福建省中电海峡智能装备研究院
Fujian Zhongdian Straits Institute of Intelligent Equipment

Asia Pacific Science Press

Advances in Management and Intelligent Technologies
ISSN(O):3079-5869
ISSN(P):3079-5850
Vol. 1 No.4 (2025)

The Integration of Artificial Intelligence into Smart Policing Systems: Applications and Risk Governance

Yun Pei*

Emilio Aguinaldo College (EAC), 006302, Manila, Philippines

Corresponding author: Yun Pei, 125354624@qq.com

Abstract: With the rapid advancement of artificial intelligence (AI), smart policing has emerged as a strategic priority in the modernization of public security systems. AI technologies such as facial recognition, video surveillance, big data analytics, and intelligent command systems have significantly enhanced the operational efficiency and precision of law enforcement. However, these technological gains are accompanied by structural risks, including data misuse, privacy violations, algorithmic bias, expanded police authority, and erosion of procedural justice. This paper reviews the current applications and development trends of AI in smart policing and critically examines the legal and ethical risks arising from such integration. It proposes a multi-dimensional governance framework comprising legal regulation, algorithm oversight, public accountability, and ethical training. The study argues that a balance between efficiency, safety, and fairness is essential for sustainable smart policing. Moving forward, it is imperative to synchronize AI governance with policing practices and promote international cooperation to establish unified standards for data protection and AI ethics.

Keywords: Smart Policing; Artificial Intelligence; Data Governance; Algorithmic Bias; Rule of Law Risk

Published: Aug 6, 2025

DOI:https://doi.org/10.62177/amit.v1i4.486

1.Introduction

Artificial Intelligence (AI), as a central force of the Fourth Industrial Revolution, is rapidly transforming industries and public administration alike. Technologies such as big data analytics, deep learning, computer vision, and natural language processing are moving beyond the laboratory to become integral tools in the governance of modern societies. Among various domains, the field of public security has emerged as one of the most prominent arenas for AI deployment. In China, the Ministry of Public Security has actively promoted the construction of "smart policing" systems supported by AI, cloud computing, and integrated data platforms, aiming to enhance operational efficiency and modernize governance structures.

Smart policing refers to the comprehensive integration of AI, the Internet of Things (IoT), and advanced information systems into law enforcement activities. It emphasizes data-driven decision-making, risk forecasting, and proactive intervention, marking a significant shift from traditional models of policing based on manpower, physical infrastructure, and basic surveillance. With guidance from policy documents such as the National Guidelines for Smart Policing Development and The Framework for Big Data and AI Integration in Public Security, local police departments across China have implemented AI-driven platforms for facial recognition, predictive policing, and emergency response coordination. These efforts are reshaping how crime is monitored, analyzed, and managed.

However, the rise of AI in policing is not without profound legal and societal implications. The large-scale collection and processing of personal data, often conducted without clear boundaries or informed consent, risk infringing on individuals' rights to privacy and autonomy. Moreover, AI algorithms—frequently trained on biased or incomplete datasets—may reproduce or even amplify discriminatory patterns in decision-making, leading to disproportionate scrutiny of certain demographic groups. The "black box" nature of algorithmic systems also challenges traditional principles of administrative accountability and procedural transparency, making it difficult for the public to understand or contest decisions made by machines.

In this context, the integration of AI into policing raises urgent questions about how to balance technological efficiency with legal legitimacy and ethical integrity. This paper aims to analyze the current development and practical applications of AI in smart policing, identify the core risks that accompany its implementation, and propose a set of governance mechanisms to mitigate these risks. By addressing both the potentials and pitfalls of AI-driven law enforcement, this study contributes to the broader discourse on responsible innovation and the future of public safety governance in the digital age.

2.Literature Review

2.1 International Research Landscape

The integration of artificial intelligence into law enforcement has become a central topic in interdisciplinary research across law, computer science, public administration, and ethics. Early studies predominantly focused on the functional value of AI tools in policing. For example, Perry et al. (2013) introduced the concept of predictive policing, which uses historical crime data and statistical models to anticipate future criminal activity and allocate police resources more efficiently. Over time, however, attention has shifted toward the risks and ethical dilemmas embedded in algorithmic systems.

Legal scholars and civil society advocates have raised concerns about the inherent biases in algorithmic policing tools. Ferguson (2017), for instance, argues that predictive algorithms often reinforce systemic inequalities, particularly when trained on biased datasets that disproportionately reflect minority communities. Pasquale (2015) emphasized the risks of opacity in algorithmic decision-making, warning that black-box systems can undermine democratic oversight and due process.

In response, the European Union has proposed regulatory initiatives such as the draft Artificial Intelligence Act, which aims to impose stricter controls on high-risk AI applications, including those used in law enforcement. These frameworks emphasize principles like transparency, human oversight, and proportionality. In the United States, while the adoption of AI policing tools is widespread, critical discourse continues to highlight the need for external audits, public accountability, and ethical AI design.

Overall, international scholarship has developed a robust critique of AI in policing, focusing on data ethics, algorithmic governance, and the protection of civil liberties. These insights provide valuable references for developing normative frameworks suitable to China's sociopolitical and legal context.

2.2 Domestic Research Developments in China

In recent years, Chinese scholars have increasingly turned their attention to the intersection of AI and public security, particularly in the context of smart city development and police modernization. Current domestic research can be broadly divided into three thematic areas:

First, studies focusing on the construction of smart policing systems emphasize the technical and organizational transformation of policing. Scholars such as Wang Dawei (2019) propose that smart policing should rely on a closed-loop operational model of "perception–analysis–command–action–feedback," underpinned by big data and integrated platforms. These studies primarily adopt a problem-solving perspective, aiming to improve the efficiency and responsiveness of police operations.

Second, research on the application of AI technologies in police work explores the deployment of facial recognition, video surveillance, natural language processing, and big data analytics. Scholars such as Li Zhenxing (2020) analyze the strengths and limitations of AI tools in assisting criminal investigations, pointing to both efficiency gains and potential overreliance on machine judgment.

Third, an emerging body of literature examines the legal and ethical implications of AI policing. Chen Ruihua (2021) has argued that the deployment of AI in law enforcement must operate within the constraints of China's Constitution, Criminal Procedure Law, and Personal Information Protection Law. Other scholars have drawn attention to the procedural risks posed by automated decision-making systems and called for the codification of boundaries for data collection and algorithmic processing by police.

While domestic scholarship provides a valuable foundation for understanding AI in policing, much of it remains focused on technical feasibility and administrative implementation. There is still a notable gap in research addressing deeper issues such as algorithmic accountability, rights-based governance, and public trust.

2.3 Synthesis and Research Gaps

In sum, both international and domestic studies recognize the transformative potential of AI in public security while emphasizing the need for caution and normative safeguards. International literature offers more mature reflections on algorithmic fairness, human rights, and regulatory innovation. In contrast, Chinese research tends to prioritize system-building and practical applications, often under the guidance of state policy.

This paper seeks to bridge this gap by combining technological insight with legal reasoning. It adopts a problem-oriented perspective to examine how AI tools are reshaping policing practices in China and how associated risks—such as data overreach, discrimination, and procedural opacity—can be effectively mitigated through law and governance. The ultimate goal is to contribute to a model of smart policing that aligns with both public safety objectives and constitutional principles.

3.Research Methodology

This study adopts a multi-method approach that integrates legal analysis, policy evaluation, and empirical case review to examine the application of artificial intelligence in China's smart policing systems and explore its associated risks. The goal is to develop a structured and normative framework that addresses both technological benefits and legal challenges in a balanced manner. The specific research methods employed are as follows:

3.1 Literature Review and Normative Analysis

A comprehensive literature review was conducted to establish the theoretical foundation of the study. This included both international and domestic academic publications, government reports, policy guidelines, and legal commentaries. Particular attention was paid to studies concerning algorithmic regulation, data governance, law enforcement ethics, and public administration.

Through normative analysis, the study interprets relevant laws such as the Constitution of the People's Republic of China, Criminal Procedure Law, Personal Information Protection Law, and Data Security Law. This legal framework was evaluated to determine its adequacy in regulating AI applications in policing and to identify areas where legal reforms or institutional innovations are needed.

3.2 Case Study Method

To capture the practical realities of AI in policing, the study utilizes case studies of specific AI-powered law enforcement systems and initiatives in China. These include, for example, the implementation of facial recognition in urban surveillance networks, predictive policing platforms used in high-risk districts, and risk-scoring systems designed to categorize individuals based on behavioral data.

Each case was examined with regard to its technical architecture, operational logic, and socio-legal implications. This method enabled a grounded analysis of how AI tools affect policing practices and how potential overreach or misuse may occur in the absence of proper regulatory safeguards.

3.3 Comparative Analysis

A comparative dimension was introduced to contextualize China's experience with global developments. Policing AI systems and regulatory responses in the United States, the European Union, and selected Asian jurisdictions were examined to highlight different governance strategies. Particular emphasis was placed on algorithmic accountability, public oversight mechanisms, and rights-based frameworks.

The goal of this comparison is to extract valuable lessons that can inform the development of China's AI policing governance model, while recognizing the unique institutional, cultural, and political factors that shape domestic policy choices.

3.4 Problem-Oriented and Governance-Focused Approach

This study adopts a problem-oriented approach that prioritizes the identification and resolution of key risks associated with AI policing—namely, privacy infringement, algorithmic bias, procedural opacity, and the expansion of police powers. Rather than focusing solely on technical capabilities, the research emphasizes governance challenges and legal design.

By situating AI policing within the broader framework of public law and administrative ethics, the study aims to offer governance-oriented solutions that can balance efficiency with accountability and safeguard the foundational principles of due process and human dignity.

4.The Role of AI in Smart Policing: Applications and Development Trends

The integration of artificial intelligence into public security has reshaped the landscape of policing in both operational and strategic dimensions. As AI technologies become increasingly embedded in law enforcement, their applications now span surveillance, data analysis, criminal investigations, risk forecasting, and decision-making. This section provides an overview of the core concepts behind smart policing and outlines key AI-driven applications, followed by a comparative assessment of domestic and international development trajectories.

4.1 Conceptualizing Smart Policing

Smart policing refers to a data-driven and technology-enabled model of public security management that leverages AI, the Internet of Things (IoT), big data platforms, and cloud computing. Its objective is to improve crime prevention, resource allocation, and real-time responsiveness by automating detection, enhancing prediction, and supporting decision-making processes.

Unlike traditional policing models that rely heavily on manpower and reactive strategies, smart policing emphasizes precision, proactivity, and integration. It creates a dynamic feedback loop encompassing intelligent sensing, algorithmic analysis, automated command, and digitalized execution. This model is particularly well-suited to address complex urban security challenges, such as organized crime, cyber threats, and mass emergencies.

4.2 Core Applications of AI in Policing

4.2.1 Intelligent Video Surveillance and Facial Recognition

AI-enhanced video surveillance systems are capable of automatically detecting individuals, vehicles, and suspicious behaviors through real-time image processing and pattern recognition. Facial recognition is a cornerstone technology that enables rapid identity verification, suspect tracking, and alert generation. Deployed across transport hubs, business districts, and residential areas, these systems significantly improve the speed and precision of law enforcement.

However, widespread deployment of such systems also triggers concerns about privacy erosion and mass surveillance. Without strict legal boundaries and public accountability, facial recognition may become a tool of intrusive state control rather than legitimate crime prevention.

4.2.2 Big Data Analytics and Predictive Policing

Predictive policing involves the use of statistical models and machine learning algorithms to analyze historical crime data, spatial patterns, and behavioral indicators. These insights are used to forecast potential criminal incidents and inform the allocation of patrol units and resources. In practice, some jurisdictions in China have implemented AI-powered platforms to assess the risk levels of individuals and neighborhoods based on diverse datasets.

While predictive models can enhance efficiency and reduce crime rates, they risk reinforcing existing social biases, especially if trained on discriminatory or incomplete data. Predictive policing can also lead to over-surveillance of marginalized communities, raising ethical and legal concerns.

4.2.3 Natural Language Processing and Case Assistance Systems

AI-driven voice recognition and semantic analysis technologies are increasingly used in the collection, transcription, and categorization of investigative records. Law enforcement officers can use AI systems to generate electronic case files, organize evidence, and detect inconsistencies in testimonies. These tools reduce repetitive manual work and improve procedural consistency.

Advanced language models can also assist in interpreting interrogations, detecting emotional cues, and evaluating credibility, although the accuracy and fairness of such interpretations remain under scrutiny.

4.2.4 Smart Patrol Robots and Command Platforms

In densely populated public areas such as airports, train stations, and commercial centers, patrol robots equipped with thermal sensors, biometric scanners, and voice interaction modules are deployed to monitor security risks and interact with civilians. At the command level, AI-enabled platforms aggregate real-time data feeds to assist with emergency response, dispatch coordination, and resource optimization.

These systems enable law enforcement agencies to operate with greater flexibility and responsiveness. However, their reliance on algorithmic decision-making introduces new challenges related to transparency, accountability, and due process.

4.3 Comparative Development Trends: China vs. Western Countries

4.3.1 China: Operational Efficiency and System Integration

China's approach to smart policing is characterized by strong government leadership, centralized coordination, and a focus on operational outcomes. Initiatives such as the "Sharp Eyes Project," the "Snow Bright System," and the "Integrated Command Platforms" exemplify the country's ambition to create seamless, multi-layered security infrastructures. These efforts emphasize real-time surveillance, centralized databases, and interdepartmental data fusion to support rapid response and precision governance.

China's smart policing development is closely tied to its broader strategy of digital state-building, where technological tools serve as instruments for social control, stability maintenance, and crime deterrence.

4.3.2 United States and Europe: Emphasis on Rights and Regulation

In contrast, Western countries have adopted a more cautious and rights-oriented approach. In the United States, predictive policing systems like PredPol have faced criticism for algorithmic bias and racial profiling, leading to their suspension or discontinuation in several cities. Civil society organizations and legal scholars have advocated for stronger oversight, transparency mandates, and public engagement.

The European Union has taken a regulatory-first stance, proposing the Artificial Intelligence Act, which imposes strict requirements on high-risk AI systems, including those used in law enforcement. These regulations mandate human oversight, risk assessments, and justification protocols, ensuring that AI applications do not undermine fundamental rights and democratic values.

This chapter demonstrates that while AI has become a transformative force in policing, its application must be guided by context-specific norms and institutional safeguards. China's emphasis on integration and efficiency contrasts with the rights-based, regulatory frameworks emerging in the West. Both models offer insights—and cautionary lessons—for the responsible evolution of smart policing worldwide.

5.Risk Assessment: Legal, Technical, and Ethical Challenges of AI Policing

While the integration of artificial intelligence into smart policing systems brings about substantial benefits in efficiency, precision, and responsiveness, it also introduces profound risks that can compromise individual rights, erode public trust, and challenge the foundations of rule-based governance. These risks are not incidental, but structural in nature—arising from the very logic of data-centric, algorithm-driven systems. This section provides a comprehensive analysis of the key challenges associated with AI policing, categorized into four major domains: data governance, algorithmic bias, procedural justice, and the expansion of police power.

5.1 Data Security and Privacy Infringement

5.1.1 Ambiguity in Data Collection and Use

One of the most pressing concerns is the extensive collection of personal information without clear legal boundaries or sufficient public awareness. AI-powered policing systems routinely harvest biometric data, movement patterns, digital communication records, and behavioral profiles. In many cases, this is done without informed consent or judicial oversight, which violates core principles of necessity, proportionality, and legality.

The lack of clarity in how data is obtained, processed, and stored creates significant potential for misuse. When surveillance becomes ubiquitous and unregulated, it risks transforming public spaces into zones of constant observation, undermining citizens' sense of autonomy and anonymity.

5.1.2 Vulnerability to Data Breaches and Cyber Attacks

The technical infrastructure of smart policing systems—often reliant on centralized databases and cloud platforms—poses serious cybersecurity risks. Without robust protections, these systems become attractive targets for malicious actors. Data leaks involving sensitive personal information can not only harm individual rights but also severely damage the credibility of law enforcement agencies.

Recent high-profile incidents of alleged data leaks from public security networks have underscored the urgent need to upgrade security protocols, strengthen data encryption, and impose strict access controls within policing systems.

5.2 Algorithmic Bias and Discriminatory Decision-Making

5.2.1 Inherited Bias from Historical Training Data

AI systems do not operate in a vacuum. Their performance depends on the quality and representativeness of the data they are trained on. In policing, historical data often reflects pre-existing social inequalities, racial profiling, or enforcement patterns skewed toward specific communities. When fed into predictive models, these biases are reproduced and amplified, perpetuating cycles of over-policing and stigmatization.

Such algorithmic bias is particularly dangerous because it can appear neutral and objective, cloaked in the legitimacy of data science, while in fact reinforcing structural injustice.

5.2.2 Lack of Transparency and Accountability in Algorithmic Decisions

The opaque nature of many AI models—commonly referred to as the "black box" problem—presents a significant barrier to accountability. Law enforcement officers and affected individuals often lack the means to understand how AI systems arrive at their conclusions. Without explainability, it becomes difficult to question, appeal, or audit AI-generated decisions, undermining both administrative fairness and legal due process.

This lack of transparency also weakens public oversight, as civil society, media, and legal institutions are unable to meaningfully scrutinize the use and impact of algorithmic tools in policing.

5.3 Challenges to Procedural Legitimacy and Rule of Law

5.3.1 Legality of Evidence Collection via AI Technologies

When AI systems are used to collect evidence—such as through facial recognition, license plate tracking, or digital footprint analysis—it raises serious questions about the legality and admissibility of such evidence in judicial proceedings. If data is acquired without proper authorization, procedural safeguards, or judicial warrants, it may be deemed inadmissible and could violate the rights of the accused.

The absence of standardized protocols for AI-assisted evidence collection risks creating a gray area where technologically enabled surveillance circumvents existing legal requirements.

5.3.2 Over-Reliance on Technology and the Erosion of Human Judgment

Another concern is the growing dependence of law enforcement officers on automated systems. While AI can support decision-making, it should not replace human judgment, especially in complex or ambiguous cases. The "automation bias"—a cognitive tendency to over-trust machine outputs—can lead to uncritical acceptance of flawed recommendations and diminish the role of discretion, empathy, and contextual understanding in policing.

The delegation of authority from humans to machines, without adequate checks and balances, risks hollowing out the procedural protections that form the cornerstone of a fair and just legal system.

5.4 Blurring Boundaries of Police Power and Public Trust Deficit

5.4.1 Expansion of Surveillance Powers Without Legal Mandate

AI technologies have the potential to significantly expand the reach of police authority, often without corresponding updates in legal frameworks. For instance, behavior-tracking algorithms, cross-platform data integration, and real-time profiling tools can be used to create "risk lists" or monitor individuals without their knowledge or consent. When such practices are deployed without explicit legal authorization, they amount to a de facto expansion of state power, eroding the principle of legality and the democratic accountability of law enforcement.

This uncontrolled expansion poses long-term threats to civil liberties and can foster a culture of pre-emptive policing that undermines the presumption of innocence.

5.4.2 Legally Permissible but Substantively Unjust Practices

Even when technically legal, certain AI-enabled practices may violate the spirit of fairness, equality, and nondiscrimination. Systems that automatically categorize individuals based on data-driven assumptions—such as predicting future criminality based on socioeconomic status or past associations—can result in discriminatory treatment without due cause.

Such practices reveal a troubling gap between formal legality and substantive justice. They highlight the risk of relying on “technologically rational” but socially harmful solutions that undermine public confidence in law enforcement institutions.

In summary, the adoption of AI in policing brings forth a dual-edged transformation. On one hand, it enhances the capability and responsiveness of law enforcement. On the other, it introduces systemic vulnerabilities that, if left unaddressed, may compromise the very principles of legality, accountability, and justice that underpin the rule of law. Effective governance of AI policing must therefore begin with a clear-eyed understanding of these risks—and a commitment to mitigating them through robust institutional design.

6.Suggestion For Institutional Pathways for Risk Governance in AI-Driven Policing

Addressing the risks associated with artificial intelligence in policing requires more than technical refinements—it demands the construction of a robust, multi-dimensional governance framework. Such a framework must align technological innovation with the principles of legality, accountability, transparency, and human dignity. This section outlines institutional strategies across four key dimensions: legal regulation, algorithmic oversight, participatory accountability, and ethical capacity-building (European Commission, 2021).

6.1 Strengthening Legal and Regulatory Foundations

6.1.1 Enacting Specialized Legislation or Technical Guidelines

Currently, China lacks a comprehensive legal framework specifically tailored to the governance of AI in law enforcement. Although general laws such as the Criminal Procedure Law, Data Security Law, and Personal Information Protection Law provide partial coverage, they do not adequately address the complex challenges posed by AI applications in policing.

To close this regulatory gap, there is a pressing need to develop either specialized legislation or authoritative technical guidelines that clearly delineate the scope, procedures, and limits of AI use in policing. Such instruments should define permissible use cases, establish approval and review processes for high-risk systems, and require ongoing evaluation of their legal compliance and social impact.

6.1.2 Clarifying the Boundaries of Data Collection, Use, and Sharing

A central element of effective governance is the clear articulation of boundaries for data processing activities. Legal instruments should enforce the principle of “minimum necessary use,” limit the scope of personal data collected, and impose strict conditions on data sharing across agencies or platforms.

Furthermore, citizens should be granted enforceable rights to access, correct, and delete their personal data held within policing systems. These measures will help shift AI policing away from opaque mass surveillance models and toward a more transparent, accountable, and rights-respecting paradigm.

6.2 Enhancing Algorithmic Oversight and Technical Safeguards

6.2.1 Establishing Mechanisms for Algorithmic Explainability and Auditing

To address the “black box” nature of AI systems, institutions must implement algorithmic explainability requirements, especially for high-stakes applications such as facial recognition, risk scoring, and predictive policing. These requirements should include:

- Mandatory documentation of model logic and training datasets
- Ex ante testing of algorithmic fairness, accuracy, and bias
- Development of user-friendly interfaces that allow officers and affected individuals to understand system outputs
- Logging of decision-making trails for retrospective auditing

Transparent algorithms are not only more accountable but also foster public trust and reduce the risk of unlawful outcomes.

6.2.2 Introducing Independent Audits and Ethical Review Procedures

Technical safeguards alone are insufficient without institutional checks. Independent third-party audits and ethical review boards should be established to evaluate AI policing tools before and after deployment. These bodies—comprising legal experts, technologists, civil society representatives, and ethicists—should assess the necessity, proportionality, and societal impact of proposed systems.

Such procedures can prevent function creep, identify unintended consequences, and offer an external check on internal police decision-making processes, thereby improving legitimacy and governance quality.

6.3 Fostering Multi-Stakeholder Participation and Accountability

6.3.1 Expanding the Right to Know and Appeal

AI policing systems must be subject to mechanisms that ensure public transparency. Authorities should disclose:

- The types of AI systems in use
- The purposes of their deployment
- The categories of data collected
- The decision-making criteria applied

Moreover, individuals should be able to file appeals if they believe they have been unfairly targeted or misclassified by an AI system. Establishing administrative complaint channels, legal remedies, and public reporting systems will strengthen citizen oversight and institutional integrity.

6.3.2 Appointing Independent Data Protection Officers

Drawing inspiration from the European Union’s General Data Protection Regulation (GDPR), Chinese law enforcement institutions could benefit from appointing dedicated Data Protection Officers (DPOs). These officers, independent of operational command structures, would be tasked with:

- Monitoring data processing compliance
- Evaluating algorithmic systems for risk and fairness
- Coordinating responses to public complaints and data breaches
- Liaising with external regulators and oversight bodies

Institutionalizing this role would create a firewall between technological ambition and regulatory responsibility.

6.4 Promoting Ethical Awareness and Human-Centered Training

6.4.1 Building AI Literacy Among Law Enforcement Personnel

The misuse of AI systems is often rooted not in malice, but in misunderstanding. As such, police officers must be trained not only in how to operate AI tools but also in how to interpret their outputs critically. Training programs should emphasize:

- The limitations and uncertainties of AI recommendations
- The importance of corroborating automated outputs with contextual analysis
- The legal responsibilities attached to AI-assisted decisions
- Recognizing and mitigating automation bias

A more informed law enforcement community is key to responsible AI adoption.

6.4.2 Integrating Ethical Reasoning and Public Values

AI systems are not value-neutral. Their use in public security must reflect ethical considerations such as dignity, fairness, and non-discrimination. Accordingly, police ethics education should include modules on digital ethics, algorithmic justice, and human rights.

Moreover, the institutional culture of law enforcement should shift from “techno-centrism” to “human-centered governance,” where technological tools serve—not substitute—principled judgment and community trust.

In conclusion, effective governance of AI in policing requires a comprehensive institutional design that blends legal authority with social legitimacy and ethical responsibility. Only through a holistic approach can the state fully harness the benefits of intelligent law enforcement while safeguarding the foundational values of justice, accountability, and public trust.

7.Conclusion and Future Prospects

7.1 Summary of Key Findings

Artificial intelligence has emerged as a transformative force in the modernization of policing, offering powerful tools to enhance surveillance, improve decision-making, and optimize public safety operations. Through facial recognition, predictive analytics, and intelligent coordination systems, AI has significantly expanded the capabilities of law enforcement agencies.

However, the study finds that this transformation is accompanied by profound legal, technical, and ethical risks. These include violations of privacy rights, algorithmic discrimination, lack of procedural safeguards, and the unchecked expansion of police power. Crucially, these are not marginal issues—they stem from the structural logic of data-driven governance and must be addressed through a coherent and principled framework.

This paper proposes a multi-dimensional governance strategy that includes:

- Establishing specialized legal and regulatory frameworks for AI in policing
- Requiring algorithmic transparency and independent oversight
- Enabling public participation and rights-based remedies
- Promoting ethical reasoning and responsible use of technology within law enforcement

Only by aligning smart policing with the foundational principles of legality, fairness, and public accountability can the benefits of AI be fully realized without compromising civil liberties.

7.2 Future Prospects

7.2.1 Synchronizing AI Governance with Policing Practice

The future of AI in law enforcement hinges on the ability to integrate advanced technology with institutional safeguards. China must accelerate the development of a coherent AI governance regime that addresses the specific challenges posed by policing applications. This requires collaboration across legislative bodies, law enforcement agencies, technologists, ethicists, and civil society actors.

Smart policing should be seen not merely as a technological project but as a governance challenge. Embedding algorithmic accountability, data transparency, and human rights protections into the design and operation of AI systems will ensure that technology remains a tool for justice—not a threat to it.

7.2.2 Promoting International Norms and Cross-Border Collaboration

As AI technologies transcend national boundaries, so too must the regulatory and ethical frameworks that govern them. China should actively engage in international dialogue and help shape global standards for responsible AI use in public security. This includes participating in the development of shared ethical codes, cross-border data governance protocols, and multilateral accountability mechanisms.

In the long term, international cooperation will be vital to addressing issues such as surveillance overreach, AI-driven discrimination, and cyber vulnerabilities. Global consensus on these matters will contribute to a more secure, just, and trustworthy digital order.

7.3 Final Remarks

The rise of artificial intelligence in policing presents both opportunity and peril. If used responsibly, AI can revolutionize public safety, strengthen rule-of-law institutions, and enhance trust between the state and society. If misused or left unregulated, it can erode rights, entrench inequality, and undermine democratic governance.

The task ahead is to ensure that AI serves not only the goal of efficient policing but also the higher ideals of justice, transparency, and human dignity. Through deliberate policy choices and thoughtful institutional design, societies can shape the future of AI-driven policing in ways that are both innovative and just.

Funding

no

Conflict of Interests

The authors declare that there is no conflict of interest regarding the publication of this paper.

Reference

[1] Perry, W. L., McInnis, B., Price, C. C., Smith, S. C., & Hollywood, J. S. (2013). Predictive policing: The role of crime forecasting in law enforcement operations. RAND Corporation. https://doi.org/10.7249/RR233

[2] Ferguson, A. G. (2017). *The rise of big data policing: Surveillance, race, and the future of law enforcement*. NYU Press. https://doi.org/10.18574/nyu/9781479892822.001.0001

[3] Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press.

[4] Wang, D. (2019). The basic logic and institutional construction of smart policing. Public Security Studies, 36(2), 10–16.

[5] Li, Z. (2020). Mechanism and risk prevention in AI-assisted criminal investigation. *Journal of Police College*, 38(4), 47–55.

[6] Chen, R. (2021). Technological governance and procedural justice: Normative pathways for AI intervention in criminal justice. Chinese Journal of Law, 43(5), 3–21.

[7] European Commission. (2021). Proposal for a regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206