Legal Risks and Governance of Face Recognition Applications in Public Health Emergencies

Jiao Guan[1] Wenjie Liu[2] Ruijie Wang[3] Honglin Zhu[4] Liuyang Jian[5] Yuqing Zhang[6]

[1,2,3,4,5,6] *College of Humanities, Hubei University of Chinese Medicine, Wuhan, Hubei, China*
[6] *Corresponding author. Email: zyq95@hbtcm.edu.cn*

ABSTRACT
The large-scale application of face recognition in the global public health emergency has caused people's concerns about privacy, surveillance, and discrimination. By defining face recognition information, sorting out the application scenarios of face recognition in public health emergency, and analyzing the legal risks brought by the application of this technology, governance paths are proposed from the following aspects, such as strengthening privacy protection, improving the legal regulation system of face recognition, actively formulating specialized standards for face recognition, and encouraging industrial self-regulation.

Keywords: *Public health emergency, Face recognition, Privacy, Personal information, Informed consent right.*

1. INTRODUCTION

Artificial intelligence, as a strategic technology and core driver of the new round of technological revolution, provides an important opportunity for intelligent response to public health emergencies [1]. Among them, face recognition technology is of great empowering utility in all aspects of the response cycle. However, "once technology enters the social fields, it is inevitably shaped and limited by the various interests, demands, and value judgments of social institutions, social organizations, and social groups" [2], and once face recognition information is misused, it will violate individual rights and interests, jeopardize social public safety, and put an end to community trust. The law should not only deal with the risks involved in the application of technology, but also respond to the threats caused by the improper use of technology to help and guarantee the realization of a "healthy society".

2. FACE RECOGNITION TECHNOLOGY AND INFORMATION

2.1 Concept of Face Recognition Technology

Face recognition is a biological feature recognition technology based on certain features of an individual face and digital information [3]. This technology extracts features and classifies and recognizes the face images in still or video by machine for the purpose of identity identification [4].

2.2 Definition of Face Recognition Information

Face recognition information refers to the machine information formed by the processing of face portrait through face feature recognition and matching algorithm [5], which belongs to biometric recognition information along with voice print, palm print, fingerprint, etc. The "Personal Information Protection Law" stipulates that biometric recognition information is sensitive personal information (Article 28). The so-called

"sensitive" means the risk to the information subject [6]. Biometric recognition information is highly sensitive. If it's leaked, it may lead to damage of personality, discrimination and violation of human dignity. Sensitive personal information is sensitive and private information, which is the core privacy of citizens [7].

3. APPLICATION SCENARIOS OF FACE RECOGNITION IN PUBLIC HEALTH EMERGENCIES

3.1 Community Management

In the community control management, residents enter and exit the community by "snapping their faces", which greatly avoids the risk of infection caused by unrelated people entering and leaving, and also reduces the pressure of community managers. In addition, face recognition technology collects the facial information of visitors on site, transmits it to the backstage, matches it with personal information, and registers it, enabling visitors to be quickly identified and confirmed, realizing automated management and facilitating the tracking of infected persons and close contacts during the outbreak of the COVID-19 pandemic.

3.2 Public Places Such As Train Stations, Airports, and Corporate Buildings

Major transportation hubs such as train stations, high-speed railway stations, and bus stations are the key places for epidemic prevention and control, and thermal imaging thermometers, such as "AI Epidemic Prevention Master" and "AI Temperature Measurement System", have become standard equipment. Some technology companies have also launched face recognition products with masks to avoid cross-infection. Many companies have also started to introduce "face recognition and body temperature testing machines", which have two major functions of face recognition access control attendance and automatic body temperature detection.

3.3 Emergency Management, Public Security and Other Departments

The combination of face recognition technology and video surveillance can achieve the following functions: identity verification, track playback, and key personnel deployment and control. It can be synchronized with the database of public security system to conduct synchronized search of all personnel and immediately alarm once key personnel are found. With this face recognition system, the public security and traffic police departments can identify the confirmed or suspected patients and quickly obtain and analyze the behavioral trajectories of the confirmed and suspected persons, so as to contain the transmission rate of the virus at the maximum speed and limit.

4. LEGAL RISKS OF FACE RECOGNITION APPLICATION IN PUBLIC HEALTH EMERGENCIES

4.1 Privacy Risk

4.1.1 Privacy "Control" Risk

The core of privacy in the information age is "control", that is, the right to decide when, how and to what extent to disclose private information. The dynamic interpersonal relationship of "human-machine intelligence interaction" in face recognition applications makes the law face a "broken-window challenge" and there is almost no place to hide personal privacy. According to the American Civil Liberties Union (ACLU), face recognition technology, which was originally intended to simply "collect and store information for emergency purposes, is increasingly being used to actively spy on people in real time" [8]. Currently, due to the needs of epidemic prevention and control and social governance, face recognition is widely used in many scenarios, and the senseless and contactless collection makes it impossible for information subjects to know when and where their personal information has been collected, and it is even more difficult to exercise control over face recognition information.

4.1.2 Risk of Illegal Disclosure of Privacy

The threshold line set by China for information collection is low. Relevant departments, government agencies and enterprises are able to collect users' personal information for the public interest or to provide commercial services, resulting in a risk of leakage of personal information. Most of the face recognition application scenarios are carried out for dynamic comparison of 1-to-N crowd, such as community access control applications, etc. The anonymity of people in public places and the need for peace of mind in private life cannot be fully guaranteed in dynamic matching [9]. Face recognition technology can easily collect all

personal information related to face information scattered all over the Internet. After analyzing the huge amount of personal information with commercial software or social software, it can obtain more personal private information such as identity information, life trajectory, health information, medical information, financial status and even emotional status, and even draw a complete personality portrait [10]. It is conceivable that once the face recognition information is illegally leaked, it will cause serious damage to the privacy and even property rights of individuals.

4.2 Risk of Informed Consent

4.2.1 Lack of Duty to Inform

Consent is based on knowing the facts of a case or the details of an incident, and the law imposes a special duty to inform on those who collect information. The "Personal Information Protection Law" provides for more detailed notification of sensitive personal information (Article 30). However, in public health emergencies, some information handlers have misconceptions about the duty to inform and self-interest, and use "superficial information" to obscure the actual fulfillment of the duty to inform. The so-called "superficial notification" refers to the privacy policy that is piled up with long, complicated, and obscure jargon, and does not effectively fulfill the legal requirement of "truthful, accurate, and complete notification to individuals in a conspicuous manner and in clear and understandable language", resulting in the fact that face recognition information flows to the direction of corporate self-interest in a seemingly reasonable way. According to the Face Recognition and Public Health Research Report (2020) [11] (hereinafter referred to as the "Research Report"), most people do not know which entities own their facial data; 89.5% of respondents believe that they should be informed of the purpose and use of obtaining facial information; 85.9% of respondents believe that they should be informed of the application scenarios for expanding facial recognition; and 93.2% of respondents believe that they should be informed in should be informed in advance if there are other uses for facial data after a public crisis is over.

4.2.2 Failure of the Consent Principle

The "Personal Information Protection Law" provides for separate consent for sensitive personal information except in special cases and rules for written consent when specifically provided for by law (Article 29). In this case, "consent" should be "explicit (express) consent", not "presumed consent" (neither implied nor silent consent is allowed). The Research Report states that in the context of public health emergencies, the "consent principle" is often a mere formality, and there is a prominent problem of "mandatory use" of face recognition technology applications, such as being applied in the "traffic security check" scenario, "real name registration", "account opening and closing", "payment transfer" and "access control and attendance ". The main manifestation is the formation of a seemingly consent-free zone through the ambiguous way of "presumed consent". The "explicit consent" is often blurred or even ignored by the subject of information collection, and "tacit declaration" or even "silence" becomes the legal passport for personal information collection by face recognition technology [12]. In the case of ignorance of the risks or under pressure of the situation, the consent of the information subject neither complies with the law nor truly reflects the will of the information subject. What it recognized is the face, what it obtained is the data, and what it violated or degraded is the subjectivity and dignity of the individual.

4.3 Risk of Algorithmic Bias

Face recognition technology is inherently error-prone. Biometric feature comparison systems never provide a answer of yes or no, but it is the probability of a match [13]. According to foreign studies, face recognition is biased to varying degrees against women, people of color, immigrants, workers, people with disabilities, low-income groups and religious minorities. According to the study by the Pew Research Center (Pew) in 2018, men appear twice as often as women in news feeds posted by Facebook, given the reality of a relatively balanced gender ratio of the U.S. population. Algorithmic bias is mainly due to the fact that face recognition later in the market relies on the "training" of data readings in the early stages, making the technology have a certain degree of fixed understanding of the characteristics of individual face information, affecting the accuracy of face recognition later in the process and leading to false recognition.

5. THE GOVERNANCE PATH OF FACE RECOGNITION APPLICATION RISK

Risk is both real and non-real. The core of risk awareness lies not in the present, but in the future. The uncertainty of risk has greatly increased, and the path of governance in risk society has shifted from post-response to prevention and control in advance [14].

5.1 Strengthening the Legal Protection of Privacy

5.1.1 Equal Emphasis on the Protection of Public Interest and Individual Privacy Interests

Individual rights and interests cannot be sacrificed in the name of public interest protection and social management efficiency, and the balanced protection of public interest and individual rights and interests should be done [15]. The priority of public interest and the protection of individual rights and interests is the key to mitigate the conflict between administrative emergency management and personal information protection. Specifically,

Public interest should not override individual rights and interests. In a conflict of interest, the public interest does not ipso facto have priority, and people's understanding of the priority of the public interest cannot be absolute and one-sided, overemphasizing the opposition of the two and ignoring the unity of the two. Secondly, it is necessary to realize the "multi-win" and "harmony" between public interests and individual privacy interests. On the one hand, the rapid development of network information technology can provide powerful technical support for the collection and storage of face information. On the other hand, face information is naturally mobile and shareable, involving concerns others and social public interests. On the surface, the more emphasis is placed on public interest and public order management, the more inclined it is to expand the scope of face recognition applications in public space, meaning the enhancement of the infringement risk of individual privacy interests. In fact, as long as the purpose of using face recognition and the processing and flow of data are strictly restricted and the use of face recognition for correlation analysis is prohibited, there is no substantial conflict between the two.

5.1.2 Clarifying the Scale of Privacy Abatement

Face recognition technology applications are more invasive to personal privacy, and almost all current face recognition systems are not infallible against automatic counterattack algorithms, which dictates that the general application of face recognition technology does not meet the minimal impairment required by the narrow proportionality principle. In terms of the overall trade-off between the costs and benefits to society, the balance that "the privacy rights that may be violated should be less than the public security interests to be protected" cannot be generally satisfied. First, the number of unnecessary face recognition applications should be reduced, and the number of face recognition applications deployed in response to crises should be reduced after the order of social life is restored to normal; secondly, stricter restrictions should be followed, which can only be applied to the specific causes of safeguarding major public interests, rather than being generally used to maintain social management, so as to minimize the possible social risks and hidden dangers.

5.2 Establishing a Sound Legal Regulation System for Face Recognition

5.2.1 Speeding up the Special Legislation of Personal Biometric Recognition Information

The legal protection of personal biometric recognition information such as face information at the national level could be seen in the "Civil Code", the "Personal Information Protection Law" and relevant judicial interpretations, which are all principled provisions on the handling of personal information and lack of practical provisions. Therefore, it is difficult to effectively protect the security of personal biometric recognition information. The special legislation on personal biometric recognition information should be completed expeditiously, and clear provisions should be made in the following aspects in addition to clarifying the scope of protection and the subject of obligation, strengthening the accountability, and increasing the punishment for infringement of biometric recognition information.

5.2.2 Adhering to the Principle of Stronger Informed Consent

Face recognition information has the characteristics of unconsciousness, non-contact and intrusiveness in use, and it is more sensitive than voice print, iris and fingerprint information, etc. The processing of face information should adhere to differential regulation means and uphold the principle of stronger informed consent.

The first is to adhere to the principle of being sufficient and necessary. "Being sufficient" means that the principle of necessity is strengthened and the collection of sensitive personal information such as face information should be kept with maximum restraint, i.e., "minimum sufficiency". From a formal perspective, information processors can only process the least amount of information relevant to the purpose of processing, and the type, amount and duration of processing sensitive personal information must be necessary to achieve the specific purpose, i.e., the least type, the least amount and the shortest duration. In essence, sensitive personal information such as face recognition information can be collected only if the purpose of processing cannot be achieved by other reasonable means [16], which is "direct relevance". Such sensitive personal information cannot be replaced by other information, which is "non-substitutable".

The second is the principle of separate and explicit consent. As face recognition information is sensitive personal information, information processors need to inform information subjects in a separate document outside their privacy policies and conditions of use, so as to enhance the transparency of processing acts and truly achieve the goal of fully informed, voluntary, clear and separate consent. The "explicit" here is generally reflected in the affirmative actions such as clicking "agree" and entering the verification code, while the "separate" emphasizes that the interface of consenting to the processing of face recognition information should not include other processing matters. In exceptions, although the consent of the information subject is not required, it is suggested to inform the purpose, manner, scope and duration of the use of face recognition information in a prominent and easily understood way. If it is impossible to inform in time, it should also be informed after the emergency or objective obstacles are removed.

Third is to construct a dynamic consent model. The dynamic consent model was first proposed by American scholars, allowing information subjects to choose their trusted way of knowing and preferred content in different situations, and have the freedom to consent or withdraw consent at any time for the authorized use of their personal information [17]. First, the information subject's participation in the information processing is substantially increased. Compared with the complicated and lengthy "user instructions" provided by various industries today, the dynamic consent model fully reflects the autonomy of the parties. Moreover, the dynamic consent model gives the information subject the right to withdraw consent after learning the facts, changing the disadvantages of the traditional model in which informed consent is consent and consent is forever.

5.2.3 Sound Regulatory Mechanism of Face Recognition Algorithm

Although the "Personal Information Protection Law" proposes norms for automated decision-making, the right of refusal and the right of interpretability from the perspective of avoiding automated decision-making that harms the rights and interests of individuals, it still cannot adequately respond to the problems of face recognition algorithms themselves being defective or being improperly utilized, and an algorithm regulatory system can be established for the whole process before, during and after the event.

Before the event: algorithm security assessment and algorithm filing should be conducted. Algorithm security assessment can ensure that the algorithm has performance control parameters such as recognition accuracy, error acceptance rate, and correct acceptance rate that are appropriate to the level of face recognition certification conducted. Algorithm filing is mainly applied to the developers of some larger and face recognition algorithms of higher risk, enabling the regulatory authorities to grasp the key contents of their algorithm applications and conduct dynamic monitoring and certification.

During the event and after the event: algorithm checking refers to the provision of public checking channels by algorithm applications to users or the public, so that users, traders or third parties have the opportunity to check whether the algorithm can achieve its claimed goals. Then, there is a considerable degree of understanding and expectation of the algorithm operating mechanism

[18]. On the other hand, algorithm monitoring is the daily monitoring of the application scenarios, data processing, and impact effects of algorithms from the purpose of early warning and prevention of possible risks arising from their application.

5.3 Active Development of Specialized Standards for Face Recognition

In the fields of information technology, environmental protection, and product quality, national standards and industry standards play an indispensable supporting role in guiding enterprises to comply. In addition to the rule of "hard law", it is also possible to refine the autonomy of face recognition technology application with the help of "soft law" such as national standards and industry standards, and incorporate them into the face recognition specification system for overall consideration. The collectors, controllers and processors of biometric information may engage in activities related to the collection, storage and processing of personal biometric information only after they have been approved and licensed for application. In the future, an innovative pattern of refining and scenario-based management of face recognition technology applications will be formed with the help of national standards and industry standards under the umbrella of general rules of laws and regulations.

6. CONCLUSION

Scientific development and technological innovation are essential for mankind to overcome catastrophes and pandemics [19], and high technology is often born with the vision of promoting the formation and development of a "healthy society". As a representative technology of the new generation of information technology, face recognition can provide a powerful technical guarantee for social governance in the context of public health emergencies. At the same time, the personal information corresponding to face recognition technology covers multiple legal interests. Without scientific and effective legal regulation, it will certainly induce complex and multiple social risks. Therefore, the one-size-fits-all use ban model is not in line with China's national conditions, and the direction of legal regulation of technology applications in China is to "advocate a responsible use" and to legislate within the limits of national development needs.

AUTHORS' CONTRIBUTIONS

Yuqing Zhang contributed the central ideas and was responsible for the final revision of the paper. Jiao Guan designed the thesis outline, coordinated the writing arrangement of the paper, and revised the first draft. Wenjie Liu and Ruijie Wang revised the thesis outline, collected and analyzed data. Honglin Zhu and Liuyang Jian collected and analyzed typical cases. All authors analysed the literature and were involved in writing the manuscript.

ACKNOWLEDGMENTS

"Research on Privacy Protection in the Context of Medical Artificial Intelligence" (YF21-Y41) by Sichuan Health Rule of Law Research Center, a key research base of philosophy and social sciences in Sichuan Province.

REFERENCES

[1] Wang Huiquan, Liu Lu. Governance of Public Health Emergencies in the Application of Artificial Intelligence [J]. Medicine and Society, 2021,34 (07): 42-46. DOI: 10.13723/j.yxysh.2021.07.009. (in Chinese)

[2] Zheng Yushuang. Solving the Problem of Technology Neutrality: Rethinking the Relationship between Law and Science and Technology in Jurisprudence [J]. Journal of East China University of Political Science and Law, 2018,21 (01): 85-97. (in Chinese)

[3] Li Qingfeng. Legal regulation of face recognition technology: value, subject and effective means [J], People's Forum, 2020 (11): 108-109. (in Chinese)

[4] Xu Jingze, Wu Zuohong, Xu Yan, et al. Face Recognition Based on PCA,LDA and SVM Algorithms [J], Computer Engineering and Application, 2019, 55 (18): 34-37. (in Chinese)

[5] Zhao Jingwu. The general rule shift of the governance logic of face recongnition — taking technical transparency as the basic position [J]. Northern Law Journal, 2022,16 (01): 5-14. DOI: 10.13893/j.cnki.bffx.2022.01.001. (in Chinese)

[6] Han Xuzhi. Research on personal information typology [J]. Journal of Chongqing University of Posts and Telecommunications (Social

Science Edition), 2017, 29 (04): 64-70. (in Chinese)

[7] Gu Liping. From Identity Recognition to Body Manipulation:Research on Privacy Protection in Intelligent Biometric Technology [J]. Journal of Shanghai Normal University (Philosophy and Social Sciences Edition), 2021,50 (05): 5-13. DOI: 10.13852/J.CNKI.JSHNU.2021.05.001 (in Chinese)

[8] American Civil Liberties Union. Dawn of Robotic Monitoring: Artificial Intelligence, Video Analysis and Privacy [EB/OL] https://www.aclu.org/report/law-ro-bot-surveillance. (in Chinese)

[9] Yuan Jun. Application Risk and Legal Regulation Path of Facial Recognition Technology [J]. Research on Information Security, 2020, 6 (12): 1118-1126 (in Chinese)

[10] Zhang Xiu. Discussion on the Ethical Principle of Injury Minimization in the Vision of Intelligent Communication — Taking Intelligent Face Recognition Technology as an Example [J]. Contemporary Communication, 2020 (02): 82-84 (in Chinese)

[11] Beijing Institute of Artificial Intelligence. Research Report on Face Recognition and Public Health (2020) [EB/OL] https://attachment.baai.ac.cn/share/aies/cn-facial-recognition-and-public-health-2020-05-17.pdf (in Chinese)

[12] Yang Fuwei, Bai Jiaye. The legal risk of face recognition technology and its scenario-based governance [J]. Journal of Chongqing University of Technology (Social Science), 2022,36 (01): 180-190 (in Chinese)

[13] Xing Huiqiang. Legal Regulation of Face Recognition [EB/OL] http://fzzfyjy.cupl.edu.cn/info/1035/13047.htm

[14] Yuan Quan. Legal Logic and Institutional Construction of Face Recognition in Public Space Applications [J]. Northern Law Journal, 2022,16 (01): 26-35. DOI: 10.13893/j.cnki.bffx.2022.01.003 (in Chinese)

[15] Yuan Quan. Legal Logic and Institutional Construction of Face Recognition in Public Space Applications [J]. Northern Law Journal, 2022,16 (01): 26-35. DOI: 10.13893/j.cnki.bffx.2022.01.003 (in Chinese)

[16] Cheng Xiao. Understanding and Application of Personal Information Protection Law [M]. Beijing: China Legal Publishing House, 2021 (in Chinese)

[17] Shi Jiayou, Liu Siqi. Personal Information Protection in Face Recognition Technology — on the Construction of Dynamic Consent Pattern [J], Financial Law, 2021 (02): 60-78 (in Chinese)

[18] Su Yu. Pedigree of Algorithm Regulation [J]. China Law, 2020 (03): 165-184 (in Chinese)

[19] Xi Jinping. General Secretary Xi Jinping's important speech at the symposium for experts and scholars points out the direction of scientific research attacks [EB/OL]. http: //www.xin-huanet.com/politics/leaders/2020-06/04/c_ 1126074999.htm. (in Chinese)