Proceedings of ICILLP 2025 Symposium: Property Law and Blockchain Applications in International Law and Legal Policy
DOI: 10.54254/2753-7048/2025.LD29245

Criminal Regulation of the Abuse of Facial Recognition Technology

Die Wu

School of Foreign Languages, Jishou University, Zhangjiajie, China
2022404180@stu.jsu.edu.cn

Abstract. Facial recognition technology has been widely used in many different industries due to the rapid advancement of technology, including identity verification, electronic payment, and security assurance. Abusive practices of using facial recognition technology are diversified. Some abusive uses of facial recognition technology may meet the constitutive elements of multiple crimes, which creates difficulties in identification. Focusing on the crime of infringing upon citizens' information, this article first defines what constitutes the crime and then distinguishes this crime from other crimes. If the two crimes are concurrent under the law, they are usually dealt with the special law or the more severe crime; if they are imagined concurrent crimes, the more serious crime is chosen for handling; if they are complicit crimes, they are usually handled according to the purpose crime; if none of the above relationships are met, the crimes should be separately convicted. Besides, the amount of facial information and the threshold for criminalization are too high. Facial information should be listed as the first-level personal information for protection. More than fifty items obtained, sold, or provided illegally should be considered "serious circumstances" and be considered a violation of personal information.

Keywords: facial recognition, crime of infringing on citizens' personal information, criminal regulation

1. Introduction

A biometric program called Facial Recognition Technology (FRT) is used to identify people [1]. With the rapid development of science and technology, facial recognition technology is widely used in authentication, electronic payment, safety guarantee and so on. Facial recognition has permeated every aspect of life, from the login verification of mobile apps to the facial payment of wechat and Alipay, and from the facial verification of community security systems to the facial comparison of criminals in public places. The technology not only provides tremendous convenience for people’s lives, but is conducive to combating illegal and criminal activities. Meanwhile, the popularity of facial recognition triggers a series of issues related to personal information protection, causing hidden trouble for personal and property security. For instance, there is a risk that personal facial information may be leaked and misused. Besides, criminals may illegally obtain facial information to forge faces and then transfer property to carry out fraud and other criminal activities through electronic payment.

© 2025 The Authors. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

DOI: 10.54254/2753-7048/2025.LD29245

For the aforementioned risks, regulations should be implemented in advance. Recently, China has taken the following measures. The "Regulations on Public Security Video-Image Information System" issued by the State Council in 2025 emphasizes the need to protect both public security and individual privacy and information rights while doing so. In the same year, the Cyberspace Administration of China and the Ministry of Public Security issued the "Regulations on the Application Security Management of Facial Recognition Technology", emphasizing the "non-mandatory" principle. The current criminal law also includes charges such as infringement of citizens' personal information and damaging computer systems to regulate the abuse of facial recognition technology.

The development of Artificial Intelligence diversifies the abusive practices of using facial recognition technology, such as creating fake dynamic facial images, providing "deepfake" software or technologies, etc [2]. Such new behaviors usually involve the infringement of multiple legal interests, the controversy over conviction and sentencing, as well as the severity of risk consequences. This article aims to focus on the crime of infringing upon citizens' personal information, exploring how new behaviors can be identified as this crime and the difficulties in the rules.

2. Analysis of the legal definition and usage boundaries of facial recognition technology behaviors

2.1. The legal nature determination of facial information

According to Article 1034 of the People's Republic of China's Civil Code, facial information is a form of biometric information and is legally protected as personal information. Additionally, the "Personal Information Protection Law of the People's Republic of China" specifically protects and classifies facial information as personal information. With regard to the processing of facial information, the "Provisions of the Supreme People's Court on Several Issues Concerning the Application of Law in Civil Cases Involving the Processing of Personal Information through Facial Recognition Technology" have outlined the guidelines for identifying infringement in common situations [3]. The "Interpretation on Several Issues Concerning the Application of Law in Handling Criminal Cases Involving the Infringement of Citizens' Personal Information" (Hereinafter referred to as "Interpretation") issued by the Supreme People's Court and the Supreme People's Procuratorate does not explicitly list biometric information, genetic information, and other personal special sensitive types of information. However, it can be known from the 192nd guiding case issued by the Supreme People's Court of China on December 28, 2022, that the criminal law regards facial information as the second-level personal information for protection. In conclusion, facial information is a type of personal information that is clearly protected by law. Illegally obtaining, using or transmitting facial information may lead to infringement and even constitute a crime.

2.2. The distinction between the rational use and abuse of facial recognition technology

According to relevant regulations such as the "Administrative Measures for the Application Security of Facial Recognition Technology", the rational use and abuse of facial recognition technology can be distinguished from the following aspects: Whether it follows the principles of legality, legitimacy and necessity; whether it complies with the principle of minimizing processing; whether it obtains individual consent; whether it is used as the sole verification method; whether it is installed in a compliant location. The following behavior is considered reasonable use. For example, the

DOI: 10.54254/2753-7048/2025.LD29245

information processing is legal, proper and necessary; the information processor only collects the minimum amount of necessary facial information; the information processor obtains the individual's voluntary and explicit consent made under full knowledge; facial recognition is not the only verification method and installing equipment in compliant places. Otherwise, it is considered abuse. Therefore, the rational use should comply with the principles of legality, propriety and necessity. It should follow the requirements of minimizing processing, obtain individual consent, non-uniquely verify methods, and be conducted in compliant locations. Any violation of these principles constitutes abuse.

2.3. The criminal risks of abusing facial recognition technology

Overuse of facial recognition technology may give rise to crimes including theft, fraud, violation of citizens' personal information, and unlawful control of computer information system tools and programs. A crime against a citizen's personal information may be committed if someone is utilizing face recognition technology improperly to gather or sell personal information under dubious circumstances. A person may be charged with the crime of computer system destruction if he/she abuses face recognition technology to erase, alter, expand, or interfere with the operation of a computer system, making it impossible for it to function normally. If the actor abuses the face recognition technology and induces the victim to act on the property, it may be a crime of fraud. It is extremely possible to make a theft of human face recognition technology and steal other people's accounts and transfer them. The abuse of face technology is more varied and the scale of the crime is increasingly widespread, forming a serious criminal risk that needs to be regulated as soon as possible.

2.4. The criminal risks of abusing facial recognition technology

2.4.1. Crime against citizen's personal information

The abuse of face recognition technology is likely to illegally obtain, provide or sell face information or other personal information, which can constitute a crime of personal information infringement against citizens. The actor may falsify the dynamic image of the face to obtain the personal information of the citizen, to illegally obtain and sell other people's information by using virtual faces to solve the real name of a software, or to provide other people with the ability to solve the face recognition system service, or to provide others with the ability to crack face recognition systems, illegally acquire and sell other people's information. All of these actions can constitute a crime of personal information infringement on citizens.

2.4.2. Crime against data system infringement

After illegally falsifying face information, cracking the face recognition system and obtaining the data in the system, it can constitute the crime of illegal access to computer information system data and illegal control of computer information systems. If the face information was forged and entered successfully into the face recognition system, the person deletes, modifies, increases, and interferes with the system function, which may constitute the crime of destruction of computer system. These actions require the actor to crack the system. If the actor does not crack the system, he/she provides others software and procedures, so that others can invade and illegally control the computer information system, which may constitute the crime of intrusion and illegal control of computer information systems and tools.

DOI: 10.54254/2753-7048/2025.LD29245

3. Difficulties in criminal rules of abusing facial recognition technology

3.1. The identification of the crime of citizen personal information

If the actor violates the citizen's personal information first, then other illegal crimes are carried out, the behavior should be divided into before and after. The act of violating the individual information of the citizen is deemed to be a crime of infringing on citizens' personal information, and the subsequent actions are determined by the composition of other charges. If it is simply to be punished in other cases, it may be difficult to protect the facial information [4]. For example, Zhang and others used illegal access to personal information to make 3d heads, and then got the money from the Alipay bonus. The act of obtaining personal information to make 3d heads constitutes a violation of citizens' personal information, and the behavior of swindling the Alipay red envelope is a crime of fraud. The court believes that these are two separate crimes that do not have a relationship and should be punished individually [5].

However, in Guo's theft, her behavior was identified as a crime of theft [6]. The defendant Guo, who ran the China Mobile business hall in the town, logged on to other victims' Alipay accounts on her phone and set up the payment password by facial recognition during the business period. Without the agreement of any of the victims, Guo logged into the Alipay accounts of each victim multiple times and stole the money from the Alipay-bound bank cards of each victim. In this case, does this behavior, which involves logging on to other victims' Alipay to her phone by facial recognition, fall under the category of illegally obtaining citizens' personal information? Is the information in Alipay considered personal information of citizens?

Most of the previous cases involved illegally obtaining citizens' personal information first, creating virtual faces with the personal information, and then using it for real-name authentication. After the real-name authentication was unblocked, they entered the app to obtain the personal information. Undoubtedly, the aforementioned actions constitute the crime of infringing upon citizens' personal information. However, if there is no step of "first illegally obtaining citizens' personal information and making it into virtual faces", but instead directly using others' real faces illegally for real-name authentication, entering the app to obtain others' personal information, it will be a difficult point in identification.

3.2. The distinction between the crime of infringing upon citizens' personal information and other crimes is ambiguous

The determination of the crime of infringing upon citizens' personal information and other crimes should start from their respective constituent elements, which is relatively simple. The intricacy stems from the possibility that a criminal conduct may satisfy the requirements for several other crimes, which has resulted in disagreements concerning the classification of the crime of violating citizens' personal information among other crimes. It's possible that the offender uses the strategy of unlawfully taking control of the computer information system in order to obtain personal data and make money. Or maybe the criminal obtains residents' personal information unlawfully and then exploits it to get past the facial recognition verification system. Recent offenses involving data systems, such as unlawfully accessing data from computer information systems and unlawfully manipulating computer information systems, are linked to the crime of violating citizens' personal information. There is a certain degree of confusion in judicial practice regarding the application of relevant charges and the number of crimes [7].

DOI: 10.54254/2753-7048/2025.LD29245

3.3. The amount of facial information and the threshold for criminalization are too high

Facial information is considered the second-level personal information for protection, as stated in the guiding case No. 192, which was published by the Supreme People's Court of the People's Republic of China on December 28, 2022. In other words, "serious circumstances" are defined as the unlawful acquisition, sale, or provision of more than 500 pieces of personal information about citizens, such as information about their accommodations, communication records, health and physiological information, transaction information, etc. Facial information has special sensitivity, which is a core feature that transcends general second-level information. Facial features are lifelong, unchanging biological identifiers of an individual. Once leaked, they will be permanently exposed. Unlike property information, transaction records and other modifiable information, facial information cannot be modified or reset to eliminate the risk of leakage [8]. The leakage of facial information is highly likely to be associated with downstream charges, such as computer-related crimes, causing even greater social harm. Therefore, the leakage of 500 pieces of facial information constitutes a serious circumstance and the threshold is too high. Moreover, the Civil Code, Administrative Law and other prior laws distinguish facial information from other personal information and provide special protection. The Criminal Law should also offer special protection for it.

4. The proper path of criminal rules for the abuse of facial recognition technology

4.1. Clarify the determination of the crime of infringing upon citizens' personal information

Use virtual faces to unblock the real-name authentication of government affairs apps. After unblocking the real-name authentication, you can enter the app and obtain personal information. It meets the criteria for stealing or illegally obtaining citizens' personal information by other means, and constitutes the crime of infringing upon citizens' personal information. Similarly, during the operation period, illegally obtaining citizens' real facial information and then entering the app to obtain personal information, after unblocking real-name authentication, also falls under the category of stealing or illegally obtaining citizens' personal information by other means.

In the aforementioned case of Guo's theft, some people may think that Guo did not explicitly demonstrate the illegal acquisition of citizens' information or the storage of facial information. Instead, she directly took advantage of her position to access the Alipay app through the real facial recognition of the victim. It does not seem to conform to the act of selling, providing or obtaining citizens' personal information to others. Article 4 of the Interpretation, however, states that "illegally obtaining citizens' personal information by other means" includes gathering citizens' personal information while carrying out obligations or rendering services, as well as obtaining citizens' personal information through purchase, acceptance, exchange, or other means that violate applicable state regulations. This means that as long as citizens' personal information is obtained through the above-mentioned illegal means, regardless of whether it is stored or not, it constitutes illegal acquisition of citizens' personal information. In this case, although Guo did not directly store facial information, she collected citizens' personal information in the course of performing her duties and providing services, which complied with the above regulations. Article 1 of the Interpretation specifies "citizens' personal information" as any type of data that is recorded in electronic or other formats and that, either by itself or in conjunction with other data, can be used to identify a particular natural person or to reflect their activities. Alipay account information includes the user's name, ID number, mobile phone number, account password, etc. These pieces of information can be

DOI: 10.54254/2753-7048/2025.LD29245

identified the identity of a specific natural person and thus belong to the category of citizens' personal information. Guo stored the Alipay information of all victims. Moreover, when entering Alipay, she would also obtain citizens' personal information, such as bank card numbers and ID numbers. Therefore, she was found to have illegally obtained citizens' personal information. This case should have been identified as the crime of infringing upon citizens' personal information, but it was not. When making a determination, it is necessary to combine judicial interpretations and relevant legal provisions to grasp the essence of the criminal act.

4.2. Clarify the distinction between the crime of infringing upon citizens' personal information and other crimes

4.2.1. Distinguish concurrence of law, ideal concurrence of offence and implicated offence

When an act simultaneously meets the constituent elements of different legal provisions or both ordinary and special provisions within the same law, it constitutes a concurrence of law. If an act simultaneously meets the constitutive elements of two or more charges but there is no overlapping or inclusive relationship in the legal provisions, it is considered an ideal concurrence of offence and should be convicted and sentenced in accordance with the principle of "choosing the more serious crime for punishment". If two or more separate criminal acts are committed based on a single criminal purpose and these acts are interrelated with each other, it constitutes an implicated offence. Determine whether the crime of infringing upon citizens' personal information has the above-mentioned relationship with other crimes, thereby clarifying the differences between them. For instance, if someone steals, buys, or unlawfully gives away someone else's credit card information, they are committing both the crime of stealing, buying, or illegally giving away credit card information and the crime of violating someone else's right to privacy. There is legal congruence between these two offenses. Both the crime of unlawfully obtaining data from a computer information system and the crime of violating citizens' personal information are met by the act of hacking into a computer information system in order to obtain citizens' personal information. These two crimes are an ideal concurrence of offence. For the purpose of illegally obtaining and selling others' information, after using the technical skills of technicians to provide services for cracking others' facial recognition systems, the information of others is illegally obtained and sold. It entails both the criminal of violating citizens' personal information and the felony of unlawfully accessing data from computer information systems. This offense is implicated.

4.2.2. Consider the essential characteristics of criminal acts

Analyze the essential characteristics of the criminal act, such as its main purpose, means and the main legal interests infringed upon. If the main purpose of a criminal is to obtain and sell citizens' personal information, although the means involve illegally controlling computer information systems, the crime of infringing upon citizens' personal information better reflects the essential characteristics of their behavior. In such cases, the crime of infringing upon citizens' personal information can be given priority for conviction, and then penalties can be determined at the discretion of the authorities based on the circumstances.

4.2.3. Take the circumstances of the case into comprehensive consideration

The circumstances of a case include the quantity, types, acquisition methods, harmful consequences, and illegal gains of citizens' personal information infringed upon. The specific circumstances of the

DOI: 10.54254/2753-7048/2025.LD29245

case should be comprehensively considered before conviction and punishment. Additionally, the criteria used to determine "serious circumstances" and "particularly serious circumstances" differ, even though the range of conviction and sentencing for the crimes of illegally obtaining data from computer information systems and violating citizens' personal information are the same. The former may have a lower standard for the quantity of information, such as account passwords, that can be criminalized. In some cases, if the quantity of obtained information and other circumstances can constitute "particularly serious circumstances" in the previous crime but only "serious circumstances" in the subsequent crime. They can also be considered as factors for conviction.

4.3. Reduce the amount of facial information and the threshold for criminalization based on circumstances

It is precisely because the human face remains relatively unchanged throughout one's life that facial features have a unique recognition ability on a global scale. This uniqueness makes it one of the most accurate methods of identity verification and also the most ideal target for criminals to attack. Criminals are highly likely to use AI technology to synthesize and forge facial information, creating highly realistic dynamic videos or images, thereby achieving their illegal goals. For example, some criminals illegally obtain facial information and forge dynamic facial videos to conduct illegal real-name authentication and unblocking, making profits from it. Moreover, the damage caused by lawbreakers is irreversible because once facial features are leaked, they are basically impossible to recover [9]. Facial recognition is distinct from second-level housing information, communication records, health and physiological information, and transaction data, as indicated by all of the aforementioned features. Facial information has social harmfulness comparable to that of the first level. Therefore, along with information about travel patterns, communication content, credit, and property, facial information should be disclosed. More than fifty items obtained, sold, or provided illegally should be considered "serious circumstances" and be considered a violation of personal information [10]. Some scholars hold the same view.

5. Conclusion

In the era of information technology, the abuse of facial information poses a huge threat to personal information and property rights as well as social order. This article conducts research on its criminal law regulation, discussing the definition of the legal attributes of facial information and the difficulties in determining the related criminal charges involved in facial recognition. In the existing criminal law determination model, crimes such as infringing upon citizens' personal information and computer-related charges can be applied, but in the face of the new forms of technology abuse, it still appears ambiguous. From the disputes over behavioral types, it can be found that there are difficulties, such as the compatibility of emerging technologies with traditional criminal charges and the high threshold for criminalizing the infringement of citizens' personal information. These issues can be addressed by clarifying the principles of conviction and punishment, and adjusting the threshold for their determination standards. In conclusion, the criminal law governance of the abuse of facial recognition technology is an important proposition for the construction of order in the digital age.

References

[1] Robles, P., Mallinson, D.J., Best, E. et al. (2025) Global Perspectives on Regulating Facial Recognition Technology Utilization for Criminal Justice Arrests. Glob. Public Policy Gov. 5, 186–204.

DOI: 10.54254/2753-7048/2025.LD29245

[2] Guo, Z. (2025) Criminalisation of the Illegal Use of Personal Data: Comparative Approaches and the Chinese choice. Humanities and Social Sciences Communications, 12(1): 1-16.
[3] The Supreme People's Court, Provisions of the Supreme People's Court on Several Issues Concerning the Application of Law in Civil Cases Involving the Processing of Personal Information through Facial Recognition Technology, July 28, 2021, Visit on August 25, 2025, https: //www.court.gov.cn/zixun-xiangqing-315831.html.
[4] Wen, Z. Q., Guo, S. M. (2023) Study on the Regulation of Face Recognition in Criminal Law. Academic Exploration, (04): 55-66.
[5] People's Court of Pengdu District, Chengdu City, The First-instance Criminal Judgment on the Crime of Infringing upon Citizens' Personal Information by Zhang Yu, Tang Jie and Li Ruia, October 28, 2019, Visit on September 23, 2025, https: //wenshu.court.gov.cn/
[6] Intermediate People's Court of Suihua City, Heilongjiang Province, Criminal Ruling of the Second Instance on Guo Moujing's Theft, June 4, 2025, Visit on September 23, 2025, https: //wenshu.court.gov.cn/
[7] Luo, X. (2023) On the Limits and Application of Criminal Regulation of Facial Recognition: From the Perspective of the Guiding Cases on the Crime of Infringing on Citizens' Personal Information. Comparative Law Studies, (02): 17-30.
[8] Wei, H. T. (2024) The Top-level Design of Criminal Law Regulation on the Abuse of Facial Recognition Technology. Contemporary Law, 38(02): 3-15.
[9] Wang, D. Z. (2021) The Criminal Protection about Biological Identification Information: Current Situation and Perfection Ways—Taking the Case of “Face Identification” in Sichuan as Starting Point. Journal of Chongqing University (Social Sciences Edition), 27(02): 133-143.
[10] Wang, Y. Y. (2023) Thoughts on Personal Information Protection in Facial Recognition. Application of Law, (02): 15-24.