also applicable to the management of business places using face recognition technology to collect, store and use personal information? In terms of risk, the personal information collected by the use of face recognition technology in business places is more likely to be leaked, and more likely to be infringed by people with ulterior motives, so the management and supervision of business places need to be strengthened, and the responsibilities of personal information collection subjects and management subjects also need to be more clear. The "Personal Information Protection Law" should be precise in implementing the responsibilities of business entities for the collection and use of personal information, and punish those who escape the net in a timely and reasonable manner.

4) The field of use of the right to delete facial recognition information is unclear

The Personal Information Protection Law clearly stipulates the right of personal data subjects to delete personal information. Article 47 of the Personal Information Protection Law stipulates that individuals can request deletion of personal information when it is processed by a processor in violation of laws, administrative regulations or agreements. The deletion here is a right of the owner of facial recognition information, and is not based on whether it is agreed in advance, that is, whether it is agreed in advance is not a defense. So, is the subject of information can be asked to delete personal information at any time, that in the field of education, student examination identity information, learning records, examination monitoring and other student personal information can be asked to delete? In the field of daily travel, can the subject request deletion of information such as subway ride records, identity verification when taking high-speed trains, and customs inspection when taking airplanes? The more areas in the society that use face recognition technology, the more content that needs legal regulation, the wider the scope of cross-use of social life information, the boundaries of the use of personal information that information subjects want to protect are blurred, and it is difficult for information subjects to consider thoroughly at one time to protect their legitimate interests.

3.2. The legal supervision measures are not specific

The abuse of new science and technology leads to the inadequacy of legal control. The gradual emergence of new technologies in social life is like a "magic box" that tempts all fields to try, Wrapped in "black technology" or "wisdom" coat of face recognition technology, unlimited in a variety of scenarios are promoted and used, and these use scenarios are in line with the legality, legitimacy and necessity of information processing, whether there is a reasonable regulatory path, there are still big loopholes, otherwise there will not be such as Guangdong Province sales Department illegal installation

ISSN 2616-7433 Vol. 5, Issue 15: 63-72, DOI: 10.25236/FSST.2023.051512

of face recognition camera cases. There are some other subtle illegal use of face recognition equipment hidden in the law has not yet regulated the place, and even some regulatory authorities lax law enforcement, accepting bribes will let these illegal phenomena escape, infringe on the personal and property interests of more citizens, serious also cause social panic, like wearing a helmet into the sales department to see the consumer, Infringe on the public interests of society.

3.3. The imperfection of the legal relief system

The rapid development of the Internet era and the proliferation of counterfeit technology, resulting in the face information infringement results spread widely and quickly, and extremely difficult to recover as before. At the same time, due to the unequal status of technology and information, it is easy for individual citizens to increase the difficulty of safeguarding their rights because of the lack of professional information technology knowledge. In addition, although the "Personal Information Protection Law" has increased the penalty amount to deter illegal information processing behavior, but from the existing scale of the face recognition industry, whether the penalty of one million has sufficient deterrence, whether it can effectively prevent the processor from "taking risks" due to interests, it is doubtful. Finally, at present, the scope of relief provided by the Personal Information Protection Law is limited to civil aspects, and the liability provisions are limited to the tort and damage liability of the personal information processor. Although the Provisions of the Supreme People's Court on Several Issues concerning the Application of Law to Civil Cases Involving the Processing of Personal Information Using Face Recognition Technology, which came into effect on August 1, 2021, and the Notice on Implementing the Personal Information Protection Law and Promoting the Inspection of Public Interest Litigation for the protection of Personal Information, which was published on August 21, 2021, provide a stronger protection for citizens' personal information Strong public relief support, however, still need to further improve the law.

4. The legislative provisions and comparison of personal information protection under the application environment of extraterritorial face recognition technology

The development of science and technology is a double-edged sword. The positive effects of a certain technology cannot be overturned just because of its negative effects. Instead, strict laws should be adopted to regulate the abuse of technology to protect personal information. Since entering the Internet era, major developed economies have established a series of regulations on the protection of personal information in order to regulate the abuse of personal information with the help of intelligent technology, the most representative of which are the United States and the European Union.

4.1. The United States: Special legislative provisions

Because the United States implements a federal system in the relationship between the central and local governments, the United States has fewer legislative provisions on the protection of face recognition information, and is generally regulated by independent legislation of the states. At the federal level, the United States has nearly forty laws on the protection of personal information, which determine the basic principles of the protection of personal information in the United States, such as the law of fair information time, and further clarify the right to know, the right to consent and the right to correct under the law. In 2019 and 2020, the US Federal Privacy Protection Act (Draft) and the Ethical Use of Face Recognition Act (Draft) were passed respectively to regulate the use of face recognition technology by corporate entities and government agencies to profit from personal biometric information. At the level of individual states, the state of Illinois passed the first law in the United States in 2008 to regulate the collection, use, processing, protection, storage, and destruction of biometric identifiers and information, namely the Biometric Information Privacy Act.The Act clearly stipulates that only the written consent of the information subject can process the face biometric information of the information subject, so as to ensure that the information subject actively rather than passively makes decisions about sensitive personal information, and strengthen the control and protection of personal information; In terms of face recognition information processing, it requires all kinds of organizations, including enterprise associations, to adopt a more stringent way to collect, store and transmit all biometric information. In 2009, Texas passed the "Biometric Information Privacy Act", which emphasizes that the biometric information of the information subject shall not be obtained without the consent of the information subject. Biometric information cannot be sold or disclosed to third parties unless certain conditions are met. In 2017, the U.S. state of Washington passed Washington State Assembly Act 1493 to regulate the conduct of individuals and non-government entities (primarily businesses) in the collection, storage and use of biometric information. After that, states and cities in the United States have introduced regulations prohibiting the use of face recognition technology by

ISSN 2616-7433 Vol. 5, Issue 15: 63-72, DOI: 10.25236/FSST.2023.051512

individual departments. In 2020, Portland, Oregon, adopted the "Facial Recognition Ordinance", which bans the use of facial recognition technology by public institutions and prohibits private companies from using facial recognition technology in public places.

4.2. European Union: Provisions for harmonizing legislation

The EU's processing rules for face recognition information are generally stricter. In the 1980s, the member states of the Council of Europe signed the European series of treaties No. 108 "Convention on the Protection of Automatic Processing of Personal Data" in Strasbourg, France, which became the first international convention to clearly define specific personal data. In 1995, the European Parliament and the Council of the European Union adopted the Directive on the Protection of the rights of Individuals in relation to the processing of Personal Data and the Free Flow of Personal Data (Directive 95), which provided standards and guidelines for the unified regulation of the data market in the European Union. Eu legislation entered a milestone stage -- the Directive era. On May 25, 2018, the European Commission's Proposal for a Regulation on Data Protection in the Processing of Personal Data and the Free Flow of related Data, the most stringent personal information protection law in history, the General Data Protection Regulation (hereinafter referred to as "GDPR"), came into force, replacing Directive 95 and becoming a directly applicable law within the EU. Giving individual member states discretion and formalizing uniform data protection rules, it has attracted worldwide attention.The GDPR protects both general information and special types of information, which include personal biometric data, including facial image data. The GDPR also addresses the issue of conflicting portrait and privacy rights by stipulating that only images that have been processed with certain techniques to identify a specific natural person can be considered biometric data. The GDPR also gives data subjects the right to claim erasure of all personal data stored by users' services, as well as a wider range of citizens' data rights, and provides avenues for relief.

4.3. A comparison between extraterritorial legislative provisions and China

Comparing the two European and American legislative provisions on the protection of personal information, the common denominator is the value tendency of holding personal rights and interests priority protection. The difference is that the United States mainly through a variety of specialized legal norms, strict and detailed provisions of biometric data collection, storage, use and destruction of the way and process; On the basis of the General Data Protection Regulation, the European Union seeks to maximize the protection of personal information by attaching restrictions to the reasonable circulation of personal data. China's existing laws have certain limitations on the scope of protection of personal information processed by face recognition technology, which is limited to the field of strong professionalism and commerciality, and there are few regulations on the application of face recognition technology to process personal information between equal subjects. In a series of processes such as collection, use and storage of personal information, information processing subjects. There are no clear provisions on the obligations of relevant subjects such as the responsible subject. In the process of improving legislation, no matter what model of learning from Europe and the United States, it is worth studying carefully, and formulating the most favorable laws for the protection of citizens' personal information to benefit the people.

5. The improvement of personal information protection in the application environment of face recognition technology

5.1. Detail the classification and protection of personal information

According to Article 28 of the Personal Information Protection Law of China, sensitive personal information is personal information that, if leaked or illegally used, is likely to cause damage to the human dignity of natural persons or harm to the safety of person or property, including biometric information, religious beliefs, specific identities, medical and health information, financial accounts, and movement tracks. As well as personal information of minors under the age of 14. The Provisions of the Supreme People's Court on Several Issues Concerning the Application of Law in Civil Cases Related to the Processing of Personal Information Using Face Recognition Technology, which came into effect on August 1, 2021, classifies face information as biometric information, and the processing of face information includes the collection, storage, use, processing, transmission, provision and disclosure of face information. In order to refine the classification and protection of personal information, it is necessary to stipulate the infringement liability and punishment degree according to different information application scenarios, from the various links of information collection means, storage method, scope of use, processing method, transmission tool, content provided, open field and

ISSN 2616-7433 Vol. 5, Issue 15: 63-72, DOI: 10.25236/FSST.2023.051512

other aspects of information technical modification, respectively. Let the infringer have nowhere to escape, and let the person who wants to infringe take the initiative to retreat.

5.2. Clarify specific legal supervision measures

Science and technology is a double-edged sword, in the big data society, law is a traditional regulatory technology, to catch up with the pace of The Times, law also needs the blessing of modern science and technology. Since face recognition technology can pose a threat to the protection of citizens' personal information, we can also change our regulatory thinking, use science and technology to regulate science and technology, use special laws and science and technology complement each other in the regulatory mode, strengthen the ability of data analysis and application, and realize the intelligent supervision and accurate supervision of modern special laws. First of all, personal information protection monitoring platform can be established by individual citizens according to personal identity verification through the National Cyberspace Administration, so as to obtain anonymous data to hide identity information login with the National Cyberspace Administration network of personal information protection monitoring platform, in addition to the consent of the individual and the state legal authorization to allow the case, control personal information data platform will not transmit information to the third party. Secondly, increase the risk warning function of the intelligent monitoring platform. In the case that the information subject cannot judge whether he should agree to the use of personal information, the early warning system of the intelligent monitoring platform will make a judgment in advance and provide warning information for the information subject, so as to protect the interests of citizens. In addition, if the individual consent behavior is made by mistake, ignorance or under duress, the intelligent monitoring system will also trigger the alarm function, timely block the transmission of information, and minimize the risk of personal information data disclosure.

5.3. Improve the specific legal relief system

The life of the law lies in the implementation, the effectiveness of the law lies in the relief, the effectiveness of the relief mechanism depends on whether the relief channels are smooth and whether the relief means are effective. Judicial relief is the bottom line and the most effective means. In the judicial practice of our country, most citizens protect their rights by means of after-action relief after being infringed because of their weak legal consciousness. For the infringement of personal information, most of the ways for Chinese citizens to get relief are to compensate for the loss, apologize, etc., but the real impact of the infringement is far from compensation can make up for. At present, in the field of face recognition, face information has its particularity, and the risk is much greater than that of fingerprint information. As a simple means of relief, after-action relief cannot compensate for the trauma caused by the infringement on the personal dignity of the information subject. In reality, due to the lag stipulated by the law and the weak legal awareness of individuals to protect personal information. Only a very small number of cases concerning face recognition infringement of personal information enter the judicial process. If it is still in accordance with the principle of "who advocates, who provides evidence", then it is very unfavorable for the infringed information subject who is not familiar with face recognition technology, and the technology obviously has a higher information control ability and evidence collection ability. Therefore, in the judicial relief process of face recognition cases, the rule of reversing the burden of proof is adopted. As long as the information subject provides preliminary evidence to prove the occurrence of an infringement or even the possibility of an infringement, there is no need to bear the burden of proof for the actual occurrence of the damage results. By the technical controller to provide evidence to prove the legality of their own behavior and the occurrence of no causal relationship with the consequences of damage, otherwise it is necessary to bear the burden of proof cannot be proved. To sum up, considering the information subject's ability to provide evidence and the risk of preventing the result, the specific relief system of special laws should be perfected, the preventive and protective functions of laws should be realized, and the legitimate rights of information subjects should be fully protected.

6. Conclusions

Economic and social development to promote scientific and technological progress, the development of modern social science and technology with each passing day, face recognition technology as a product of the new era has gradually spread to a wider range of fields, I believe in the near future, face recognition technology in depth and breadth will be further extended. At the same time, the application scenarios of face recognition technology will be more extensive in the future, and face information will gradually become the core production factors of some industries. However, face

ISSN 2616-7433 Vol. 5, Issue 15: 63-72, DOI: 10.25236/FSST.2023.051512

recognition technology is like a double-edged sword, while enjoying the technology to bring great convenience to people's lives, the legal risks of face recognition technology cannot be ignored, and the abuse of face recognition technology may seriously threaten the privacy of individuals, personal freedom, personal and property security. The introduction of the "Personal Information Protection Law" undoubtedly gave us a layer of protective clothing, but now the face recognition technology is still weak artificial intelligence, when the strong artificial intelligence technology appears, the protection of personal information will be more important, the "Personal information Protection Law" amendment and improvement need to constantly catch up with the pace of development of The Times, a variety of specialized laws are also urgently needed to be introduced, To protect the rights of citizens, society and the state in an all-round way.

Acknowledgements

The completion of this paper is inseparable from the support and help of teachers, classmates and friends. Here, I would like to express my heartfelt thanks to them.

My supervisor Yan Shao gave me comprehensive and detailed guidance in the process of completing the thesis, and made great efforts in the selection of the topic, the revision of the outline and the completion of the thesis. Although she is very busy at work, she still takes the time to give me careful guidance and support. She helped me solve the problems I encountered in my research, so that I avoided many detours in the writing of my paper.

In addition, from the topic selection to the completion of the paper, my classmates have given me great encouragement and support. They often ask me about my work, life and the completion of my papers, and make reasonable suggestions based on their experience, and often remind me to take my papers seriously, not to be careless at any time, and to be careful when revising them. In addition to my family, they have given me meticulous care in life and work, and now I have the research results of my thesis.

References

[1] Resheng Zhang. Face Detection behind Face brushing Face Recognition Face retrieval [M]. Beijing. Publishing House of Electronics Industry, 2017. 23-34.
[2] Rong Wang. The Era of Big Data [M]. Beijing. Posts and Telecommunications Press, 2017. 45-55.
[3] Yuan Li. Research on Personal Information Protection in the Era of Big Data [M]. Wuhan. Hua zhong University of Science and Technology Press, 2019. 56-67.
[4] Huaqiang Cui. Research on Private International Law of Online Privacy Rights Protection [M]. Beijing. Law Press, 2016. 46-53.
[5] Hong Wang. Review of current regulations and analysis of legislative trends of Face recognition technology application [J]. Journal of Northeast Normal University (Philosophy and Social Sciences Edition), 2022(03). 78-86.
[6] Nan Ni, Min Wang. Legal regulation of Personal Information protection in Face recognition technology [J]. Journal of Humanities, 2022(02). 121-131.
[7] Jingjing Wei. Research on the legal Issues of Face Recognition Technology Application in the Civil Field [J]. Journal of Hubei Second Normal University, 2022, 39(01). 61-65.
[8] Zhongshao Gao. Legal Regulation of Face Recognition Information Processing Behavior [J]. Learning Forum, 2022, 20(02). 56-59.
[9] Yanling Jiao. Identification of Tort Liability for Face Recognition [J]. Social Sciences of Chinese Universities, 2022(03). 78-86.
[10] Junping Liu. The Dilemma of Face Recognition Data Protection and its legal Solutions [J]. Science and Law, 2021(02). 44-49.
[11] Jiayou Shi , Siqi Liu. Personal Information Protection in Face Recognition Technology -- on the construction of dynamic consent model [J]. Law of Finance and Economics, 2021(02). 60-78.
[12] Lang Jin. Research on Face Recognition Application and Protection Path [J]. Journal of Qiqihar University (Philosophy and Social Sciences Edition), 2021(03). 88-92.
[13] Shifang Shang, Yanling Jiao. Ethical Considerations on Personal Information Protection in Face Recognition technology Application [J]. Chinese Medical Ethics, 2021, 34(09). 1133-1138.
[14] Yuxuan Zhang. Personal Information protection under face recognition technology—taking design protection as the approach [J]. Journal ofHenan Polytechnic University (Social Science Edition), 2021, 22(02). 18-24.