

The Impact of Digital Surveillance and Artificial Intelligence on Modern Policing: Ethical, Legal, and Criminal Justice Implications

Kwadwo Sarpong¹, Micheal Abimbola Oladosu^{2*} and Moses Adondua Abah³

¹Department of Communication, Eastern New Mexico University, Portales, New Mexico, USA.

²Department of Chemical Sciences, Faculty of Science, Anchor University, Lagos, Nigeria.

³Department of Biochemistry, Faculty of Pure and Applied Sciences, Federal University of Wukari, Wukari, Taraba State, Nigeria

Abstract

Background: The convergence of digital surveillance technologies and artificial intelligence (AI) has fundamentally transformed law enforcement practice in the twenty-first century. Facial recognition technology, predictive policing algorithms, automated licence plate recognition, and AI-enhanced body-worn camera systems are now routinely deployed by police agencies worldwide.

Objective: This review critically examines the ethical, legal, and criminal justice implications of these technologies, drawing on peer-reviewed scholarship, regulatory documents, and empirical evidence published between 2020 and 2025.

Methods: A structured narrative review was conducted, synthesising evidence from criminology, law, computer science, and public policy.

Results: Evidence consistently demonstrates that AI policing tools offer efficiency gains but simultaneously reproduce and amplify racial bias embedded in historical crime data. Legal frameworks lag behind technological deployment, creating accountability gaps. The EU AI Act (2024) represents the most comprehensive regulatory response to date, while the United States retains a fragmented patchwork of state-level policies.

Conclusion: Responsible integration of AI into policing requires binding transparency obligations, independent algorithmic auditing, human-in-the-loop decision requirements, and robust community oversight to safeguard due process, equality, and civil liberties, and providing a prospective outlook on the advancement of construction materials in influencing sustainable, adaptive, and intelligent built environments.

Keywords: artificial intelligence; digital surveillance; facial recognition; predictive policing; criminal justice; algorithmic bias; body-worn cameras; EU AI Act; law enforcement ethics; data privacy

INTRODUCTION

Digital surveillance technologies and artificial intelligence (AI) have rapidly permeated contemporary law enforcement, promising enhanced operational efficiency, faster case resolution, and more objective decision-making. Law enforcement agencies in the United States, European Union, United Kingdom, Canada, and Australia now routinely deploy facial recognition technology (FRT), predictive policing algorithms (PPAs), automated licence plate recognition (ALPR), social media analytical

tools, and AI-assisted body-worn camera (BWC) systems [1–3]. These technologies collectively form an emergent surveillance architecture that fundamentally restructures police–community relations, evidentiary standards, and the procedural rights of suspects and defendants.

Corresponding Author: Micheal Abimbola Oladosu
Department of Chemical Sciences, Anchor University of
Lagos, Lagos, Nigeria

Despite their promise, these systems carry profound risks. Empirical research has documented that FRT algorithms produce significantly higher error rates for women and individuals with darker skin tones, raising the prospect of wrongful arrests grounded in biometric misidentification [4,5]. Predictive policing systems, trained on historically biased arrest data, systematically redirect police resources to communities of colour, perpetuating cycles of over-policing and socioeconomic disadvantage [6,7]. Meanwhile, the legal frameworks governing these technologies remain fragmented, outdated, or, in many jurisdictions, absent. The result is a regulatory vacuum in which significant coercive power is exercised on the basis of opaque algorithms without meaningful accountability [8,9].

This review paper examines the technological landscape of AI-driven surveillance in policing, the ethical tensions these tools create, the evolving legal responses across major jurisdictions, and the implications for criminal justice outcomes. The paper adopts a multidisciplinary perspective, drawing on criminology, legal scholarship, computer science, and human rights discourse. Three analytical tables and three conceptual figures complement the textual analysis. The overarching aim is to provide researchers, policymakers, and practitioners with a rigorous, evidence-based synthesis that can guide responsible AI governance in public safety contexts.

THE TECHNOLOGICAL LANDSCAPE OF AI IN MODERN POLICING

Facial Recognition Technology

Facial recognition technology constitutes one of the most consequential and contested AI tools in contemporary law enforcement. FRT systems analyse geometric and textural features of facial images, comparing them against databases containing millions of photographs drawn from arrest records, driver's licences, social media, and other sources [4]. Platforms such as Clearview AI, which has scraped over 50 billion images from public internet sources, have been adopted by hundreds of law enforcement agencies despite unresolved questions about legality and consent [5].

The performance characteristics of FRT vary substantially across demographic groups. The U.S. Government Accountability Office (GAO) reported in 2024 that several federal agencies deployed FRT without adequate civil rights policies or staff training [3]. Academic and governmental reviews have identified that state-of-the-art FRT systems exhibit error rates disproportionately elevated for Black women compared with White men, an artefact of non-representative training datasets. Such demographic differentials carry direct consequences in operational policing: erroneous FRT matches have been documented as the proximate cause of wrongful arrests, illustrating the real-world harm of deploying technically immature biometric tools in high-stakes investigative contexts [4]. Table 1 provides a comparative overview of the principal AI and digital surveillance tools currently deployed in policing, including their intended applications, operational benefits, and documented concerns, whereas Figure 1 presents the Growth in law enforcement FRT adoption across five major jurisdictions (2018–2024).

Table 1. *AI and Digital Surveillance Tools in Modern Policing: Applications, Benefits, and Concerns*

AI/Digital Tool	Application in Policing	Benefit	Key Concern
Facial Recognition Technology (FRT)	Suspect identification from CCTV/databases	Rapid cross-referencing of billions of images	Racial bias; wrongful arrests
Predictive Policing Algorithms (PPA)	Crime hotspot prediction; risk scoring	Efficient resource allocation	Perpetuates racial over-policing
Body-Worn Cameras (BWC) with AI	Behavioural monitoring; evidence capture	Enhanced accountability & transparency	Data volume; privacy; officer acceptance
Automated Licence Plate Recognition (ALPR)	Vehicle tracking; outstanding warrant checks	Real-time vehicle identification	Mass surveillance; data retention
Social Media Surveillance AI	Threat detection; gang network mapping	Early intervention capability	Free speech: chilling effect
ShotSpotter / Acoustic Detection	Gunshot detection and patrol dispatch	Faster emergency response	Inaccuracies: over-policing minority areas

Source: *Compiled by the authors based on references [1,3,4,5,8,11,12,14].*

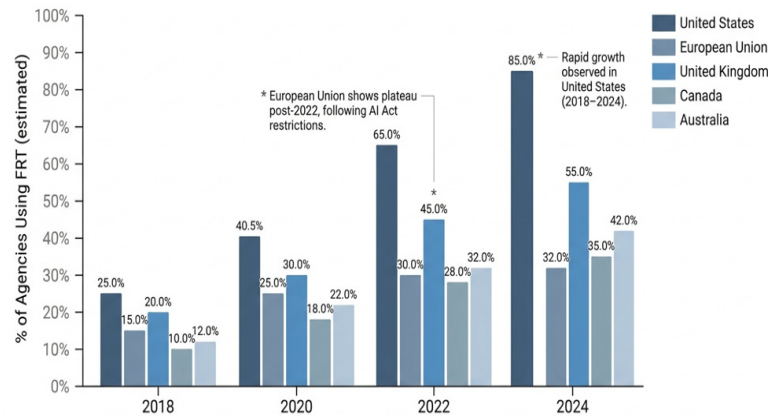


Fig 1. Growth in law enforcement FRT adoption across five major jurisdictions (2018–2024).

Sources: Adapted from references [3,4,5].

Predictive Policing Algorithms

Predictive policing algorithms (PPAs) use historical crime data, sociodemographic variables, and geospatial analysis to forecast where crimes are likely to occur and who is most likely to commit or become a victim of crime. Systems such as PredPol (now Geolitica), HunchLab, and the Chicago Police Department's Strategic Subject List (SSL) have been widely adopted in the United States and increasingly piloted internationally [6,7].

A consistent body of research demonstrates that PPAs systematically overpredict crime in Black and Latino neighbourhoods because they are trained on arrest data that reflect historical patterns of racially disproportionate policing rather than actual offending rates [6,8]. Hung and Yen's (2023) analysis of algorithmic fairness in predictive policing demonstrated that even ostensibly race-neutral variables, such as ZIP code, family structure, and prior police contacts, function as racial proxies within machine learning models [8]. This creates a self-reinforcing feedback loop: algorithmic predictions concentrate policing in certain areas, producing more arrests in those areas, which subsequently reinforces the algorithm's prediction of high crime [7]. The Chicago Police Department discontinued ShotSpotter contracts in 2024 following investigations showing the system produced inaccurate alerts and exacerbated unconstitutional stop-and-frisk practices in communities of colour [9].

Body-Worn Cameras and AI-Assisted Review

Body-worn cameras (BWCs) have become a widespread reform mechanism, adopted by thousands of law enforcement agencies globally as a means of increasing transparency and accountability in police-civilian encounters [10,11]. However, the sheer volume of footage

generated-Axon, the leading BWC manufacturer, hosts over 100 petabytes of video data-has rendered comprehensive human review infeasible, spurring adoption of AI-powered natural language processing (NLP) systems to automate the analysis of BWC audio and video [12].

Adams et al. (2025) conducted pre-registered randomised controlled trials in two large US police agencies and found that AI-powered behavioural monitoring of BWC footage was associated with measurable improvements in officer professionalism metrics when officers received feedback [13]. Davies and Krame (2023) proposed an integrated framework combining BWCs, drones, and AI to enhance police readiness and incident response, highlighting that BWC footage increasingly influences criminal justice proceedings, including guilty plea rates and evidentiary proceedings [11]. Nonetheless, concerns persist regarding officer acceptance of electronic performance monitoring, privacy implications for civilians captured on footage, and the risk that AI classification of officer behaviour may embed human evaluator bias into automated systems [14].

ETHICAL IMPLICATIONS

Algorithmic Bias and Racial Discrimination

The most extensively documented ethical concern associated with AI in policing is algorithmic bias, the production of systematically skewed outputs that disadvantage members of marginalised communities. Research on FRT consistently finds higher false-positive rates for individuals with darker skin tones, with some algorithms exhibiting error rates up to ten times greater for Black women than for White men [4,15]. These disparities are not incidental; they reflect training data that over-represents arrests of Black individuals, themselves a product of racially differential policing practices [7].

With respect to PPAs, Sholademi and Raji (2024) found that Black defendants were disproportionately assigned high-risk recidivism scores relative to White defendants with comparable criminal histories, a disparity observed across multiple commercially deployed risk assessment tools [16]. Gallon (2023) demonstrated through analysis of Los Angeles Police Department archives that predictive algorithms directed resources disproportionately towards Black and Latino communities even when location, not race, was the direct input variable [17]. The American

Philosophical Association's examination of algorithmic fairness in policing (2022) argued that existing notions of mathematical fairness are insufficient; substantive fairness requires that communities most affected by predictive policing provide meaningful consent and receive tangible benefits from its deployment [18]. Figure 2 illustrates the algorithmic bias feedback loop in predictive policing.

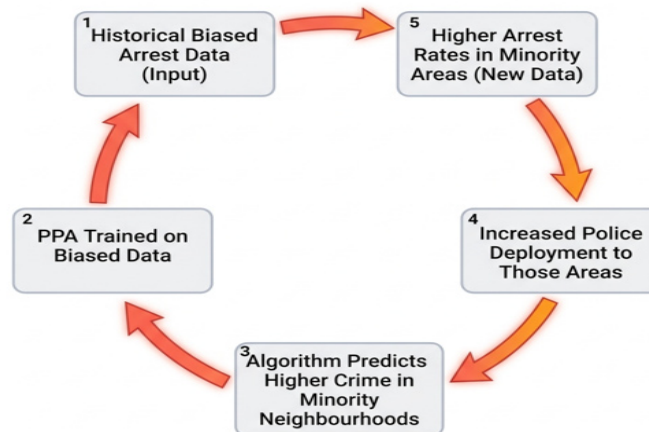


Fig2. The algorithmic bias feedback loop in predictive policing.

Sources: [6,7,8,17].

Privacy, Mass Surveillance, and Civil Liberties

The deployment of AI-driven surveillance at scale raises foundational questions about the right to privacy and the chilling effect on constitutionally protected activities. Real-time facial recognition in public spaces enables continuous tracking of individuals who have committed no offence, creating a capacity for population-level surveillance that is qualitatively different from targeted policing of known suspects [5]. Social media surveillance tools employed by law enforcement similarly affect the exercise of free speech and the right of assembly, particularly in the context of protest movements where activists are identified and monitored through automated image analysis [1,2].

Wang et al. (2024) situated these concerns within a broader human-rights framework, arguing that mass biometric surveillance implicates the freedoms of association, expression, and conscience, and that the state bears an affirmative obligation to justify such surveillance through necessity and proportionality analyses rather than merely invoking public safety [4]. Okonkwo (2023) underscored that AI surveillance architectures undermine the universal entitlement to digital privacy and dignity, particularly when deployed asymmetrically against marginalised communities who have historically been subject to disproportionate state scrutiny [19].

Transparency, Accountability, and Due Process

Accountability for AI-driven policing decisions is frequently diffuse or absent. Proprietary algorithmic tools are typically shielded from disclosure under trade secrets law, preventing defendants from scrutinising the evidentiary basis for their arrest or prosecution. This dynamic fundamentally conflicts with due process principles that require defendants to confront and challenge evidence used against them [8,9]. Erdogan (2024) traced this problem through EU law, finding that even under GDPR Article 15 access rights, individuals subject to law enforcement AI were systematically denied meaningful access to data held about them by police agencies [20].

The European Data Protection Board's Statement 3/2024 emphasised that data protection authorities must function as the primary supervisory bodies for high-risk AI systems in law enforcement, precisely because such systems produce automated profiling outputs with severe consequences for data subjects [20,21]. Sachoulidou (2024) further argued that the EU AI Act, while establishing important prohibitions on real-time biometric surveillance and predictive individual risk assessment, contains exceptions and loopholes sufficiently broad to permit continued deployment of many contested tools in law enforcement contexts [22].

LEGAL AND REGULATORY FRAMEWORKS

The European Union: A Risk-Based Regulatory Paradigm

The European Union's AI Act (Regulation 2024/1689), which entered into force on 1 August 2024, represents the world's first comprehensive legislative framework for AI regulation. The Act adopts a risk-based tiered classification system, prohibiting high-risk, limited-risk, and minimal-risk AI, and specifically classifies biometric surveillance and predictive policing among the most stringently regulated categories [21,22]. Real-time remote biometric identification (including live FRT) in publicly accessible spaces is categorically prohibited, with narrow law-enforcement exceptions permitting retrospective post-event identification only on judicial authorisation in relation to serious criminal offences [21].

The AI Act operates in conjunction with the GDPR (Regulation 2016/679) and the Law Enforcement Directive (2016/680), creating a layered data governance framework [20]. Processing biometric data for identification purposes requires an explicit legal basis under GDPR Article 9, and agencies employing AI-enhanced surveillance are likely to require Data Protection Impact Assessments under Article 35 [21]. Data Protection Authorities (DPAs) have been urged by the European Data Protection Board to serve as the national AI market surveillance authorities, consolidating data protection and AI oversight within a single regulatory body [20]. Fines under the AI Act reach €35 million or 7% of global annual turnover for prohibited

AI practices—the most stringent financial penalties in global AI governance [21].

The United States: Fragmented State-Level Regulation

The United States lacks comprehensive federal legislation governing AI in policing. Instead, regulatory responses have emerged at state and municipal levels in response to specific harms. San Francisco, Boston, and several other cities enacted bans on government use of FRT between 2019 and 2022; however, in a notable reversal, San Francisco voters approved a 2024 ballot measure granting police broader authority to deploy surveillance technology including FRT and drones in response to urban disorder concerns [5].

At the federal level, the GAO's March 2024 report found that only three of seven scrutinised DHS and DOJ agencies had civil-rights-specific FRT policies in place, and that most agencies had deployed FRT before implementing mandatory staff training [3]. The Biden administration's October 2023 Executive Order on AI directed federal agencies to develop sector-specific standards, but critics noted that the Order's law enforcement provisions were aspirational rather than enforceable [16]. Illinois remains the most protective state jurisdiction through the Biometric Information Privacy Act (BIPA), which requires informed consent and private rights of action for biometric data collection, a model increasingly recommended for federal adoption [2].

The United Kingdom, Canada, and Beyond

Table 2. Comparative Regulatory Frameworks for AI Surveillance in Policing Across Major Jurisdictions

Jurisdiction	Key Legislation/Policy	FRT / PPA Stance	Oversight Body	Penalty (max)
European Union	EU AI Act 2024 (Reg. 2024/1689); GDPR	Real-time FRT banned; PPA prohibited; exceptions for terrorism/missing persons	DPAs + AI Office	€35 million or 7% global turnover
United States	No federal AI law; state-level bans (Illinois BIPA; California AB 1215)	Fragmented; cities ban FRT; predictive policing widely used	DOJ/DHS + GAO audits	State-dependent; civil liability
United Kingdom	Data Protection Act 2018; Surveillance Camera Code	Live FRT trialled by MPS; scrutinised by courts	ICO; Surveillance Camera Commissioner	£17.5 million or 4% turnover
Canada	PIPEDA; provincial privacy statutes	Clearview AI deemed unlawful; provincial commissioners active	Office of Privacy Commissioner	Orders to stop; no fines yet
Australia	Privacy Act 1988; proposed reforms (2024)	Sector guidance only; FRT use is growing	OAIC + state ombudsmen	AUD 50 million (proposed)

Source: Compiled by the authors based on [2,3,5,20,21,22].

The United Kingdom's Surveillance Camera Commissioner and the Information Commissioner's Office (ICO) have scrutinised live FRT trials conducted by the Metropolitan Police Service, with courts upholding proportionate retrospective use while raising concerns about operational governance [5]. Canada's Office of the Privacy Commissioner issued landmark findings declaring Clearview AI's mass facial image scraping unlawful under PIPEDA in 2021, and provincial commissioners, notably Ontario's, have produced detailed guidance frameworks for police use of FRT [2].

Australia is pursuing a comprehensive Privacy Act reform, with a 2024 review recommending substantially increased fines and mandatory privacy impact assessments for government AI systems. Globally, the emerging consensus from regulatory bodies in democratic states is that FRT use in law enforcement must be authorised by specific legislation rather than merely inferred from general police powers, be subject to judicial oversight, and be audited by independent bodies with authority to recommend or mandate discontinuation [5,22]. Table 2 presents a comparative regulatory overview across five major jurisdictions, highlighting the diversity of legal approaches to FRT, PPAs, and AI policing governance.

CRIMINAL JUSTICE IMPLICATIONS

Evidence, Prosecution, and Wrongful Conviction

The introduction of AI-generated evidence into criminal proceedings poses novel challenges to evidentiary standards, disclosure obligations, and the reliability of verdicts. BWC footage analysed by AI NLP systems can produce automated professionalism or misconduct scores that may be presented in disciplinary or civil proceedings without adequate validation of the underlying algorithm's accuracy or fairness [13,14]. Guler et al. (2025) demonstrated that the availability of BWC footage was strongly associated with substantiation of use-of-force allegations at the NYPD, with allegations involving African American and Hispanic complainants more likely to be substantiated when footage was available, a finding consistent with the hypothesis that BWC technology may partially mitigate racial bias in police oversight [23].

Conversely, FRT-based misidentifications have directly contributed to wrongful arrests, an irreversible harm that standard prosecutorial safeguards are ill-equipped to detect when the underlying match is treated as technically objective. The absence of disclosure requirements for proprietary algorithms means that defence counsel in many jurisdictions cannot access the model's error rates, training data, or known biases—a violation of the principle

that defendants must be able to confront and test evidence [8,20]. Legislative interventions such as the New York City Public Oversight of Surveillance Technology (POST) Act represent tentative steps toward mandatory disclosure, but enforcement mechanisms remain weak [16].

Sentencing, Recidivism Risk Assessment, and Parole

Beyond investigation and arrest, AI tools increasingly influence sentencing and parole decisions through actuarial risk assessment instruments such as COMPAS, Level of Service Inventory-Revised (LSI-R), and the Public Safety Assessment (PSA). These tools generate recidivism risk scores that advise judicial officers, parole boards, and prosecutors, potentially compressing the individualised sentencing discretion that common-law and constitutional traditions protect [16,18].

Gallon (2023) reported that Black defendants were 77% more likely to receive high violent-recidivism risk scores than White defendants with comparable criminal histories when assessed by commercially deployed algorithms [17]. Hung and Yen (2023) argued that algorithmic fairness cannot be reduced to calibration or statistical parity alone, but must incorporate substantive social justice considerations, including the consent of affected communities to the use of such tools [8]. Lee (2025) found that exposing police officers to algorithmic recidivism predictions reduced racial disparities in their subjective probability estimates, but only when the officer's racial identity was Black, suggesting that implicit bias interacts with algorithmic anchoring in complex ways that simple exposure to AI outputs does not resolve [25].

Implications for Community Trust and Police Legitimacy

Perceptions of procedural fairness are foundational to police legitimacy and community compliance with the law. A study examining public support for AI in policing (2025) found that citizens who perceived AI policing tools as procedurally fair were significantly more likely to support their use, but that trust in law enforcement was itself a precondition for accepting AI-augmented police authority [24]. Conversely, communities disproportionately surveilled by AI tools, particularly communities of colour, exhibit lower baseline trust in police, undermining the legitimacy of AI deployment in those contexts [7,18].

The evidence is consistent: without meaningful community engagement, transparency about how AI tools work, and demonstrated accountability when they fail, AI-enhanced policing will deepen existing legitimacy deficits. Effective governance models must therefore incorporate not

merely technical safeguards but structural democratic accountability mechanisms, civilian review boards with genuine authority, community consultation requirements before technology procurement, and publicly accessible annual reporting on AI tool deployment, accuracy, and demographic impact [2,9,22].

TOWARDS AN ETHICAL AND REGULATORY FRAMEWORK FOR AI POLICING

Synthesising the foregoing evidence, Table 3 presents a structured ethical framework for evaluating and governing AI deployment in policing contexts. The framework is organised around six core principles: transparency, non-discrimination, proportionality, accountability, due process, and privacy, each of which maps onto specific operational requirements and recommended safeguards.

These principles should not be understood as aspirational ideals alone; they must be operationalised through binding legal obligations, independent oversight institutions, and enforceable sanctions. The EU AI Act's architecture, with its prohibited practices list, high-risk classification system, mandatory conformity assessments, and DPA

enforcement role, provides the most developed template for translating ethical principles into law. However, even the EU framework contains national security loopholes and implementation discretions that may undermine its effectiveness in law enforcement contexts [20,22].

A minimum standard for any jurisdiction deploying AI in policing should include: (a) pre-deployment algorithmic impact assessments; (b) ongoing demographic bias audits; (c) human-in-the-loop requirements for any AI output that triggers a coercive police action; (d) judicial pre-authorisation for any real-time biometric surveillance; (e) full disclosure to defendants of AI tools used in their investigation and prosecution; and (f) public registries of all AI tools deployed by law enforcement agencies

DISCUSSION

This review reveals a fundamental tension at the heart of AI-augmented policing: the same technologies that offer genuine public safety benefits, faster identification of violent offenders, more efficient deployment of limited police resources, enhanced accountability for officer conduct, also enable unprecedented surveillance capacity, reproduce systemic racial discrimination, and

Table 3. *Ethical Principles Framework for AI Deployment in Policing*

Ethical Principle	Definition	Application to AI Policing	Recommended Safeguard
Transparency	Open, understandable AI decision processes	Algorithmic outputs must be explainable to courts, suspects, and the public	Mandatory algorithmic audits; public registries of deployed AI tools
Non-discrimination	Equal treatment regardless of race, gender, or socioeconomic status	FRT and PPA systems exhibit higher error rates for darker-skinned individuals	Bias audits before deployment; diverse training datasets; race-aware impact assessments
Proportionality	Surveillance intensity must match the severity of the threat	Real-time mass biometric surveillance exceeds what is proportionate for minor crime prevention	Judicial pre-authorisation; narrow legislative exceptions; sunset clauses
Accountability	Clear lines of responsibility for AI-driven decisions	Automated decisions (e.g., risk scores) should not stand alone as grounds for arrest	Human-in-the-loop requirements; civilian oversight boards; right of appeal
Due Process	Right to challenge evidence used against an individual	Defendants often cannot interrogate proprietary AI tools used to incriminate them	Disclosure obligations; open-source or independently audited algorithms for court use
Privacy	Protection of personal data from unreasonable surveillance	Mass surveillance chills free speech and assembly; data retained beyond necessity	Data minimisation principles; strict retention limits; DPIA requirements (GDPR Art. 35)

Source: *Compiled by the authors based on references [1,2,4,8,18,19,20,21,22].*

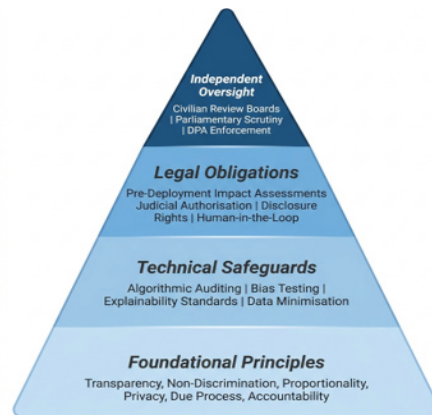


Fig3. A proposed governance framework for ethical AI integration in law enforcement.

Sources: Adapted from references [1,5,21,22].

erode procedural rights that underpin the legitimacy of criminal justice systems. This tension cannot be resolved by technological refinement alone; it requires normative choices about what kind of policing society wishes to enable and what constraints are necessary to protect the dignity and rights of individuals subject to police power.

The evidence reviewed here suggests that the current trajectory- rapid technology deployment outpacing regulatory oversight, poses unacceptable risks. The documented harms of FRT misidentification, PPA-driven over-policing, and algorithmic risk scoring in sentencing are not theoretical; they are materialising in real arrests, prosecutions, and incarcerations of individuals who may be innocent or who are subject to systemic discrimination [7,8,17]. Regulatory frameworks such as the EU AI Act represent important progress, but their effectiveness will depend critically on implementation, particularly on whether DPAs and courts are willing to challenge law enforcement agencies' invocation of national security and operational necessity exceptions [20,22].

A significant gap in the current evidence base concerns the long-term community-level effects of sustained AI surveillance on social trust, democratic participation, and patterns of lawful behaviour. Longitudinal studies are needed that move beyond measures of crime rates to capture the broader civic costs of surveillance architectures. Similarly, interdisciplinary research bridging computer science, law, and criminology is needed to develop algorithmic auditing methodologies that are technically rigorous, legally actionable, and accessible to non-specialist judges and policymakers [1,22].

CONCLUSION

Artificial intelligence and digital surveillance are reshaping modern policing in ways that are simultaneously

transformative and deeply problematic. This review has demonstrated that while AI tools offer measurable operational benefits, they also pose documented and serious threats to equality, privacy, due process, and community trust. The ethical, legal, and criminal justice implications are interconnected: algorithmic bias produces discriminatory policing outcomes; inadequate legal frameworks fail to hold agencies accountable; and compromised due process undermines the fairness of criminal adjudication.

The path forward requires a robust, binding, and internationally coordinated governance response. The EU AI Act provides a meaningful template, but national implementations must resist the dilution of protections through broad national security exceptions. Beyond law, governance must be participatory: communities most affected by AI policing must have voice in decisions about technology procurement, deployment, and discontinuation. This is not merely an ethical aspiration but a practical prerequisite for the police legitimacy that effective crime prevention ultimately requires.

Researchers, clinicians, policymakers, and civil society actors must collaborate to develop evidence-based standards for algorithmic impact assessment, to advocate for legislative reforms that embed due process in the AI age, and to hold law enforcement agencies accountable through both legal mechanisms and public transparency. The governance choices made in the next decade will determine whether AI becomes a tool for more just and effective policing, or a vehicle for entrenching and amplifying the inequities that have long beset criminal justice systems.

DECLARATIONS

Funding: The authors received no specific funding for this work.

Conflict of Interest: The authors declare no conflicts of interest.

Author Contributions: All authors contributed equally to conceptualisation, literature search, writing, and revision.

Ethics Approval: Not applicable (review article; no human participants).

REFERENCES

- Dubravova H, Cap J, Holubova K, Hribnak L. Artificial intelligence as an innovative element of support in policing. *Procedia Comput Sci.* 2024;237:237-244. doi:10.1016/j.procs.2024.05.101
- Robles P, Mallinson DJ, Best E, Devaney C, Azevedo L. Global perspectives on regulating facial recognition technology utilization for criminal justice arrests. *Glob Public Policy Gov.* 2025;5(2):186-204. doi:10.1007/s43508-025-00117-9
- U.S. Government Accountability Office. Facial recognition technology: federal law enforcement agency efforts related to civil rights and training [GAO-24-107372]. Washington, DC: GAO; 2024. Available from: <https://www.gao.gov/products/gao-24-107372>
- Wang X, Wu YC, Zhou M, Fu H. Beyond surveillance: privacy, ethics, and regulations in face recognition technology. *Front Big Data.* 2024;7:1337465. doi:10.3389/fdata.2024.1337465
- Lynch N. Facial recognition technology in policing and security—case studies in regulation. *Laws.* 2024;13(3):35. doi:10.3390/laws13030035
- Minocher X, Randall C. Predictable policing: new technology, old bias, and future resistance in big data surveillance. *Convergence.* 2020;26(5-6):1108-1124. doi:10.1177/1354856520933838
- Berk RA. Artificial intelligence, predictive policing, and risk assessment for law enforcement. *Annu Rev Criminol.* 2021;4(1):209-237. doi:10.1146/annurev-criminol-051520-012342
- Hung TW, Yen CP. Predictive policing and algorithmic fairness. *Synthese.* 2023;201(6):206. doi:10.1007/s11229-023-04189-0
- Ziosi M, Pruss D. Evidence of what, for whom? The socially contested role of algorithmic bias in a predictive policing tool [Preprint]. arXiv:2405.07715. 2024. Available from: <https://arxiv.org/abs/2405.07715>
- Ali MU, Wright JE. Use of performance information and external accountability: the role of citizen oversight in mitigating the motivated evaluation of body-worn camera evidence. *Am Rev Public Adm.* 2024;54(3). doi:10.1177/02750740241229998
- Davies A, Krame G. Integrating body-worn cameras, drones, and AI: a framework for enhancing police readiness and response. *Policing: J Policy Pract.* 2023;17(1):1-13. doi:10.1093/policing/paad083
- Camp NP, Voigt R. Body camera footage as data: using natural language processing to monitor policing at scale and in depth. *Behav Sci Policy.* 2025;10(2):16-25. doi:10.1177/23794607241308636
- Adams IT, McLean K, Alpert G. Improving police behavior through artificial intelligence: pre-registered experimental results in two large US agencies. *Criminology.* 2025;64:502-516. doi:10.1111/1745-9125.70028
- Adams IT. Automation and artificial intelligence in police body-worn cameras: experimental evidence of impact on perceptions of fairness among officers. *J Crim Justice.* 2025;97:102373. doi:10.1016/j.jcrimjus.2025.102373
- Nazer L, Zatarah R, Waldrip S, Janny XCK, Moukheiber M, Khanna AK, et al. Bias in artificial intelligence algorithms and recommendations for mitigation. *PLOS Digit Health.* 2023;2(6):e0000278. doi:10.1371/journal.pdig.0000278
- Raji I, Sholademi DB. Predictive policing: the role of AI in crime prevention. *Int J Comput Appl Technol Res.* 2024;13(10):66-78. doi:10.7753/ijcatr1310.1006
- Gallon A. Racism repeats itself: AI racial bias in predictive policing algorithms. *Proc Bay Honors Res Symp.* 2023. Available from: <https://thinkyou.bayhonors.org>
- Purves D. Fairness in algorithmic policing. *J Am Philos Assoc.* 2022;8(4):741-761. doi:10.1017/apa.2021.39
- Okonkwo OA. Ethical tensions between AI surveillance architectures, human rights preservation, and the universal entitlement to digital privacy and dignity. *Magna Sci Adv Res Rev.* 2023;9(2):222-238. doi:10.30574/msarr.2023.9.2.0179
- Erdogan Peter I. Diving into the iceberg: establishing transparency in AI for law enforcement. *Eur Papers.* 2024;9(3):956-977. doi:10.15166/2499-8249/794
- European Parliament, Council of the European Union. Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Off J Eur Union.* 2024;L 1689:1-144. Available from: <https://eur-lex.europa.eu>
- Sachoulidou A. Harnessing AI for law enforcement: solutions and boundaries from the forthcoming AI Act. *New J Eur Crim Law.* 2024. doi:10.1177/20322844241260114

23. Guler A, Boke K, VanDorick D. The influence of body-worn camera footage on use-of-force investigations within the New York City Police Department. *Crime Delinq.* 2025. doi:10.1177/00111287251391200
24. Ezzeddine Y, Bayerl PS, Gibson H. Safety, privacy, or both: evaluating citizens' perspectives around artificial intelligence use by police forces. *Polic Soc.* 2023;33(7):861-876. doi:10.1080/10439463.2023.2211813
25. Lee YS. Can AI help reduce human bias? Insights from police rearrest predictions. *Proc Fourth Eur Workshop Algorithm Fairness.* PMLR. 2025;294:499-504. Available from: <https://proceedings.mlr.press/v294/lee25a.html>

Cite this article:: Micheal Abimbola Oladosu et.al. *The Impact of Digital Surveillance and Artificial Intelligence on Modern Policing: Ethical, Legal, and Criminal Justice Implications* *International Journal of Research in Management Science and Engineering (IJRMSE)* 2026; 3(1): 55-64.

Copyright: © 2026. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.