WEP Warwick Evans Publishing

Transactions on Social Science, Education and Humanities Research
ISSN: 2960-1770, eISSN: 2960-2262 | Volume 13
ECSS 2024

Face Recognition Technology Ethical Governance Issues

Lan Ma [1, a], Yaqiong Peng [1, b], Changmao Cao [2, c, *]

[1] School of Marxism, Jianghan University, Wuhan 430056, China

[2] School of AI, Jianghan University, Wuhan 430056, China

[a] lanhorse@163.com, [b] 305714578@qq.com, [c] 791543985@qq.com

* Corresponding Author

Abstract. Face recognition technology is a biometric recognition technology based on computer technology to identify people's facial features. When modern intelligent societies commonly use machine "face authentication" to prove individual identity, this common behavior will bring various risks, including the risk of the technology itself and the social risks of technology abuse. From the perspective of governance, the construction of a governance framework that includes ethical principles and a technology monitoring mechanism can timely reduce or even resolve the harm that technology can do to society and individuals, and reflecting the humanistic orientation of the "good use" of technology.

Keywords: Face recognition technology; Risk management; Ethical issues; Governance.

1. Introduction

As a physiological and psychological basis for perceiving identity, emotion and spatial relationship, the human face plays an important role in social life. In the ancient times of China, the unique facial features of the human body were used to identify criminals. Artists often use the face as a carrier to convey meaning, show themselves, and express perception and emotion. Today, Face Recognition Technology (FRT) is a kind of biometric technology based on computer technology to identify people's facial feature information. This technology has already penetrated into our daily life, from the face unlock function of smart phones to the identity recognition of access control. As an emerging technology, face recognition invaded every aspect of our lives, which was closely related to the interests of the general public, and the related risks would attract more attention.

2. Ethical risks of FRT

2.1. The risk of the FRT itself

Identification errors include two situations: one is that the face image information contained in the face database is inaccurate and prone to recognition errors; the other is that the system fails to associate the captured face image with the corresponding image in the database, and the target cannot be identified, resulting in recognition errors. For example, the facial recognition system used by the military police in Rio de Janeiro mistakenly identified a woman as an escaped criminal and arrested her [1]. It can be seen that the existing facial recognition technology is far from reliable and will inevitably face a series of risks. Unlike unique DNA information, human faces have similarities and are easy to change. Recognition technology relies on the input of the proportion and structural features of the face, and it is difficult for facial recognition to work if they are identical twins or two people who are extremely similar after facial plastic surgery.

Because facial recognition technology relies on machine learning from a large database, if the algorithm fails to include different races, genders, ages, origins or backgrounds, it is easy to produce facial recognition bias based on the database. The recognition of certain specific groups in facial recognition technology varies due to demographic characteristics such as age, gender, race, and ethnicity. Even in constantly updated facial recognition systems, the recognition rate of men is higher

than that of women; the recognition rate of elderly people is also higher than that of young people[2]. The efficiency of facial recognition technology is observed to decrease by 2 to 3 percentage points with each doubling of the size of the facial recognition database, according to additional statistical data [3]. These seemingly insignificant "technical problems", when applied to social practice, may sacrifice the interests of some people and create important ethical risks. This requires researchers to abide by the corresponding professional ethics and adhere to the ethical principle of non-harm in the development, testing, and use process.

The opacity of facial recognition technology can also lead to risks. Technical opacity refers to both the opacity of the technology itself and the opacity of the deployment process of facial recognition technology. Face recognition technology is hidden, embedded technology, it is embedded in machine systems, its operation is difficult for non-specialists to understand. Most of the algorithms in face recognition systems are proprietary software and it is difficult to inspect and review them. Even if the code can be examined line by line, it is difficult to examine the running code because it is implemented through multiple layers of transformations. At the basic level there is the current passing through the silicon chip, and at the highest level there are program instructions, but it is almost impossible to trace the connections between the programs being executed. In short, software algorithms are operationally opaque. In addition, the deployment of the face recognition technology system is achieved in a non-invasive, contact-less, flexible mobile way, and in many occasions, the use of the face recognition technology system does not require the participation and consent of the scanning target. However, the use of face recognition technology in public often occurs without prior notification. If relevant governance measures are not taken, it may cause systemic risks, including the way face images are obtained and used, and the problems caused by algorithms that do not consent or choose not to be identified. Therefore, informing the purpose and reasons for the use of facial recognition technology in public places, as well as the time and scope of facial data storage, can improve the transparency of the use of technology.

2.2. Social risks of technology abuse

In addition to the technical risks, the misuse of facial recognition technology can also lead to social risks, among which the most concern is the infringement of privacy and the generation of new social injustice.

In 2019, the "first face recognition technology case" in Hangzhou attracted the attention of the whole society to the abuse of face recognition technology. The case is questioning the commercial use of face recognition technology. The case is a landmark ruling that has aroused public discussion on the protection of facial privacy. When government departments use facial recognition technology to verify someone's identity, the individual's attitude towards the technology is insignificant. Face recognition technology is not only commonly used by law enforcement agencies, but also in the private and commercial sectors. Furthermore, facial data stored in code makes people's facial identities easy to be obtained by third parties, and once the data is retained, it can be easily reused for profit. Shoshana Zuboff, a professor at Harvard University, described this process as "surveillance capitalism", arguing that data extraction greatly reduces the information cost of corporate actors and redistributes privacy rights from consumers to companies. Therefore, the information asymmetry between private face recognition users and data subjects increases the possibility of misuse of the technology.

In addition, the abuse of facial recognition technology is likely to cause new social injustice problems. When face recognition as an intelligent technology can provide a very cost-effective method for society, it will make most organizations gradually rely on this technology and naturally become the default technology to solve a range of technical and social problems. But the reality is that it is no longer just a tool for identifying terrorists, but it has become a set of standards and a system in itself. The "ambiguous" nature of face recognition technology makes it difficult for society to scrutinize it, creating unprecedented opportunities for "invisible" Micro politics to become ubiquitous. The social injustice caused by its design or use lies in the way it is designed and operated. The design of

technology includes certain interests and excludes others. This is exactly what ethics needs to pay attention to, that is, the interests of some people are excluded due to the characteristics of face recognition technology itself. Current situation of ethical risk management of face recognition technology

With the advent of intelligent society, the rapid development and overuse of facial recognition technology have put the entire society in a difficult situation. In this case, it is difficult to solve the current risks generated by the technology without resorting to a unified regulatory framework and governance measures applicable to facial recognition technology. However, like other emerging technologies, the government's awareness of ensuring the responsible use of facial recognition technology usually lags behind the abuse of this technology. While it takes time to develop new legal norms, it is necessary to conduct timely ethical governance according to the applicable standards of the existing legal framework.

The United States has taken early legal measures on biological recognition technology. In 2008, the State of Illinois passed the Biometric Information Privacy Act, which is the first regulatory bill for biological recognition technology in the United States. The Act requires enterprises to clearly inform users in writing how biometric information is collected, stored, and used before collecting personal biometric information, and enterprises can only collect users' biometric information after obtaining their written consent [4]. In the European Union, the processing of biometric data is explicitly covered in the General Data Protection Regulation (GDPR), which came into force in 2018 and sets a global benchmark for privacy and personal data protection . China and the West share the same regulatory attitude towards facial recognition technology, both have taken proactive governance measures. However, the difference is that there are no large-scale restrictions or bans on facial recognition technology at present, but existing legal norms can prevent the abuse of facial recognition technology to a certain extent. In 2019, the Data Security Management Measures were released, emphasizing the protection of personal biometric information. In 2021, the Supreme People's Court also issued the "Provisions on Several Issues Concerning the Application of Law in the Trial of Civil Cases related to the Processing of Personal Information by Face Recognition Technology", which helps to deal with and solve some dispute issues related to face recognition technology in practice. In 2022, The General Office of the State Council of China issued the Guidance on Strengthening the Ethical Governance of Science and Technology, which is deployed at the national level and shows the importance it attaches to the ethical governance of science and technology.

3. Current situation of ethical risk management of face recognition technology

With the advent of intelligent society, the rapid development and overuse of facial recognition technology have put the entire society in a difficult situation. In this case, it is difficult to solve the current risks generated by the technology without resorting to a unified regulatory framework and governance measures applicable to facial recognition technology. However, like other emerging technologies, the government's awareness of ensuring the responsible use of facial recognition technology usually lags behind the abuse of this technology. While it takes time to develop new legal norms, it is necessary to conduct timely ethical governance according to the applicable standards of the existing legal framework.

The United States has taken early legal measures on biological recognition technology. In 2008, the State of Illinois passed the Biometric Information Privacy Act, which is the first regulatory bill for biological recognition technology in the United States. The Act requires enterprises to clearly inform users in writing how biometric information is collected, stored, and used before collecting personal biometric information, and enterprises can only collect users' biometric information after obtaining their written consent.In 2019, the United States introduced the Commercial Facial Recognition Privacy Act, which provides legislative supervision over the commercial application of facial recognition. The law prohibits the use of facial recognition technology without the consent of data subjects, and sets certain limits on what information enterprises can collect about individuals and

what they can do with it . This legislation is an important measure for privacy protection. Currently, several states in the United States have enacted bills prohibiting facial recognition technology, and explicitly prohibit government departments from using facial recognition technology in public places. The strict stance of the United States towards facial recognition technology is not only reflected in the legislation, but also in some high-profile case handling.

In the European Union, the processing of biometric data is explicitly covered in the General Data Protection Regulation (GDPR), which came into force in 2018 and sets a global benchmark for privacy and personal data protection. According to this law, biometric data is defined as "personal data generated by specific technical processing related to the physical, physiological or behavioral characteristics of natural persons, such as facial images". The GDPR introduces the principle of data minimization, which states that the collection of personal data is "limited to cases where it is necessary for the purpose for which the data is processed" and where the collection of biometric data is "necessary for reasons of significant public interest" [4]. The EU has adopted the principle of protecting people from the threat of facial recognition technology, prohibiting the processing and sharing of biometric data without consent. In April 2021, a bill aimed at strengthening the regulation of artificial intelligence technology was released, banning automatic facial recognition in public places within the EU, with only three exceptions: looking for missing children; removing the threat of terrorist attacks; and pursuing specific criminal suspects within the scope of the law [4]. The EU Data Protection Commission (EDPB) and the EU Data Protection Supervision Agency (EDPS) have further called for the prohibition of the use of artificial intelligence to automatically identify personal features in public places, including faces, gaits, fingerprints, DNA, voices and other biological information [5]. The EU is planning to impose stricter restrictions on the use of facial recognition technology to give EU citizens clear rights to use their facial data.

China and the West share the same regulatory attitude towards facial recognition technology, both have taken proactive governance measures. However, the difference is that there are no large-scale restrictions or bans on facial recognition technology at present, but existing legal norms can prevent the abuse of facial recognition technology to a certain extent. The Network Security Law of the People's Republic of China implemented in 2017 prohibits network service providers from collecting and selling personal information of citizens without consent [6]. The Information Security Technology Personal Information Security Code, issued in 2018, sets out guidelines for consent on how personal data can be collected, used and shared. In 2019, the Ministry of Science and Technology promulgated the Principles of New Generation AI Governance: Developing Responsible AI, which included the principle of respecting privacy. In 2019, the Data Security Management Measures were released, emphasizing the protection of personal biometric information. In 2020, the Personal Data Protection Law was issued, providing a more comprehensive framework for the protection of personal data rights, and introducing the concept of biometric data protection. The Civil Code of the People's Republic of China, which took effect in 2021, stipulates that biometric data of individuals should be protected. In July 2021, the Supreme People's Court also issued the "Provisions on Several Issues Concerning the Application of Law in the Trial of Civil Cases related to the Processing of Personal Information by Face Recognition Technology", which helps to deal with and solve some dispute issues related to face recognition technology in practice [7]. For example, the extension of the use of face recognition technology to process personal information related civil cases is clearly defined, which specifically refers to a series of civil cases caused by the use of face recognition technology to process face information in violation of the law. In March 2022, The General Office of the State Council of China issued the Guidance on Strengthening the Ethical Governance of Science and Technology, which is deployed at the national level and shows the importance it attaches to the ethical governance of science and technology.

4. Face recognition technology ethical risk management dilemma and its reasons

4.1. Conflict of values

There is a conflict between values such as public security and personal privacy. Do Whether it is the legislative department or enterprises, it is very difficult to balance the conflict of values such as public security and citizens' personal privacy. Public security includes different levels, the first is the security of the national level, such as the harm caused by terrorist attacks to the public; There is also a breakdown of security at the community level, such as law and order. Different levels of public security may ultimately have an impact on an individual's life, property, or liberty. Preventing and strengthening security protection through face recognition technology is an effective technical measure, which helps to enhance the security of individuals and society, such as preventing online fraud and preventing criminal behavior. From an ethical perspective, privacy is a right for individuals to enjoy the protection of their private affairs, and is the pursuit of personal freedom and dignity. If a society does not have a common understanding of individual privacy protection, the society will not have respect and trust, and there will be no long-term stability and unity. The privacy right related to personal data of facial recognition largely lies in the right to control access and use of these data. For example, technically restricting unauthorized access to private information and solving privacy infringement problems with technology can strengthen privacy protection. Of course, the right to privacy is not absolute, and its boundaries are not clear or need to be broken under certain conditions. For example, in a public space, people have the right not to have their personal face images taken by facial recognition machines, so as not to be freely circulated on the Internet. If some public spaces are monitored by facial recognition technology to detect and prevent crimes, and the resulting personal facial images are only provided to the police and used to identify criminal suspects in the area, then the right to privacy may be overridden by security interests. Therefore, in any case, to use face recognition data or not to use it is not an absolute right, but a restricted right. At the same time, expanding the use of face recognition databases and systems must serve specific security purposes and have clearly proven effective.

4.2. Differences in personal privacy awareness.

There are great differences in people's understanding of personal privacy in different periods and backgrounds. Although maintaining public security is a basic value of human society, it is also a basic ethical principle and value concept of democratic society to focus on the protection of personal privacy. Due to different cultural backgrounds, people in some countries are more sensitive and concerned about the privacy of individuals, while in other countries, people have a tolerant attitude towards privacy. However, as the concept of data privacy becomes more and more popular, people's awareness of privacy is also increasing. According to the survey data of the Observation Report on the Landing Scene of Face Recognition (2019) published by Southern Metropolis Daily, a total of 80% of the respondents worry that the safeguards of the face recognition system operators are not enough, and 74% said that they would prefer to use traditional identification methods rather than face recognition technology [8]. In particular, the commercialization of face recognition technology should be wary of the misuse of private collection, processing, analysis and use of personal information. Most commercial facial recognition technology does not make substantial notice of the collection method, scope, purpose, storage time, etc., or seek the consent of the subject when collecting facial information. In addition, people's differences in understanding of personal privacy rights are also reflected in the differences in protection methods. Ethical concerns about face recognition data for subjects are usually related to injury events, including tangible injuries, such as health injury, financial losses, or discrimination. Therefore, the core issue is who uses facial recognition technology? And under what circumstances and for what purpose? Should the use of face recognition technology be banned until the legal framework and privacy and security safeguards are perfected? Different answers to these questions are related to the differences in the understanding of privacy.

4.3. Conflict of interest.

There will also be conflicts between the economic interests of different political groups, and between corporate and individual interests. These conflicts are demonstrated as follows: when balancing the values of personal privacy and justice against social and economic interests, governments and enterprises prioritize economic growth and tend to defend the utilization of face recognition technology due to its societal benefits. In a market-driven society, the pursuit of social and economic interests is the objective of capital, sometimes overshadowing individual concerns. Face recognition technology also represents an emerging force in scientific and technological innovation, serving as a wealth-generating tool across various sectors while fostering competition among nations. Consequently, it stimulates advancements in face recognition technology as a crucial asset for maintaining scientific and economic advantages, leading to substantial investments in this domain. From an economic standpoint, certain countries exhibit caution regarding how foreign companies access global face data by adopting a dual-target approach that often blames firms from other nations. Ethical conflicts surrounding face recognition technology can also directly relate to technical aspects such as standards and routes. Ultimately, those who establish new regulations for technology enjoy first-mover advantages; thus having control over setting standards and rules can bring huge benefits to businesses.

5. Suggestions for ethical risk governance of face recognition technology

5.1. Risk assessment of the technology

Conduct a rigorous risk assessment of face recognition technology and establish a practical framework for ethical governance. Risk assessment serves as an essential validation process in technological innovation. The initial step involves defining the risks associated with face recognition technology, including potential harm inflicted upon individuals as well as weighing societal risks against costs and benefits. Risk assessment is an ongoing dynamic feedback process that relies on input from technical experts while also considering stakeholder feedback following the marketization of this technology.

5.2. Embedding ethical principles and rules

Integrate ethical principles and rules into the governing mechanism of face recognition technology. Ethical principles are specific codes of conduct agreed upon through ethical deliberation that align with the interests of all parties involved. In relation to the application of face recognition technology, establishing minimum data principles, transparency principles, non-discrimination principles, and informed consent principles can ensure responsible that facial recognition technology develops in a safer manner. These principles require that facial data be collected only in the minimum range necessary, avoid excessive data collection, processing, and storage, disclose relevant information in a timely and sufficient manner, explain all possible predicted risks, and ensure the autonomous control of facial data subjects over biological data.

5.3. Establishment of a government-oriented regulatory

How to strengthen regulation at the institutional level and rational and reasonable ethical governance is a necessary procedure. Comprehensive and integrated face recognition databases and systems need to be regulated by the government. It is the responsibility of the government and enterprises to let the public know about the use of face recognition systems, and to obtain authorization and consent from individuals to use the technological systems for specific and legitimate purposes. Additionally, the government should act as an intermediary between various stakeholders in society by facilitating dialogue platforms between professionals and the public while promoting scientific education on face recognition systems through media channels.

5.4. Categorical governance

The formulation of regulatory policies needs to take into account the specific situation, formulate and adjust relevant governance measures in a timely manner, and categorize governance without generalization. Until legal provisions related to face recognition technology come into effect, consideration should be given to suspending the use of such technology in public spaces, especially campuses, hospitals and government agencies. Facial recognition technology for commercialization and online platforms should also be subject to judicial review, and penalties, including administrative measures and administrative fines, should be imposed for violations.

5.5. Enhance international cooperation

International cooperation on face recognition technology aims to foster responsible research and utilization of related technologies on a global scale, involving technology research and development, technology sharing, technology security, and national interests. After all, the fundamental purpose of the development of face recognition technology is to serve as a means to promote human prosperity, improve personal and social well-being, and bring technological progress and innovation. Therefore, when it comes to the differences in capital investment, economy, culture and legal norms between different countries, increasing international cooperation and data sharing is conducive to constructing universal value norms that are in line with all of humankind, eliminating the chasm, and preventing the occurrence of behaviors that impact on the common ethical bottom line of humankind.

Acknowledgements

(1) Humanities and Social Sciences Research Project of the Ministry of Education (20YJAZH076);

(2) Jianghan University Humanities and Social Science Pre-Support Project (2023YYJ05).

References

[1] Guimarães Moraes, Thiago Guimarães Moraes, et al. Smile, you are being identified! Risks and measures for the use of facial recognition in semi- public spaces. AI and Ethics. 2021(2): 159- 172.

[2] Davies T. N.,Hoffman D. D.Facial Attention and Spacetime Fragments. Axiomathes. 2003(13): 303-327.

[3] Lucas D. Introna. Disclosive ethics and information technology: disclosing facial recognition systems. Ethics and Information Technology, 2005(7): 75 -86.

[4] Qingxiu Bu. The global governance on automated facial recognition (AFR): ethical and legal opportunities and privacy challenges. International Cybersecurity Law Review. 2021(1): 1-33.

[5] The EU artificial intelligence legislation is in progress: calling for a ban on face recognition in public places, strict regulation or for the market [EB / OL]. (2021 - 06 – 28) [2024-07-08].

[6] Cybersecurity Law of the People's Republic of China [EB / OL]. (2016 - 11 – 08) [2024-06-20]. https://www. chinastor. com/netsafe/051IDP2017.html.

[7] The Supreme People's Court. Provisions on Several Issues of Applicable Law in Hearing Civil Cases Related to the Processing of Personal Information by Facial Recognition Technology [EB/OL]. (2021-07-28) [2024-06-20]. https: // www.court.gov.cn/zixun-xiangqing-315851.html.

[8] Face recognition Landing Scene Observation Report (2019) [EB/ OL]. (2019-12-05) [2024-06-08]. https://xw.qq.com/ cmsid/20191205A0DETN00?F=newdc.