ISSN: 3008-1769

# The Game Between Intelligent Monitoring and Privacy in AI Policing

Ying Zhang*

Ih Zasag University, Law, Ulaanbaatar 14200, Mongolia

* Corresponding Author

## Abstract

**The fast development of artificial intelligence technology has pushed forward the intelligent transformation of police work. The artificial intelligence police system with intelligent surveillance at its core has had significant effects in areas like crime prevention and emergency handling. But its ability to collect a large amount of data and analyze behaviors has also caused wide disputes in terms of privacy protection. This article discusses the game relationship between intelligent surveillance and privacy rights in artificial intelligence policing from multiple aspects such as technology application, ethical conflicts, and legal regulations. It suggests building a balanced path through technological optimization, legal improvement, and public participation to offer theoretical support for the win-win situation of public security and individual rights.**

## Keywords

**Smart Surveillance, Privacy, AI.**

## 1. Introduction

In recent years, artificial intelligence (AI) policing has been rapidly implemented worldwide. For instance, in Suzhou's smart security community, an AI recognition system in elevators is used to intercept electric bicycles entering buildings in real time, effectively preventing fire hazards. In Nanjing, the police have achieved "second-level response" to emergencies through an AI collaboration platform, significantly enhancing the efficiency of law enforcement. These practices demonstrate that intelligent monitoring technology has become an important tool in public security governance.However, the unlimited infiltration of technology has also increased the risk of privacy violations: the high density of AI cameras in Macau's casinos makes tourists worry about the misuse of their behavior data, while smart locks in community surveillance chains might undermine trust in the community. Finding a balance between security and privacy has become a key issue in the development of AI policing.

## 2. The technical empowerment of intelligent monitoring and the improvement of public safety

### 2.1.Precision in crime prevention

Accurate AI monitoring for crime prevention uses deep learning algorithms to identify abnormal behaviors and predict risks. For example, combined with facial recognition technology, the system can quickly lock on to suspects and track their movements, significantly reducing the time it takes to solve a case. The practice of 5,097 smart security communities in Suzhou shows that the real-time perception of community disputes and safety hazards by AI devices has reduced the crime rate by more than 30%.

ISSN: 3008-1769

### 2.2.Intelligent reconstruction of police processes

AI technology has transformed the policing model from "reactive response" to "active defense". Through data sharing and instruction collaboration, the Nanjing Police Collaboration System improves the efficiency of case processing by 40% and reduces the problem of prevarication caused by information silos. In addition, the AI-driven simulation training system can generate hundreds of emergency scenarios to help police improve their combat capabilities in a virtual environment.

## 3. Ethical dilemmas and technical challenges of privacy erosion

### 3.1.Generalization and loss of control of data collection

The smart surveillance system collects personal privacy widely in the name of security, including facial features, personal behavior patterns, and even social information. Research shows that 70% of users lack the right to know how their data is used, and there's a widespread occurrence of collecting beyond what's necessary. For example, some public cameras record pedestrian conversations without clear notification, which is a serious invasion of communication privacy.

### 3.2.Algorithmic bias and social discrimination

AI model training data contains discrimination such as race and gender, which may cause systematic bias in monitoring results. In one city in the United States, a facial recognition system misjudged the probability of crime by an African-American group, which sparked mass protests. Such technical deficiencies not only weaken the credibility of law enforcement, but also exacerbate social inequality.

### 3.3.The suppression of the right to liberty by the normalization of surveillance

The AI sweep creates a "self-reflection effect." Gamblers in Macau avoid doing anything normal because they are afraid their actions will be recorded, which reflects the mock enforcement of technology on personal freedom. The surveillance from AI-driven smart locks highlights the distrust between neighbors, emphasizing the alienation in social relationships.

## 4. Balanced Path: Technical Regulation, Legal Improvement and Public Participation

### 4.1.Ethical embedding of technical optimization

Privacy design is a key reason for resolving conflicts. For example, when using federated learning technology for cross-institution data sharing, original data doesn't need to leave local systems, satisfying the needs of criminal analysis while also avoiding the risks of centralized storage. Additionally, techniques like data anonymization and dynamic de-identification can be employed to ensure that personal identity information cannot be traced during the analysis process.

### 4.2.Dynamic adaptation of the legal framework

The existing laws should respond to technological changes: clarify the boundaries of data collection, refer to the EU's AI Act, and stipulate that monitoring systems only collect "the minimum necessary data," while also setting a storage time limit; build mechanisms for algorithm accountability, require the disclosure of the training datasets and decision logic of AI models, and accept audits by third parties; enhance pathways for infringement remedies, drawing from China's Personal Information Protection Law, granting individuals the right to delete data and the right to object to reduce the cost of protecting their rights.

ISSN: 3008-1769

### 4.3.A co-governance model with public participation

Build a platform for multi-party discussions that brings public opinions into tech deployment decisions. For example, a city in the UK used a citizens' jury to review the installation of surveillance cameras and ultimately passed a compromise plan to limit night vision features after getting 80% support. Plus, strengthening privacy education can raise public awareness of digital rights, which helps create a network for social oversight against tech abuse.

## 5. Conclusion

In AI policing, smart surveillance serves as a "guardian" of public safety but can also turn into a "grave digger" for privacy rights. The hidden ethical risks behind technological neutrality push us to move beyond a purely efficiency-driven mindset towards a governance model that is more human-centered. Future research needs to further explore the application of blockchain technology in data traceability and the compliant flow mechanisms of cross-border surveillance data, ultimately achieving a dialectical unity of security and privacy.

## Acknowledgements

Ih Zasag University.

## References

[1] Chen Ma:Reflections on Big Data Investigation and Citizens' Privacy Protection from the Perspective of Game Theory (Science and technology information, China 2001), p.20-23.

[2] LiPing Wang:Privacy regulation in the context of artificial intelligence(Network security technology and application, China 2022), p.124-126.

[3] Xiu Zhang:Discussion on the ethical principles of harm minimization from the perspective of intelligent communication(Contemporary Communication, China 2020), p.82-84.

[4] https://cloud.baidu.com/article/3324979