Discussion on Ethical Conflicts and Regulations Regarding the Abuse of Visual Recognition Systems in Public Spaces

Xiufeng Zhang[1*], Xintong Lin[1]

[1] Guangdong Polytechnic Normal University, Guangzhou, 510000, China

[*] 1509376259@qq.com

https://doi.org/10.70695/IAAI202501A7

Abstract

Against the background of frequent abuse of visual recognition systems in public spaces, this paper conducts a preliminary review of domestic and international research on frontier technology ethics. It highlights that the potential privacy invasion risks of facial recognition technology, as well as the infringement of personal dignity, cannot be ignored. Research indicates that applying the principle of proportionality and the basic rights rule is crucial for regulating the use of facial recognition technology. To reduce moral risks in technology application and enhance public trust, this paper proposes important recommendations, including restricting the qualifications of entities collecting and processing facial information, clarifying the purpose of use, strictly implementing information processing procedures, and establishing a supervision mechanism. These measures aim to mitigate ethical risks in technology applications, enhance public trust, and promote legislative progress and the refinement of ethical frameworks.

Keywords Artificial Intelligence; Visual Recognition; Ethics; Morality; Public Space

1 Introduction

In recent years, the accuracy of facial recognition technology has gradually improved. Literature review reveals that the accuracy of facial recognition under different experimental conditions ranges from 95.5% to 99.4%, reflecting the relative stability of this technology in practical applications [1]. However, with the improvement of recognition accuracy, the false recognition rate has been relatively controlled at the level of 0.16% [2]. Nevertheless, this false recognition rate may still bring potential ethical risks, especially in fields involving public safety and personal privacy. When the recognition system mistakenly identifies innocent individuals as criminal suspects, it may cause serious impacts on their lives and reputations.

Globally, the research and ethical issues of PSVRS (Public Space Visual Recognition Systems) have attracted widespread attention from academia and society [3]. Scholars in many Western countries, such as E.A.Smith of the University of California, Berkeley, have conducted in-depth discussions on the application of visual recognition technology in surveillance systems and the ethical and moral crises it causes through a combination of qualitative and quantitative research methods. Specifically, through long-term and short-term empirical case analysis, they have revealed the potential risks of such technologies in infringing personal privacy and liberty.

It can be seen that the existing research is not entirely in place in terms of identifying moral crises. Although some scholars have conducted preliminary discussions from the perspectives of privacy protection, false recognition, and algorithmic discrimination, the in-depth analysis of moral crises is relatively insufficient.

2 Overview of the Characteristics and Application Status of Facial Recognition Technology in Public Spaces

FRT (Facial Recognition Technology) is an advanced technology based on biometric recognition. Its core lies in conducting identity verification by capturing and analyzing facial features. The basic principle of this technology is to use computer vision and machine learning algorithms to extract facial features from images captured by lenses, such as facial contours, eye spacing, and nose shape, and compare them with information in a database to identify specific individuals. With the rapid development of DL (Deep Learning) and Big Data technologies, the accuracy and processing speed of facial recognition technology continue to improve, leading to its widespread application in various fields such as public safety, financial payment, and social media.

2.1 Application Scenarios of Facial Recognition Technology

In today's society, FRT has been widely used in various scenarios in public spaces, such as Security Surveillance, Traffic Management, and Public Services [4]. In Security Surveillance applications, FRT enhances the prevention capabilities of public safety by quickly identifying potentially risky individuals. However, this technology faces many ethical challenges in practical operation. For example, how to ensure the balance between data privacy and individual freedom? In the field of Traffic Management, FRT is used to monitor traffic flow and capture traffic accidents in real-time, but excessive monitoring may lead to Data Abuse and Privacy Violations. At the same time, compared with traditional monitoring methods, FRT's efficiency and accuracy have indeed improved the efficiency of automatic law enforcement, but the potential biases of its algorithms may lead to misjudgments of specific groups, reigniting debates on social inequality.

2.2 Risks of Facial Recognition Technology Applications

The widespread application of FRT in public spaces raises many potential risks, especially in terms of security, privacy, and ethics [5]. Since facial recognition systems rely on a large amount of biometric data, its security has become an important concern. Data breaches may lead to the abuse of personal information, thereby triggering identity theft and other cybercrimes. Some studies indicate that hacker attacks and data breach incidents have shown a significant upward trend in the past few years, further emphasizing the threat to personal privacy.

2.3 Current Status of Legislative Protection for Facial Recognition Technology Applications

When discussing the current status of legislative protection for facial recognition technology applications, we need to deeply analyze whether the current legal framework effectively protects citizens' personal privacy rights and data security rights. Currently, China has formulated clear norms for the collection, processing, and storage of personal information in laws and regulations such as the PIPL (Personal Information Protection Law) and the CSL (Cybersecurity Law). However, based on the unique nature of biometric data collection in facial recognition technology, its potential ethical crises still appear particularly prominent.

2.4 Current Status of Law Enforcement Protection for Facial Recognition Technology Applications

In the application field of FRT, law enforcement and public safety are undoubtedly one of its most representative real-world scenarios. In recent years, with the rapid development of technology, FRT has played an increasingly significant role in public safety, especially in the process of crime prevention and investigation. Against this backdrop, governments and law enforcement agencies around the world have increased their investment in facial recognition technology, committed to enhancing social security and prevention capabilities. For example, China widely applies facial recognition technology in urban public safety management, achieving rapid identification and tracking of suspicious personnel through real-time monitoring and data analysis. This measure has shown positive results in reducing violent crimes and effectively responding to terrorist activities.

3 Legal Analysis of the Regulation of Facial Recognition Technology Applications

Facial information is not only a representation of individual identity but also carries profound connotations of personal dignity. The widespread application of FRT in public spaces inevitably erodes individual privacy, truly arousing people's deep concerns about its legality and rationality.

3.1 Privacy Self-Determination Concerned with Facial Information

Against the backdrop of the rapid development of facial recognition technology, the right to privacy self-determination, as an important legal right of individuals in the face of information collection, is becoming increasingly prominent.

3.2 Informed Consent Derived from Facial Information

In today's society, with the rapid development of AI technology, Facial Recognition Systems have been widely used in various public spaces in society, and their potential ethical and legal issues are gradually emerging. Especially within the theoretical framework of informed consent combined with moral constraints, how to protect personal privacy and data rights has become an urgent problem to be solved. The concept of informed consent not only requires providing individuals with sufficient information before data collection but also ensuring that they make autonomous choices based on complete understanding.

3.3 Manifestations of Facial Recognition Technology Infringing Personal Rights and Interests

Firstly, illegal collection. Against the backdrop of the rapid development of FRT, its widespread application in Public Space has become a common phenomenon [6].

Secondly, abuse of information recognition. Information recognition technology has been widely used in modern society, among which FRT is particularly typical. However, with the widespread implementation of this technology, the abuse of information recognition has occurred, leading to serious infringement of the Dignity of Citizens. The unwarranted monitoring behavior based on information recognition technology makes individuals lose their Right to Privacy in Public Space. This is not limited to the leakage of personal information but also blurs the boundaries of individual freedom, forming a hidden and universal social pressure.

Thirdly, covert infringement of citizens' right to know through information use. In the contemporary digital society, the widespread application of visual recognition systems in public spaces, especially FRT, has increasingly attracted attention and discussion from academia and society. This technology uses high-precision algorithms and big data analysis to capture and recognize individual characteristics in real-time. However, the potential privacy infringements in this process are often overlooked. The covert nature of information use makes it possible for citizens' personal information to be collected, stored, and even abused without being informed, resulting in potential Information Asymmetry and infringing citizens' basic requirements for the right to know about their own information.

Finally, information storage leaks reduce citizens' trust. In modern society, the rapid development of information technology, especially the widespread application of AI and VR (Visual Recognition) Technology, while providing technical support for enhancing public safety and social governance, also brings potential ethical and moral issues. Information storage leaks, especially in the process of implementing FR (Facial Recognition) technology, often pose a serious threat to citizens' privacy rights. For example, the collection and storage of personal images and identity information by private companies often lack transparency and effective supervision, leading to improper use or leakage of data, thereby causing citizens to face irreversible trust crises while enjoying the convenience of technology.

3.4 Analysis of the Basic Principles of Public Application of Facial Recognition Technology

The application of facial recognition technology needs to emphasize the two dimensions of legitimate purpose and necessity. This provides a systematic framework for evaluating the public application of facial recognition technology.

Firstly, the application of facial recognition technology has a legitimate purpose. The purpose of applying FRT in public safety, security management, and other fields is to seek well-being for the public and safeguard the legitimate rights and interests of the public.

Secondly, the application of facial recognition technology is necessary. FRT, as an important biometric recognition technology, is increasingly widely used in public spaces. However, it is necessary to control the specific scenarios, locations, covered populations, and the amount of data collected to the minimum necessary extent, and it cannot be expanded arbitrarily.

3.5 Analysis of the Basic Principles of Public Application of Facial Recognition Technology

Compared with the relatively mature application of facial recognition technology abroad, China started late in this field, but the rapid application of technology in recent years has achieved leapfrog development in the industry. Domestic technology companies such as Megvii and CloudWalk have launched various facial recognition-based solutions, applied to public safety, smart cities, and many other fields. At the same time, while these applications bring convenience, they also expose risks such as Privacy Security and Information Abuse [7].

Table 1. Overview of the Application Status of Facial Recognition Technology in Public Spaces

Application Field	Technical Characteristic			Risks	Current Status of Legal Regulation
Real-time	Universality	High Recognition			
Security Surveillance	Yes	Yes	Yes	Privacy Security	Weak Supervision
	Yes	Yes	Yes	Information Abuse	
	Yes	Yes	Yes	Civilized Dignity	
Urban Management	Yes	Yes	Yes	Privacy Security	Weak Supervision
	Yes	Yes	Yes	Information Abuse	
Commercial Marketing	Yes	Yes	Yes	Privacy Security	Weak Supervision

Research shows that the excessive application of technology may constitute an infringement on the Dignity and Privacy of citizens. Especially against the backdrop of monitoring behavior spreading throughout urban public spaces, the abuse and leakage of personal information have become urgent moral crises to be resolved. Empirical research indicates that the public often does not know how their information is being used when faced with facial recognition monitoring, lacking the Right to Information, which directly affects individuals' Trust and acceptance of the technology.

3.6 Basic Rights Rules Provide Legislative Guidance for Personal Information Protection

As one of the core elements in the legal system of personal information protection, the basic rights rule provides necessary theoretical support for protecting individuals' privacy rights and personal dignity in the digital age. Under this framework, the provisions related to personal information protection in international human rights law and the constitutions of various countries should be given special attention [8]. For example, the EU GDPR (General Data Protection Regulation) clearly stipulates the rights of data subjects and strengthens the control of personal information, which provides a strong reference for legislation worldwide [8]. As the core framework guiding the implementation and protection of individual rights, the Fundamental Rights Rules are becoming increasingly important for the review guidance of personal information protection. The basic rights rule emphasizes the comprehensive respect and protection of individual dignity, privacy rights, and personality rights, providing a solid theoretical foundation for improving the legal regulation of facial recognition technology.

4 Legal Regulation Suggestions for Facial Recognition Technology Applications

4.1 Restricting the Qualifications of Entities Collecting and Processing Facial Information

Establishing a qualification review system for data collectors. Globally, with the implementation of privacy protection laws such as the GDPR, the responsibility of information collectors for the security maintenance of privacy information involved in facial recognition technology is increasingly prominent. Therefore, reviewing the information security maintenance standards followed by collectors has become a crucial legal regulatory measure. A series of Standard Audit Methodologies can effectively assess the compliance of facial recognition-related companies and their information security management capabilities. It is necessary to establish a qualification review mechanism for collectors to ensure that they have the corresponding technical capabilities and ethical awareness, and to avoid entities without secure processing capabilities from obtaining sensitive data.

Constructing a facial data audit system. Conducting periodic audits of data owners is an important way to protect individual rights and reduce the risk of misidentification. The audit of information system accuracy not only involves the data collection quality and algorithm efficiency at the technical level but also needs to consider the operating environment and usage context of the system in practical applications.

4.2 Evaluating the Necessity of Facial Recognition Applications in Specific Scenarios

Conducting legitimacy and necessity assessments for FRT applications in specific scenarios. First, it is necessary to consider the balance between the potential benefits of the technology and the related risks. The application scenarios of facial recognition, including public safety, commercial marketing, and user identity authentication, each carry different legal and ethical considerations. In various scenarios, it is necessary to use the Scenario Analysis method to comprehensively analyze its commercial value and moral bottom line when evaluating its necessity.

4.3 Regularly Disclosing the Status of Facial Information Management and Providing Explanations

The Information Disclosure Analysis Method provides a framework for analyzing the effectiveness of information disclosure, thereby enhancing public trust in facial recognition by ensuring transparency in technology applications [9].

Actively fulfilling the obligation to explain and illustrate has become a key link in ensuring the compliance of information collection and processing. The obligation to explain and illustrate can effectively promote the transparency of facial information in public spaces, thereby enhancing the public's right to know about the application of facial recognition technology. For example, when collecting personal biometric information, relevant agencies should clearly inform the identified person in advance of the purpose, scope, and storage and processing methods of the information collection. This process not only helps to enhance public trust in technology applications but also provides users with the right to choose, allowing them to decide whether to authorize information use based on informed consent.

4.4 Data Processing Under Supervision

In the context of modern society, with the widespread application of FRT, the transparency of data processing and citizen supervision have become particularly important. To effectively protect citizens' privacy rights and data security, it is necessary to establish a comprehensive supervision mechanism. Using the SMEM (Supervisory Mechanism Evaluation Method) can effectively enhance the transparency of information processing, thereby ensuring compliance with relevant laws and regulations [10]. Establishing a clear and effective regulatory system is particularly important. On the one hand, a clear regulatory function can protect the public interest. By setting relevant legal frameworks and standards, it can ensure that the application of facial recognition technology does not infringe on individuals' basic rights. For example, on the basis of China's current PIPL, combined with specific provisions for facial recognition applications, it can promote the protection of personal data and ensure the legality and compliance of data processing.

In addition, establishing a regular inspection system for the application of facial recognition technology in public spaces is one of the important strategies to ensure the reasonable and compliant use of this emerging technology. Regular inspection systems can not only effectively prevent the abuse of facial recognition systems and potential ethical crises but also enhance public trust in technology supervision. According to relevant research, regular technical evaluation procedures can detect vulnerabilities in the system early, such as insufficient data storage security or algorithmic bias, thereby reducing the negative impact of technology on society.

5 Conclusion

Legal provisions such as the GDPR, which the international community has certain experience in, can provide useful references for relevant legislation. Drawing on advanced foreign legislative concepts and practical experience can more effectively protect citizens' privacy and reduce the risk of technology abuse. Therefore, relevant legislation should pay special attention to how to balance social public safety needs and individual privacy rights when clarifying the rights and obligations between data controllers and data subjects. At the same time, it is necessary to strengthen the qualification review and compliance review of information collectors to ensure that they follow the principles of necessity, legality, and minimum limitation when collecting facial recognition data, so as to achieve appropriate regulation of technology use.

Conflicts of Interest

The authors declare no conflicts of interest.

References

1. Wang, H. Y. (2022). Thoughts on the construction of a student-centered moral life in the activity field. School education(02), 94-96.
2. Jiang, Y. (2022). Legal regulation of abuse of relative advantage position. People's Judicature(10), 101-106.
3. Wang, F. (2022). The role of teachers in public spaces. School Administration(09), 03-04.
4. Eissa, G., & Lester, S. W. (2021). A Moral Disengagement Investigation of How and When Supervisor Psychological Entitlement Instigates Abusive Supervision. Journal of Business Ethics, 180(2).
5. Zhang, L. Y., Zhou, D. S., Liu, L. M., Liu, X. B., Yuan, T., Zhao, M., & Ren, K. (2023). Research on detection and recognition system of oil and gas pipeline weld seam based on machine vision technology.
6. Qiao, Y. D., Chen, D. K., Sun, Y. W., & Wang, H. Y. (2022). An intelligent color design method for visual communication design for public crisis. Color Research & Application, 48(1).
7. Olasov, I. (2022). Grandstanding: The Use and Abuse of Moral Talk. Essays in Philosophy, 23(1/2).
8. Liu, H. T., Li, Y. G., & Liu, D. C. (2021). Object detection and recognition system based on computer vision analysis. Journal of Physics: Conference Series, 1976(1).
9. Mell, I. (2021). Parks, COVID-19 and the impact of austerity funding on public-service provision in a time of crisis. The Town Planning Review, 92(2).
10. Wang, L. L., Satapathy, S. C., Agrawal, R., & García Díaz, V. (2021). Symbol recognition system based on 3D stereo vision. Journal of Intelligent & Fuzzy Systems, 40(4).

Biographies

1. **Xiufeng Zhang** Ph.D., associate professor and master's supervisor at Guangdong Polytechnic Normal University， director of the Three in One Education Construction Department of Guangdong Vocational Education Research and Guidance Center, and secretary general of Guangdong Vocational Education Guidance Committee.
2. **Xintong Lin** Guangdong Polytechnic Normal University，master of College of Marxism.

基於公共場域視覺識別系統濫用的倫理沖突以及規製探討

張秀峰　　林馨桐

摘要：在公共場域中視覺識別系統濫用現象頻發的背景下，通過初步梳理國內外在前沿技術倫理方面的研究現狀，了解到人臉識別技術潛在的隱私侵害風險以及對個人尊嚴的侵犯同樣不容忽視。研究表明，應用比例原則和基本權利規則對規範人臉識別技術的使用至關重要。從而提出了限製人臉信息收集與處理主體資格、明確使用目的、嚴格信息處理程序及建立監督機製的重要建議，旨在減少技術應用中的道德風險，提升公共信任，從而推動相應的立法進程和倫理框架的完善。

關鍵詞：人工智能；視覺識別；倫理；道德；公共區域