

A Research on the Protection of Personal Information in the Context of Face Recognition Technology

Yating Wang *

Harbin University of Commerce, Harbin, China

* Corresponding Author Email: 617278486@qq.com

Abstract. The rapid development of science and technology, coupled with the extensive use of the Internet, has led to the emergence of face recognition technology as a prominent high-tech power, which has become an integrated part of people's daily life. While facilitating convenience in life, face recognition technology also presents a multitude of legal risks and challenges. The diversity and opacity of the Internet provide an optimal environment for those engaged in illicit activities to exploit its shortcomings for a range of illegal and criminal pursuits. As restrictions on the use of face recognition technology are lifted and its scope of application expands, the risk of data leakage and violations of individual privacy, as well as its potential use as a tool for crimes, continues to rise. China still has deficiencies and vulnerability in the implementation of face recognition technology. For instance, the pertinent legislation and regulatory frameworks governing the face recognition industry and the collection and utilization of personal data remain somewhat ambiguous and incomplete, which may result in the infringement of privacy rights. It would be prudent for China to draw upon the experiences and solutions that have been developed domestically and abroad to improve and tailor the existing legal system and regulations to the country's specific circumstances. This approach would serve to reinforce the protection of personal information, facilitate the more effective utilization of the technology for the benefit of the nation and society, enhance convenience for citizens, and reinforce their sense of security and well-being.

Keywords: face recognition technology, personal information protection, privacy protection, legal system, rules and regulations.

1. Introduction

1.1. Background and Significance of the Study

The development of the economy and society has witnessed a rapid growth in the application of face recognition technology in recent years. Nevertheless, while this technology offers great convenience, it also gives rise to numerous issues. For instance, the safeguards to protect personal biological information are not entirely effective, which can result in the disclosure of such data. Furthermore, big data analysis may be employed to speculate on private information such as personal hobbies, occupations, and even home addresses from the biological information collected legally or illegally, from which huge profits can be made. In the context of rapid Internet development, individuals may unwittingly leave a trail of personal information across their browsing histories, comments, and videos they consume. In addition to the aforementioned biometric traits, such as the face, fingerprints, palm prints, voice prints, and facial recognition features, which are commonly known in daily life, personal bio-information also encompasses genetic data, ear features, and iris patterns. The face recognition technology is widely applied in the contemporary society, benefiting a diverse range of domains including national security, commercial transactions, public safety, and online healthcare. Despite the existence of certain provisions in the Civil Code, the Personal Information Protection Law, the Cybersecurity Law, and the Law for Protection of Consumer Rights and Interests, as well as their associated implementing regulations, there remain some notable deficiencies.

1.2. Significance of Research

In light of China's accelerated economic and social advancement, coupled with shifts in the social milieu, there has been a discernible rise in public consciousness regarding the privacy protection. This greater legal demands on the safeguarding of personal data. Despite the existence of pertinent provisions within the Civil Code, the legal framework remains insufficient with regard to the means of defending one's rights and interests, the presentation of evidence, and the clarification of the rights and obligations in response to the infringement of personal information caused by facial recognition technology. However, the role of face recognition technology in public services, commerce, financial payments, and overall security of big data is of significant importance. In order to address these issues, it is essential to draw from experiences and identify challenges to facilitate the reasonable application of face recognition technology while better safeguarding personal information and hedging the risks.

2. Research Content and Methods

2.1. Research Content

The author will present the background by clarifying the origin and definition of face recognition technology, identifying its characteristics, and briefing the current development of face recognition technology. Subsequently, the author will conduct a comprehensive examination of the legal risks associated with face recognition technology, including the infringements on personal information or other rights, the various types of information security risks, and the possible lack of supervision. Additionally, the author will discuss the differences between face recognition and other biometric methods. By conducting a comprehensive examination of the legal and regulatory framework surrounding face recognition, the author aims to elucidate the current challenges and experiences of China's legal construction in this domain, with the objective of enhancing the pertinent legal system. In light of the current applications and the challenges facing the face recognition in China, it is imperative to draw upon the experiences of Western countries in regulating face recognition technology and optimize the legal framework in China. The author emphasizes the role of legal protection, featuring the enactment of specialized regulations, the reinforcement of governmental functions, the enhancement of administrative supervision, the self-restraint and self-regulation within the industries applying face recognition technology, and the establishment of a comprehensive protection system for personal facial information.

2.2. Research Methods

(1) Literature Research Method. By conducting a comprehensive review of pertinent literature, the author made a systematic understanding of the national laws and regulations pertaining to the protection of personal information, and of the theoretical findings concerning the legal protection of privacy in the context of artificial intelligence.

(2) Comparative Research Method. By employing the comparative research method, the author introduced the advanced experience of foreign countries in protecting personal privacy information in relation to the face recognition technology and compared with the status quo of China. This approach makes it possible to learn from successful practices of foreign countries and improve the domestic system for rights protection accordingly.

(3) Empirical Research Method. The author employs the empirical research method to investigate potential improvements to the current legal norms for the protection of personal information related to the face recognition technology in China, as well as relevant typical cases, in the effort to ascertain the most effective measures that are in line with the current situation in China, for personal information protection in the context of artificial intelligence.

3. Innovations and Shortcomings

3.1. Innovations

The rapid development of face recognition technology has led to an increased risk of privacy leakage. The protection of personal privacy while enabling the technology to provide services to a variety of industries represents a significant challenge that must be addressed. This paper will discuss the application of face recognition technology and the new issues it raises with regard to the protection of personal information. While numerous scholars have acknowledged the novel challenges posed by the advent of artificial intelligence and have conducted many researches on the safeguarding of citizens' privacy and the protection of personal information, the application of face recognition technology and the associated issues on personal privacy are still considered a relatively nascent research area. This paper's distinctive contribution lies in the summary of prior research findings and to take a further step to discuss personal information protection in the context of face recognition technology based on these findings.

3.2. Shortcomings

The theoretical frame in the paper requires further refinement due to the lack of literature references and the limited academic expertise of the author. Furthermore, the related issues in the field of criminal law involving face recognition are not sufficient, leaving a considerable room for improvement. It is hoped that this paper will make a modest contribution to the protection of personal information in the context of face recognition technology.

4. Text

The information associated with face recognition is sensitive to a certain degree, and it is this quality that makes the protection of such information a more complex undertaking in actual practice. The extant legislation and judicial interpretations in China failed in providing a perfect answer to the normalization of face recognition and the protection of personal information arising from the spread of face recognition technology. For example, the remedies in the event of the theft of face information, the accountability of the entities utilizing face recognition technology, and the methods of safeguarding personal data in the context of face recognition technology. Consequently, an analysis of the application scenarios, purposes, limitations and principles of face recognition technology is essential for the protection of people's personal data.

4.1. Face Recognition Technology and Its Application

Today, the widespread use of artificial intelligence, big data, and the Internet of Things has brought about a multitude of conveniences for the general public. Nevertheless, as public awareness of self-rights grows, so do people's concerns about the global proliferation of high-tech products. People can't help but wonder, "Is my personal information at risk?" In order to more effectively safeguard the personal information, it is essential to make a comprehensive assessment of the impact of facial recognition technology on personal information and the obstacles we have encountered in protecting it.

4.1.1. The Concept of Face Recognition

Face recognition is a biometric technology for identification based on the analysis of human facial features. It is a set of related technologies that use cameras to capture images or video clips containing human faces, automatically identify and track the faces in the images, and then perform face recognition on the detected faces, also known as portrait recognition, facial recognition, and so on. The term "face recognition" is typically used to refer to the process of identifying and verifying individuals based on their optical facial images. Article 5.2.2(c) of the Practice Guidelines for Cybersecurity Standards - Classification and Grading Guidelines for Network Data, as formulated in

December 2021 by the National Technical Committee 260 on Cybersecurity of Standardization Administration of China, defines that “the individual biometric information refers to the original information and comparison information of individual biometrics identification, which includes biometric information such as face, fingerprints, gait, voiceprints, genes, iris patterns, etc.” It can be concluded that face information is a form of biometric information. Furthermore, the Civil Code of China explicitly lists biometric information as a form of personal data, which means that facial recognition information falls under the scope of personal information protection.

4.1.2. Technology Application

In recent years, the accuracy of facial recognition has made great strides, bringing the technology to the stage of large-scale commercial application, including security, finance, transportation, law enforcement, to name a few. This paper will make discussions based on some typical areas of application.

(1) Internet+Healthcare

The technology of face recognition has been widely used in various fields due to its contributions to efficiency and convenience, and it has demonstrated its unique advantages in the field of healthcare. The application of the technology in this field covers a wide range of scenarios from medical checkups in communities to large-scale medical institutions, which not only improves the efficiency and quality of medical services, but also provides patients with a more convenient and safer experience. For example, digital physical examination devices (such as electronic blood pressure monitors, weight scales, glucose meters, etc.) used in physical examinations at community level are able to match the test data together with the patient's facial information and store them in electronic medical records or health files, making it easy for doctors and patients themselves to quickly understand their health status, which in turn helps in formulating optimal treatment plans.

(2) Public Security

The technology of face recognition plays an important role in the field of public security, and its wide application has brought a lot of convenience to people's lives and work, especially in criminal investigation and apprehension of criminal suspects. The combination of “face recognition” and video surveillance has become a typical model for the application of this technology, which is considered an important approach in maintaining social stability. Facial recognition systems have been commonly used in many hotels, guesthouses and B&Bs.

(3) Transportation

Traffic enforcement agencies across China have begun to promote the facial recognition technology to monitor vehicles and pedestrians for offenses such as running red lights. In the travel sector, train stations have adopted the technology to identify passengers and ensure legal entries, which not only improves travel efficiency but also reduces tedious duplication of efforts by service providers.

(4) Life Scenes

The technology of face recognition is also used in everyday life, such as in property management. The technology not only improves the security of neighborhoods, but also offers residents a more convenient living experience. Thanks to the technology, residents no longer need to carry keys or access cards, and can easily enter apartment complexes by simply scanning their faces. In the past, some local laws have often encouraged the use of facial recognition. For example, Article 29 of the Measures for Property Management in Weihai City in 2022 (amended in 2022) states that: “Residential complexes are encouraged to build security systems including video surveillance, face recognition devices and vehicle recognition devices to enhance security. The data of the security system shall be shared with the public security authorities.” However, there are also some residential complexes that force owners to have their faces scanned to enter and exit the complex or unit door without their consent.

4.2. Application Risks Deserve Attention

The prevalence of face recognition technology in various scenarios will inevitably result in the collection of a greater volume of personal information from the public. It is therefore essential to give full consideration to the various risks associated with the use of this technology and the typical ways in which this technology infringes upon personal information. This will enable more effective monitoring of this technology and the protection of personal information.

Facial information, classified as a type of biometric data, is distinctive, directly identifiable, easy to collect, non-anonymous, multi-dimensional, and immutable. Once stored, it can correspond to a specific individual for an extended period. It is important to note, however, that there is also a potential risk of leakage of facial information. In contrast to encryption techniques such as passwords and fingerprints, it is challenging to maintain the security of face information by modifying or replacing it once it has been disclosed. The leakage of face information may result in the exposure of personal privacy, which can subsequently lead to a range of major threats in various domains, including public safety and law aspects, jeopardizing personal and property safety. For example, in August 2019, a database of Suprema, a biotech company, was exposed to the public, resulting in the unauthorized disclosure of the biometric data of over one million individuals, which included facial features and fingerprints collected by the Metropolitan Police Service, UK, local small businesses, and major government agencies [1]. In consideration of the pervasive nature of data breaches involving face information, it is evident that conventional forms of compensation are inadequate to fully address the associated losses. Furthermore, the dissemination of leaked facial information is typically conducted via the Internet, which renders the identification of liability a challenging endeavor. In the context of data breaches involving facial features, it has become a significant problem to determine the accountability of the designers, users, and regulators of these algorithms, as well as to identify the perpetrators. The current principle of fault liability is inadequate to apportion these liabilities clearly, and the absence of reasonable standards creates challenges in asserting and defending rights. In the absence of clearly defined criteria for the allocation of liabilities, it will be complicated to protect rights and interests through litigation, and it will be even more difficult to recover damages resulting from the leakage of face data.

A data breach that occurred in 2019 resulted in the unauthorized disclosure of 2.5 million individuals' facial information stored by Shenzhen SenseNets raised widespread concerns about the security of personal data in the community [2]. In a series of experiments, technicians extracted facial information from photos and synthesized it into a dynamic face. They then placed the dynamic face video, stored on a cell phone, in front of a face recognizer in a supermarket. It seems that the payment can be made with the synthesized face video alone, without the person in question being physically present to authorize the transaction.

4.3. Status and Effectiveness of the Face Recognition-related Legal System in China

The Personal Information Protection Law of China explicitly specifies the fundamental tenets of personal information processing, including: lawfulness, legitimacy, necessity, honesty, transparency, clarity of purpose, and minimization of processing, etc. In addition, the law imposes more rigorous conditions and procedures for the processing of personal biometric information. It is stipulated that such processing must be authorized by the individual concerned and must be carried out for a specific purpose and with sufficient necessity. The Regulations on Security Management of Face Recognition Technology Application (Pilot) (Draft for Public Comments) provide further regulations on the application of face recognition technology, including the conditions of use, obligations to protect the personal information, offering specific guidance for administrative enforcement. The Decision on Strengthening the Protection of Network Information, adopted by the Standing Committee of the National People's Congress on December 28, 2012, contains provisions on the protection of citizens' personal information. Articles 14, 29, 50, and 56 of the Law for Protection of Consumer Rights and Interests (amended in 2013) provide for the protection of consumers' personal information. In order to achieve this objective, China has introduced a series of laws, regulations and policies to protect the

security of personal information. Such legislation includes the Cybersecurity Law of the People's Republic of China and the Personal Information Protection Law of the People's Republic of China, among others. These legal instruments provide explicit stipulations regarding the collection, utilization, and safeguarding of personal data. Furthermore, the safeguarding of minors' personal information has become an even more crucial issue in the context of the growing prevalence of face recognition technology. The State Council promulgated the Regulation on the Protection of Minors on the Internet, which includes a dedicated chapter (Chapter 4) on the “protection of personal information online” for minors. This serves to reinforce the protection of minors' personal information.

The Amendment VII to the Criminal Law of the People's Republic of China in 2009 introduced two new criminal offenses: “selling or illegally providing citizens' personal information” and “illegally obtaining citizens' personal information”. These were subsequently consolidated into a single criminal offense, namely “selling or illegally providing citizens' personal information”. Article 253-1 of the current Criminal Law of the People's Republic of China defines the crime of “infringing on citizens' personal information”. This is defined as the sale or provision of citizens' personal information to third parties in contravention of pertinent state regulations. In cases of severity, the criminal shall be sentenced to a term of imprisonment of up to three years or to criminal detention, and shall be fined concurrently or singly. In cases of significant severity, the criminal shall be sentenced to a term of imprisonment of between three and seven years, and shall be fined concurrently. Furthermore, Article 44 of the Cybersecurity Law of the People's Republic of China addresses the protection of citizens' personal information. Besides the laws, the Regulations on Property Management of Residential Complexes in Chuzhou City, Regulations on Property Management of Residential Complexes in Fuyang City, Regulations on Property Management in Yancheng City, and Regulations on Property Service Management in Guang'an City all stipulate that property management services shall not engage in the following behaviors: forcing property owners and property users to access the shared facilities and equipment by sharing their biometric data, such as fingerprints and face features. The practice of mandatory face recognition has recently been abandoned in numerous locations in order to safeguard the privacy and security of travelers. The Shanghai Municipal Public Security Bureau has emphasized the prohibition of “mandatory face-scanning” for travelers who have brought their ID cards with them. Furthermore, the bureau has produced a standard “Flowchart for Accommodation Registration of Travelers” which requires that hotels seek travelers' consent before conducting face verification [3].

4.4. Problems Remaining in the Protection of Personal Information in the Context of Face Recognition Technology in China

The impact of technologies on people's social lives is often a double-edged sword, and this is also true of face recognition technology. While the technology offers significant convenience and is widely welcomed across various domains, it is undeniable that there are some practical problems with its utilization. The current legal framework is inadequate in terms of safeguarding personal information and lacks clear mechanisms to protect individual rights. Consequently, public authorities face significant challenges in protecting the public's right to privacy. Furthermore, the goal of the effective protection of personal information has been made even more unachievable due to the public's apathy towards the importance of rights protection and the fact that some enterprises fail to adhere to the requisite principles in the utilization of face recognition technology. It is thus imperative to undertake a detailed examination and analysis of the issues pertaining to the safeguarding of personal information in the context of face recognition technology.

4.4.1. Low Awareness of the Public Regarding the Personal Information Protection

While the advent of face recognition technology has brought about a host of benefits in China, it has also given rise to concerns about the protection of personal information. The awareness of personal information protection is relatively inadequate. The accelerated application of new technologies, such as big data and artificial intelligence, has resulted in the pervasive collection and processing of personal information. However, the relevant laws and regulations may not have kept

pace with the technological advancements. Furthermore, there is information asymmetry between information collectors and common users. Users are frequently uncertain about the manner in which their information is collected, utilized, and safeguarded. The transmission of data, images, and videos over the Internet, as well as the sharing of personal locations through social software, often occurs without individuals being aware of the risks to their privacy. The pervasive deployment of face recognition technology increases the risk of perpetrators exploiting the facial data for illicit purposes. In addition to the lack of awareness of the public, the lack of awareness of businesses is also a significant contributing factor. To illustrate, a certain project developed in Jinjiang District, Chengdu City, serves as a case in point. In order to identify the customers, the parties involved installed a risk control system featured AI face recognition in the sales department, which was utilized to capture face images of the customers who visited the premises without their consent [4].

4.4.2. The Data Collectors Have Failed to Fulfill Their Obligation to Protect the Data

The development and use of equipment for face recognition are no longer the domain of a few large companies. Instead, a growing number of companies are applying this technology by purchasing equipment and services, which has resulted in an increasing diversity of the entities engaged in the collection of face-related data. Nevertheless, a considerable number of enterprises have yet to implement adequate measures for the protection of face data, or even to recognize the risk of information leakage and its potential consequences. This suggests a significant lack of awareness and effort on the part of companies as data collectors to protect data.

The collection and use of face data can be divided into two distinct categories: online and offline. In the online scenarios, Internet platform companies typically present users with a “face authentication” service agreement. Only after the user has consented to the terms of this agreement will the company proceed to collect the face data. And the data will be transmitted directly to the enterprise's cloud server. In such instances, the network service provider, the entity responsible for data collection, and the subject of data collection, is often the same company. Accordingly, the user may be aware of the identity of the entity responsible for data collection. However, the service agreement frequently neglects to specify the company's intended use of the face data, the valid duration of the authorization, and the security measures to be employed. In addition, the precise scope of the company's responsibility for data security is often not explicitly explained.

On the other hand, during the offline data collection, the controller of the face recognition device is often not the data processor, creating challenges in defining the respective responsibilities pertaining to data security. To illustrate this point, consider the case of an access control system using face recognition installed in a residential complex in Hangzhou City. In this case, the property management company procured face recognition equipment developed by a technology company and mandated that the residents record their face data into the system. The data is stored on the back-end servers of several third parties, including the property management company, the sub-district office and the public security authority. In the application of face recognition technology, the involvement of multiple entities in the process of data collection and storage can render it challenging for citizens to ascertain the source of potential data leakage.

4.4.3. The Significant Deficiencies in Law Enforcement

First, with regard to the primary body of law enforcement, it is evident that there is a dearth of cross-departmental collaboration among various law enforcement departments. The technology of face recognition touches many departments and areas, thus requiring cross-departmental cooperation to ensure the security of personal information. Nevertheless, while tackling with actual problems, the issue of multiple enforcement keeps reoccurring. To illustrate, there is a notable absence of collaboration and communication between the diverse entities including the market supervision departments, cyberspace administrations, public security departments and so forth. This lack of coordination often results in the failure to share information, the existence of overlapping regulations, and the emergence of regulatory gaps. Despite the enactment of legislation and regulatory frameworks governing the use of face recognition technology and the protection of personal data, law

enforcement agencies may still be lacking in their strictness and timeliness in the actual enforcement of these regulations when the law enforcers fail to promptly detect and halt violations of personal privacy, resulting in the inappropriate utilization of facial recognition technology by certain businesses or individuals for the collection and exploitation of personal data belonging to others. Secondly, with regard to the efforts of law enforcement agencies and their timeliness, it can be observed that these agencies may lack sufficient knowledge and expertise in the field of facial recognition technology and personal information protection. This may be due to a lack of relevant training and education. Consequently, it becomes challenging for law enforcement agencies to accurately identify and assess the risks in personal information protection when dealing with cases involving the technology. This ultimately results in inadequate efforts in law enforcement and the failure to prosecute certain violations of the law. Finally, it is possible that law enforcement agencies are not as active as they could be in promoting public awareness of personal information protection. The inadequate public education and awareness may result in a lack of sufficient public attention to the issue of personal information protection, thereby increasing the risk of leakage and misuse of personal data.

4.5. Ways to Protect Personal Information in the Context of Face Recognition Technology in China

4.5.1. Promoting the Standardization and Normalization of Administrative Law Enforcement

(1) Emphasizing Administrative Enforcement Responsibilities

In the application of face recognition technology, the relevant administrative departments have issued a series of norms to clarify the specific requirements pertaining to the application of the technology, the collection and processing of data, and the security measures. These norms require that the entities applying the technology adhere to laws and regulations to ensure legality, legitimacy, and security during the use of the technology. Concurrently, the norms underscore the responsibilities and obligations of the technology users, including the safeguarding of data security, the respect for individual privacy, and the addressing of violations. It is incumbent upon users of the technology to ensure that it functions properly while also taking effective measures to safeguard private personal information and prevent information leakage and misuse. For instance, administrative regulations prohibit the utilization of face recognition technology in certain locations as a means of safeguarding personal privacy information. Specifically, the installation and use of face recognition devices are proscribed in private residences, restrooms, and other locations where personal privacy is expected. For instance, a residential complex in Tianjin installed face recognition equipment at the entrance the purpose of access control. However, the installation did not obtain the consent of the owners and the necessary security measures were also absent, which resulted in a violation of personal privacy. This violation was met with condemnation from the public and subsequently rectified. At the same time, the procuratorate, in its capacity as a legal supervisory entity, is empowered to initiate public interest litigation in accordance with the law when it identifies deficiencies in the protection of personal information related to face recognition. In such instances, the procuratorate may urge relevant enterprises and governmental departments to enhance the security of personal data and foster a collaborative environment wherein the general public can engage in and oversee the addressing of these issues.

(2) Enhancement of Joint Law Enforcement Mechanism

The advancement of social and economic progress has led to the diversification of business fields and modes of operation, resulting in notable impacts on traditional sectors and fields. Presently, when enterprises typically engage in activities across multiple sectors and fields, it is not feasible for individual departments to achieve unified and comprehensive supervision on their own. It is therefore necessary to establish a mechanism featuring joint enforcement to address the issue of ineffective regulation, and to bridge the gap between government departments. The current structure of government departments, with their disparate responsibilities, procedures, and enforcement standards, makes it challenging to respond to problems in a timely and effective manner. However, a joint

enforcement mechanism, which integrates the resources of various departments, clarifies the division of labor, and harmonizes enforcement standards, would serve to resolve the problems of incomplete regulation, poor efficiency, and repeated enforcement. This approach can assist in enhancing the existing enforcement and governance practices, maximizing the integration of administrative resources, and effectively responding to privacy infringement issues through the application of face recognition technology.

(3) Giving Full Play to Government Initiative

The diversification of regulatory measures by government departments allows for a more rapid response to privacy breaches, facilitating the more timely and effective resolution of such issues [5]. In order to safeguard the right to privacy, several U.S. states have enacted separate laws to protect face recognition information. In May 2019, the city of San Francisco enacted the Stop Secret Surveillance Act, which is intended to preclude the city from employing facial recognition technology for the purpose of surveillance over the residents' activities. Subsequently, in August 2019, the state of Massachusetts within the United States implemented a ban on the utilization of facial recognition technology by both governmental entities and law enforcement agencies, and decreed that evidence acquired via this technology shall be inadmissible in legal proceedings [6]. China may benefit from adopting a similar approach, whereby local governments are granted the authority to identify and address the underlying causes of privacy breaches at an early stage.

4.5.2. Giving Play to the Deterrent Effect of Criminal Justice Sanctions

In terms of criminal law, penalties should be increased at the legislative level by making specific criminal offenses, because when entering the judging stage, the boundaries between this crime and that crime, felonies and misdemeanors are not very clear, in the determination of individual cases there is certain bias in understanding and confusion in application. It is insufficient to address the issue of facial recognition technology solely through amendments to criminal law. The distinctiveness and importance of face features necessitate a multifaceted approach to safeguard them [7]. In fact, it is more appropriate to do the protection of face information in advance by technical means, followed by the preventive legal regulations. Penalties, as an after-the-fact means of relief, are inadequate to restore the victim's loss. At the same time, the legal interests of citizens can be protected by strengthening the interface between criminal justice and administrative law enforcement in the process of prosecuting crimes against face information. Administrative law enforcers can use the existing information platform to share face recognition cases in their possession with judicial authorities in a timely manner to ensure that the progress of cases is tracked and monitored.

For each face-recognition-related case that enters the judicial process, judicial organs throughout the country shall make full use of the existing legal tools to punish the violators and safeguard the lawful rights and interests of citizens in accordance with the provisions of the Supreme Court on Several Issues Concerning the Application of Law to the Trial of Civil Cases Related to the Handling of Personal Information Using Face Recognition Technology. For infringements that have not yet entered the judicial process, it is expected from market supervision departments to industry authorities to take the initiative to investigate and address the issue proactively, in order to combat such infringements [8]. It is incumbent upon the People's Procuratorate to fulfill its legal supervisory obligations, to oversee the transfer of cases from administrative law enforcement authorities and the investigation of cases by public security organs, and to guarantee that cases are handled in accordance with the law. Besides, collaboration among pertinent governmental departments is essential to address the technical challenges and concerns managerial issues in industries associated with face-recognition-related crimes.

4.5.3. Strengthening Industry Self-Regulation

As companies profit from face recognition technology, it is expected of them to enhance their sense of social responsibility and implement necessary measures to safeguard the private information of the masses. The U.S. legislative framework allows for greater spaces for businesses to flourish, which is vital for economic and technological advancement. However, it also underscores the

necessity for industry self-regulation. It is therefore recommended that industry associations and chambers of commerce should establish detailed, specific, and operable industry norms and technical standards to clarify the operational processes and requirements for various aspects of face recognition. For instance, explicit consent shall be obtained when collecting face information, and, encryption shall be employed when storing relevant information, and, the scope of utilization of such information shall be strictly limited. In the financial industry, banks and financial institutions are obliged to implement double authentication when using facial recognition for the purpose of identity verification, and to implement rigorous access control with regard to clients' face data. In the Internet industry, the chamber of commerce may encourage e-commerce platforms and social media companies to adopt privacy protection technologies, such as encrypting face information during data transmission, to prevent information leakage. In the security industry, industry self-regulatory organizations may establish the maximum duration for which face recognition can be utilized in surveillance systems and maximum storage period allowed, beyond which data must be automatically deleted. In the domain of intelligent access control, it is imperative that enterprises proffer alternative authentication options when recommending face recognition, thereby upholding the right of users' right of choice. Moreover, it is also important to reinforce collaboration and communication across industries and enterprises to facilitate the exchange of successful experiences and best practices, thereby elevating the self-regulation in various industries.

4.5.4. Reinforcement of Social Supervision

The safeguarding of personal data has emerged as a pivotal concern in the context of the growing prevalence of face recognition technology. While the laws and regulations are subject to delays and shortcomings, the introduction of social supervision can serve to address these deficiencies and facilitate enhancements to the existing systems. As the primary constituent of society, citizens are entitled to oversee the implementation of pertinent legal measures and assess their effectiveness. It is recommended that the government or relevant organizations establish dedicated online and offline channels for receiving public complaints regarding improper conduct. Upon receipt of complaints and reports, government departments shall be obliged to promptly conduct investigations and provide feedback within a specified time frame. Furthermore, they shall be expected to impose severe penalties on the law violators according to the relevant laws, thus creating a deterrent effect.

For instance, organizations that collect and utilize facial data in contravention of legal requirements should be liable for substantial financial penalties and compelled to rectify the situation. The media, on the other hand, as a medium for the dissemination of information, bears the responsibility of spreading knowledge about the principles of face recognition technology, its applications, and potential risks of the leakage of personal information. Concurrently, as a public opinion supervisor, the media should lead the effort to oversee and expose the actions of enterprises and organizations that infringe upon personal information through the application of face recognition technology.

4.5.5. Strengthening Corporate Compliance

Given the sensitivity of face data, companies must adhere to not only the general regulations governing the processing of personal information but also the specific guidelines for the handling of sensitive personal data when employing face recognition technology. Prior to the collection of face information, enterprises are required to consider the Personal Information Protection Law, the Security Requirements for Facial Recognition Data, and other pertinent regulations in order to ascertain whether the use of face recognition is appropriate in specific scenarios, such as, at the entrance of a train station, or the entrance of a residential complex [9]. In instances where the collection of facial information is deemed appropriate or necessary, the user must be informed of the purpose of the collection, the intended use, and any potential risks in a clear, unambiguous, and readily comprehensible manner, and the express consent of the user must be obtained prior to the commencement of any such collection. Furthermore, the enterprises must adhere to the principle of data minimization in the processing and collection of face information, to prevent the over-collection

of data and potential infringements on personal privacy. To illustrate, an access control system should only collect the facial features for identity verification, without the retention of other superfluous information. In addition, enterprises are expected to engage the services of professional third-parties to audit their personal information protection compliance, identify potential risks, and make timely improvements. They are also expected to develop emergency response plans for personal information leakage and other security incidents, with clearly-defined response processes and a defined division of responsibilities. In the event of a data breach, prompt measures shall be taken to notify users, assess damages, and implement remedial measures. Corporate compliance is an indispensable part of personal information protection in the context of face recognition technology. By strengthening legal compliance in personal information protection, enterprises can reduce legal risks and protect the rights and interests of users, which in turn enhances the social image and reputation of themselves.

5. Conclusion

In light of the growing prevalence of face recognition technology, it has become indispensable in numerous contexts, giving rise to public apprehension regarding the leakage of personal data. The technology enables efficient identification of citizens and improves the efficiency in the domains of public safety, finance and transportation, contributing to the rapid development of society. However, as with all technologies, there are some negative aspects to facial recognition. Given its extensive application, a multitude of initially inconsequential personal data has acquired heightened significance, thereby posing a greater challenge to the safeguarding of personal information in China. Face information is frequently collected and processed as a highly sensitive category of personal data in the application of facial recognition technology. However, unregulated collection and use have led to a growing need of people to protect the face data. It is imperative that the protection of face information be incorporated into the framework for the safeguarding of personal data. Moreover, due consideration must be given to the distinctive characteristics of this form of information. The prevailing frameworks tend to focus on the general character of personal information, which may inadvertently result in the neglect of the uniqueness of face information and the consequent inadequacy of protection measures. It is therefore necessary to emphasize the standardized application of face recognition in order to ensure the adequate protection of the face data while simultaneously enabling the effective utilization of such data to fulfill the intrinsic value of personal information.

The face data captured by the face recognition systems is the unique mark for identifying each citizen and is therefore a highly distinctive feature. Consequently, in the event of the leakage of face information, the individual in question will be exposed to the entire society, which introduces a significant risk to security. It is therefore necessary to reinforce the standardized use of face recognition technology. In light of the current dearth of supervision pertaining to face recognition technology in China, it would be beneficial to examine the two disparate legal models that exist in the EU and the US, and to put forth a solution tailored to the country's specific circumstances. In order to strike a balance between the advancement of science and technology and the protection of citizens' privacy, it is necessary to enhance the legal framework for the protection of privacy and to clarify the responsibilities of the regulatory authorities. Concurrently, it is imperative to reinforce the safeguarding of privacy and mitigate or even eradicate the prospective hazards posed by face recognition technology in respect of the industry's self-regulatory framework.

References

- [1] www.nosec.org. NOSEC Security Information Platform, 'Biotech Firm Suprema Leaks Facial and Fingerprint Information on More Than 1 million People'. 2019. 8. 15.
- [2] huanqiu.com. Facial Recognition Company SenseNets Accused of Data Breach Containing Personal Information of 2.56 million People. February 15, 2019.
- [3] China City News, 'Safeguard Travelers' Privacy and Security! Many Places Require Hotels to Eliminate the Mandatory Face Scanning, 2024. 4. 29.

- [4] www.scjrb.com, Focus on March 15 | The Unauthorized Use of Ai for Collecting Face Information Has Cost a Fine of 300,000 Yuan for This Company Based in Chengdu. 2024. 3. 15.
- [5] Yu Yang, 2021, 'On the Regulatory Construction of Risks in the Application of Personal Biometric Information', *Administrative Law Review*, 2021, No. 6.
- [6] Hong Yanqing, 'Exploration into the legal governance of facial recognition technology has gained momentum', www.cnki.net, *Chinese Journal of Information Security*, 2019, No.8.
- [7] Ouyang Benqi, Wang Zhaoli, 2021, 'The Boundaries of Legality and the Limits of Criminal Law Application of Face Recognition', *People's Procuratorial Semimonthly*, 2021, No. 13, The Boundaries of the Application of Criminal Law to Acts Involving Face Recognition.
- [8] hubpd.com: "Silk Road Discourse" In Regulating Face Recognition, Justice and Administration Need to "Perfectly Match", 2021. 7. 29.
- [9] Chen Mengyuan, Exploring the "Way" of Facial Recognition Data Compliance: A Five-Step Guide to Getting There, toutiao.com, 2024. 6. 20.