The Positive Role of Face Recognition Technology and Risk Prevention and Control

Guangqiao Xing, Hongxia Wei, Miaomiao Li

(School of Marxism, Anhui University of Finance and Economics, China)

Abstract: Face recognition technology is one of the important technologies in intelligent social governance. It is now widely used in the fields of smart payment, identification and transportation. However, while face recognition technology brings convenience to people, there are also many risks, including technical risk, infringement risk and social risk. In this regard, the legal system for face information protection should be improved, administrative supervision measures should be perfected, and the industry's self-regulatory mechanism should be established. It is necessary to give full play to the advantages of face recognition technology, but also to prevent and control the risks it may bring, so as to achieve a balance between the development of science and technology and risk regulation, and to realize the goal of synergistic governance of the rule of law and intelligent society.

Keywords: face recognition technology; application risk; risk prevention and control

The research of face recognition system began in the 1960s, which is a technology to identify people by their facial feature information. With more and more applications of face recognition, it is widely used in security monitoring, criminal tracking, law enforcement supervision, shopping and payment, and so on, bringing great convenience to people's life. However, the hidden problems of face recognition technology are also becoming more and more significant. While bringing significant social benefits, this technology may violate citizens' privacy, democratic freedom and human rights, and even their property. Based on this, it is necessary to study the ways of risk management of face recognition technology, establish the basic principles of face recognition technology utilization, and clarify the importance of face recognition technology regulation.

I. The positive role of face recognition technology

Face recognition technology is one of the most widely used technologies in the transformation of intelligent social management. The authentication and recognition functions of face recognition technology automate the collection of personal information in virtual space.

(i) Concepts and characteristics of face recognition technology

Face recognition technology is a biometric image capture computer technology that can be used for authentication or identification of persons to connect them explicitly to indexed data. Its application process generally includes the following steps: facial information acquisition, extraction of facial features and identification of individuals. Specifically, firstly, digital image acquisition needs to be accomplished by a face image detector. Second, the acquired image data are normalized, and specialized processing including fine transformation of spatial vectors to align eyes, detection of skin color, and background masking is usually performed. Third, the face features in the face image are extracted; ideally, the face feature information output from this step is unique when the face image undergoes changes in pose, illumination, facial expression, etc. Finally, the face recognizer matches the preprocessed face image with the image database and outputs the matching list, and the face recognition operation is completed. To summarize, face recognition technology can also be understood as feature extraction, classification and recognition of static or video face images by machine to achieve the purpose of identity identification.

Face recognition technology includes the following features. First, it has recognition automaticity. Face recognition technology can remotely recognize a natural person without physical contact, even without people's knowledge. Second, it has verification relevance. Face recognition technology can digitally convert the collected facial images, and directly carry out the comparison of data-based information in the subsequent use process, which means that as long as the face information that appears within the range of the collection equipment can be accurately associated with other information such as gender, age, nationality, ID number and other information of the person being collected.

(ii) Positive effects of face recognition technology

Face recognition technology has brought about social progress, with the advantages of convenience, non-compulsory and accuracy. In terms of convenience, the collection equipment is simple, and common cameras can be used to suspend the collection of face images, without the need for particularly complex specialized equipment, and the image collection can be completed within a few seconds. People do not need to show their cell phone QR codes, carry access cards campus cards and other relevant proof, just wait a few seconds to brush their faces. Non-mandatory on the recognized face image information can be actively acquired without being detected by the measured individual. Face recognition utilizes visible light to obtain face image information, unlike fingerprint recognition or iris recognition, which requires the use of electronic pressure sensors to capture fingerprints or infrared rays to capture iris images, which can be easily detected by the individual. In terms of accuracy, the recognition effect can be better achieved without interfering with people's normal behavior, without worrying about whether the identified person is willing to put their hands on the fingerprint capture device, whether their eyes can be aligned with the iris scanning device and so on. In places with high security requirements, face recognition technology requires the actual existence of the recognized object, so others can not be easily imitated. At the same time, face recognition technology can effectively distinguish the difference between real faces and pictures and sculptures, which is difficult to realize other recognition technology.

(iii) the type of application of face recognition technology

With the improvement of the intelligence level of artificial intelligence system, various intelligent systems have been widely used in people's lives, and face recognition system, as a member of artificial intelligence system, has been widely used. The face recognition system in different places has different management functions to meet the needs of different scenes. At present, face recognition technology is mainly used in four scenarios. The first is the field of identity recognition. As most of the neighborhoods and office buildings can not do closed management, thanks to the face recognition system can store the identity information registered by the owners of the community when they move in, the system will automatically determine whether the personnel in and out of the community for the internal personnel or unfamiliar personnel, to effectively safeguard the safety of personnel. Secondly, it is applied in the field of transportation and travel management. High-speed rail, airports, bus stations and other high traffic, face recognition gates can better assist the station management to strengthen the management of station passengers. It can also lock and flee suspects and lawbreakers through face recognition, improving station security and management efficiency. Third, the field of access control system. It can be applied to the access control of key areas such as government departments, banks and hospitals. At present, many colleges and universities are using smart campus face recognition gate system, which can effectively control the random entry and exit of outsiders and provide strong protection for campus security. Fourth, the field of electronic applications. For example, in the past, e-commerce transactions often use password payment, which may be used by lawbreakers once stolen. The use of human face, a biometric identification for credit card network payment, better protects the security of the transaction and ensures the unity of the digital information owner and the actual owner.

II. The risk analysis of face recognition technology

Technology is a double-edged sword, face recognition technology also has two sides. While bringing benefits to people, it also brings many potential risks. On the one hand, it includes the risks caused by the loopholes within the technology; on the other hand, it includes the social risks that may be triggered by the specific application process of this technology in the society.

(I) Technical risks implied by face recognition technology

The processing of face recognition data includes the collection, storage, use and deletion of face recognition data, which involves a number of links. Face recognition technology itself is in the development stage, and there are still imperfections in each link. There are numerous countermeasure technologies that utilize face photos or videos to bypass the recognition mechanism, which challenges the security of face recognition technology. Although faces have uniqueness, they may also have similarities. If the uniqueness of the face of the recognized subject is not high, then the face recognition technology may be problematic. A common example is twins with very similar facial features. After all, face recognition technology is still being perfected, and in such cases, there is a high likelihood of recognition errors. In addition, faces can be faked with age, beauty make-up retouching, technological synthesis, and environmental factors. Because of the fact that in portrait recognition, it still mainly relies on the collection of camera facilities, the imaging technology is not mature enough, and at the same time, some of the application software itself also has loopholes, which makes the face recognition technology also has the possibility of being cracked. In recent years, in China's fight against cybercrime, there have been a number of cases in which technical means have been used to bypass face recognition to commit crimes. For example, Shanghai handled the "Yang Dalei, Wu 2 infringement of citizens' personal information case", the defendant Yang Dalei in order to bypass the authentication of the face recognition system, through the technical means of photos made into a 3D face video, breaking through the face of real-name authentication links. Zhejiang Wenling for the "Yang Chao, Sun Fangzhu, Wan Xingjian destruction of computer information systems case", the defendant Yang Chao use of other people's identity information, high-definition portrait, Alipay account number, etc., to create a human face verification of dynamic images, fraudulent use of other people's identities for Alipay account information modification or real-name authentication.

In addition, the use of face recognition technology has brought about many derivative ethical risks. Face-swapping video is one of them. Based on the depth of forgery technology, the video will be intelligent technology processing, so as to realize the video characters for face-swapping, the use of Yang Mi and other public figures to produce face-swapping video is one of the typical. Nowadays, the images of many public figures are used in face-swapping videos to increase attention in exchange for benefits, especially in certain pornographic website videos. These videos have been widely disseminated and have aroused public concern in the field of ethics and morality. The general public is unable to recognize the authenticity of these videos, which has caused great damage to the reputation of the person concerned. It can be seen that the development of face technology is now not only limited to identifying identity, but in the process of utilization, the leakage of face information has led to the risk of face swapping, which has triggered a series of discussions on the ethicality of face recognition technology.

(ii) Infringement risks arising from face recognition technology

Individual biometric features can be categorized into three types: personal privacy information, general personal information and personal data. In the intelligent society, the face information in the use of face recognition technology contains a variety of legal interests, including both personality right legal interests and property legal interests. Therefore, it may involve various aspects of personal property, privacy, security and even reputation.

First of all, it may violate personal privacy. Nowadays, face information is widely used, and public places are full of all kinds of monitoring equipment. From the perspective of criminal offense, this technology has brought convenience to the maintenance of social security, and has also made criminals invisible, protecting people's property and life safety. But at the same time, if the facial recognition technology collects facial information improperly, it is very likely to produce a huge threat to the privacy of citizens. According to the Civil Code of the People's Republic of China, privacy is the private space, private activities and private information that a natural person does not want others to know. In fact, as far as the human face is concerned, it is a symbol of people's identity characteristics and has a public nature, which does not seem to belong to the category of privacy. But faces belong to a kind of information privacy. When a particular face is combined with the time and space of its appearance, privacy may also be formed. On the one hand, the face image itself serves as a kind of identity information that can be used for identification. On the other hand, through data algorithms and other technologies, information such as age, race, health status, sexual orientation, and emotional changes of others can be extracted from facial information. In addition, the recognition process of face recognition technology is characterized by autonomy, non-contact, and no need for cooperation or consent from others, which makes facial information always on the verge of danger, and makes it difficult to ensure that the collectors will not misuse facial images out of self-interest. For example, the failure of Deep Web Vision Technology Co., Ltd. to password-protect the database of face information in its possession triggered a large-scale data leakage incident, which seriously infringed on the privacy and security of users.

Second, it may damage personal property rights and interests. The value of information in the data era has reached an unprecedented level. The electronic face information processed by algorithms under face recognition technology is a biometric information, which also has property attributes. Nowadays, many companies and financial institutions apply face recognition technology in their daily work to deal with business, but after obtaining the user's facial information, due to the complexity of the actual operation, technicians cannot ensure that the face information is in a safe and undisclosed state for a long period of time, and once intercepted by lawless elements, other people's property may be stolen. Especially in the context of face payment and face authentication, the theft and misappropriation of face information will directly result in property loss, and the improper use of AI face-swapping technology will also incubate fraud and coercion-type property crimes. At the same time, face information is often tied to information such as name, identity photo, bank card account number and cell phone number, which is required for registering a company, applying for credit and other behaviors. For the subject of information, once the leakage of such information, not only will the subject of information will cause personal injury, but also may cause serious property security risks, so that the subject of information loss is huge.

(iii) Social governance risks arising from face-recognition technology

Face recognition technology breeds a series of social crime risks, easily destabilizing society and affecting social governance. Once the face recognition database is attacked by the network, the face feature data and the personal information of the citizens bound to it will be illegally traded as electronic data, leading to the disruption of social order. At the same time, face recognition technology may pose a threat to citizens' freedom, creating a kind of social community panic and bringing about a social crisis of trust. The over-application of facial recognition technology is step by step putting citizens' daily lives under a kind of "panoramic prison".In November 2018, seven members of the House of Representatives of the Democratic Party of the U.S. questioned the accuracy of facial recognition technology and suggested that citizens may no longer be willing to actively participate in public marches, demonstrations, and protests in public places due to their fear of facial recognition technology. events such as marches and demonstrations held in public, or even no longer have the courage to speak out in public. In the context of face recognition technology, the risk of freedom comes from two main sources: the freedom to use face recognition technology or not and whether citizens can still enjoy freedom after using face recognition technology? The answer is yes. However, the non-contact, unconscious nature of the technology is forcing us to use it passively, violating the right to free choice. Since face recognition technology collects data very quickly, if left unchecked, it will pose a social governance problem if left to market manipulation. Since face information is unique and non-confidential, it is impossible for us to prevent the occurrence and expansion of damaging results by changing passwords and freezing accounts, as we do with ordinary personal information, not to mention hiding a person's face. If the portrait information is leaked in the future, do we have to wear masks when traveling or prevent the risk through cosmetic surgery?

At the same time, there may be discrimination in face recognition technology, which may also cause social class conflicts. It mainly refers to the fact that in the process of face recognition, the operator consciously adjusts the recognition rate of certain or certain types of people higher or lower, or consciously inputs specific recognition data, resulting in discrimination in recognition. For example, smart security systems in certain countries focus on low-income blacks with higher recognition rates. At the domestic level, some companies use face recognition to analyze the shopping habits of users and recommend different products or services accordingly, giving another set of price standards with obvious differences.

III. Face recognition technology risk prevention and control

Face recognition technology risk does not belong to a single risk, but a variety of combinations of complex risks, from its risk causes and extraterritorial experience. From the point of view of its risk causes and extraterritorial experience, the regulation of face recognition technology risk can not rely only on a single means. In this regard, the application of face recognition technology should be reasonably regulated from multiple perspectives to realize effective prevention and control of its potential risks.

(I) Improve the legal system of face information protection

Some data show that the face recognition market scale will reach 4.28 billion in 2020, and the application of face recognition in the economic field has become a trend. Therefore, face recognition technology should not be treated in a one-size-fits-all manner, and a rational application should be advocated. Given that face information is an important area of personal information protection, the Personal Information Protection Act should be used as a basis for establishing relevant basic principles, clarifying the obligations of information controllers, and providing universally feasible legal guidelines in the future.

First, the legal principles for the application of face recognition technology should be clarified, specifically including the principle of informed consent, the principle of accuracy and transparency, and the principle of narrow proportionality. The principle of informed consent aims to safeguard individual autonomy and reflects respect for the self-determination of citizens' personal information. The informed consent of users not only reflects respect for the free will of citizens, but is also an important means of risk prevention and risk minimization. The principle of informed consent not only requires companies to inform the process and risks of using face recognition technology, but also to obtain written, explicit consent from users. Users have the right to choose, no matter which subject operates face recognition, people have the right to refuse to "swipe". The principle of accuracy and transparency includes not only transparency but also accuracy. In the era of big data, the need for frequent processing and multiple utilization of information requires companies to establish continuous information disclosure to ensure the accuracy of data as much as possible. The principle of narrow proportionality expresses a concept and idea of moderation and balance, which emphasizes the appropriateness of means and ends. The whole process of the use of face recognition technology must be in line with the purpose of the law and the interests of users, and for illegal behavior, its regulatory measures and means should be appropriate and reasonable, and when it is really impossible to avoid the occurrence of harmful results, it should be adopted in a way that minimizes the damage. It is necessary to prevent risks and obtain benefits at the same time.

Second, clarify the obligations of users of face recognition technology. The exchange of information between the information subject and the enterprise is not reciprocal. Once the subject in question agrees to the collection of information, the subsequent processing of the information is completely handed over to the enterprise, and the information subject is unable to participate in subsequent sessions. Moreover, as long as the information subject has signed the informed consent form, most of the risks he or she may face thereafter will be borne by him or her. This is very unfair to the information subject. In the process of using face information, the one who really benefits is actually the user of the information technology. If only the information subject bears the consequences, he or she neither gains benefits from it, and his or her privacy and property rights are also violated, which undoubtedly aggravates the pressure on the information subject and reduces the responsibility of the enterprise concerned.

Third, differentiate the focus of legal protection under different application scenarios. Face recognition technology involving public interests should focus on prior regulation, restricting the use of face recognition technology by relevant public authorities. Face recognition technology involving only private interests should focus on after-the-fact accountability, protecting the legitimate rights and interests of the information subject and pursuing the responsibility of the enterprise organization.

(ii) Improvement of administrative supervision measures

The lack of regulatory body is one of the reasons for the ineffective protection of personal information in China. As far as the administrative supervision of the existing risks of face recognition technology in China is concerned, the lack of clear legal authorization for the supervision work, coupled with the unclear division of responsibilities of the relevant departments for the supervision of face information, has led to a chaotic situation in which the supervision of face information in our country is in a multi-headed supervision at present. Therefore, the establishment of a specialized regulatory body can realize the integrated management and ensure the safe nature of the collection and use of personal information.

In terms of administrative legal protection, although data protection agencies such as "Net Information Office" and "National Information Center" have been established, and some places have set up "Big Data Bureau", these agencies do not belong to the nature of administrative supervision. However, these organizations are not administrative supervisory bodies in nature and do not have the legal function of supervising the collection of personal information. Since the technical characteristics of face recognition may bring many unknown risks, the regulatory mechanism should be flexible, dynamic and progressive. The following two points can be used as concrete implementation methods for the regulatory mechanism: First, while strengthening the regulation of information security, promote communication between the government and enterprises, strengthen information security guidance, and provide external legal compliance guidelines for enterprises. Improve the internal regulatory mechanism of enterprises to ensure that they are in a reasonable and uninterrupted dynamic development process. Secondly, strengthen administrative supervision while focusing on the linkage with legislation, with laws and regulations as the value guide for the use of technology, supplemented by external supervision. In addition, the regulatory body can set up an open and transparent complaint mechanism. As direct victims of personal information infringement, citizens have limited influence, making it difficult to prove their case and realize their legitimate demands. With the establishment of a complaint mechanism, private citizens who discover that others are collecting personal information in violation of the law can report the situation to the regulator and seek protection from public power. Upon receipt of a tip, the regulator must immediately conduct an investigation and should take measures to minimize citizens' losses. In particular, when the leakage of personal information causes irreparable damage to citizens, the regulatory body may use technical means to find the source of the leakage and intercept it in a timely manner, and evidence of the infringement collected in the process may be used as the basis for penalties, and may also be provided to citizens who are actively defending their rights to help them seek judicial remedies.

(iii) Establishment of a self-regulatory mechanism for the industry

Facial recognition technology is developing rapidly, the law has a lag, and the governance of facial recognition technology can not rely entirely on the government. For industry operators, based on common interests, it is easier to accept and recognize the rules established by their own industry, so it is easier to play its role in the specific implementation process. Specifically include two aspects, one is to strengthen the construction of industry self-regulatory organizations, the second is to establish industry self-regulatory norms.

Protection of facial information requires enterprises to consciously implement the relevant laws, the law into the enterprise system and action, which is the role of industry self-regulation. However, China's industry self-regulatory organizations have not yet matured. Therefore, in the construction of industry self-regulatory organizations, it is not only necessary to rely on the strength of enterprises themselves, but also need the appropriate intervention of the government. On the issue of construction of industry self-regulatory organizations, the government can provide priority credit through financial support to enterprises that join industry self-regulatory organizations and comply with industry self-regulatory conventions, as a way to motivate enterprises to actively join industry associations and comply with industry norms. For the industry self-regulatory organizations exist in the formulation of the norms of the problem of insufficient capacity, you can establish the government and industry associations legislative talent exchange mechanism to achieve the sharing of talent. For industry self-regulatory organizations to develop, practicable industry standards, industry self-regulatory conventions, can be incorporated into laws and regulations in due course, to give it the power of enforcement. In addition, industry self-regulatory norms should be established, which is the most effective measure to regulate the collection of personal information in the industry. Self-regulatory norms have a broader scope of constraints, and the entire industry can be required to jointly comply with such norms, and uniform standards should be formulated within the industry to constrain all organizations, and to provide a bottom line for the obligations of different enterprises to collect personal information by using face recognition technology.

Adjustment and design of products involving infringement of the right to personal information by the industry through self-regulation norms, establishment of a multi-level security mechanism integrating ex-ante prevention and ex-post regulation, and shifting from unilaterally emphasizing the information subject's independent control of personal information to industry self-regulation and supervision through the industry's collective assumption of the corresponding legal and social responsibilities, have the advantages of timeliness and high efficiency.

IV. Conclusion

As an emerging information recognition technology, face recognition technology will have a broader development space in various fields of society. However, technology is a "double-edged sword" with two sides, which can bring us high convenience and high income, but also bring many potential risks. Therefore, we should attach great importance to the problems arising from the application of face recognition technology, improve the legal system, improve administrative and regulatory measures, and establish the relevant industry self-regulatory mechanism, so as to ensure that "science and technology for the good", and to achieve a balance between scientific and technological progress and risk prevention and control.

References:

[1] Xu Jingze ,Wu Zuohong ,Xu Yan et al. Fusion of PCA, LDA and SVM algorithms for face recognition[J]. Computer Engineering and Applications,2019,55(18):34-37.

[2] Yuan Jun. On the application risk and legal regulation path of face recognition technology[J]. Information Security Research,2020,6(12):1118-1126.

[3] Wang Lusheng. On the integration regulation of "deep forgery" intelligent technology[J]. Oriental Law,2019(6):58-68.

[4] Zhang Yong. Legal Protection of Personal Biological Information Security--Taking Face Recognition as an Example[J]. Jiangxi Social Science,2021,41(5):157-256.

[5] Guo Chunzhen. Governance of face recognition technology application in the era of digital human rights[J]. Modern Law,2020(4):24.

[6] Xing Hui-Qiang. Legal regulation of face recognition[J]. Comparative Law Research,2020(05):62.

[7] Zhu Lingfeng. Data Compliance 2020 Outlook[J]. Internet Economy,2020(1):64-69.

[8] Tian Ye. The Dilemma and Way Out of the Principle of Informed Consent in the Era of Big Data---Taking the Protection of Personal Information in Biobanks as an Example[J]. Law and Social Development,2018(6):111.

[9] Zheng Xiaojian. The status of the principle of proportion in the modern civil law system[J]. Legal Science,2017(6):101.

[10] Zhang Jihong. Dilemma and way out of industry self-regulation of personal information protection in the era of big data[J]Finance and Economics Law,2018(6):57-70.