
Artificial Intelligence in Crime Control: Legal, Ethical, and Human Rights Challenges

Monika Sharma,
Assistant Professor,
School of Law, Starex University,
Gurugram, India

Dr.Rajni Kaushal
Assistant Professor,
School of Law, Starex University,
Gurugram, India

Abstract

Artificial Intelligence (AI) has emerged as an influential tool in modern crime control systems, transforming policing, surveillance, criminal investigations, and risk assessment processes. Technologies such as predictive policing, facial recognition, and algorithmic decision-making are increasingly used to improve efficiency, resource allocation, and crime prevention. While these innovations offer significant administrative and investigative advantages, their growing integration into criminal justice systems raises serious ethical, constitutional, and governance concerns. AI-driven systems often rely on large datasets and opaque algorithms that may reinforce existing social biases, threaten privacy rights, and undermine procedural fairness and accountability.

This paper critically examines the legal and ethical challenges arising from the use of AI in crime control. It analyses how AI-assisted policing and surveillance may conflict with fundamental rights such as equality, privacy, free expression, and due process. Through a comparative study of regulatory approaches in the European Union, the United Kingdom, the United States, and India, the paper highlights the emerging emphasis on transparency, explainability, human oversight, and rights-based governance of high-risk AI systems. The paper argues that although AI can significantly strengthen crime control mechanisms, it should function only as a supportive tool under strict human supervision and constitutional safeguards to ensure accountability, fairness, and protection of human rights in the criminal justice system.

Key Words: - Artificial Intelligence (AI), Crime Control, Algorithmic Decision-Making, Legal Accountability, Ethical Challenges, Human Oversight, Comparative Legal Frameworks.

Introduction

Artificial Intelligence (AI) is a significant instrument in the contemporary crime control machinery around the globe. AI is defined as computerized systems whereby techniques, including machine learning, predictive analytics and facial recognition are applied in processing vast volumes of data and help to make decisions. In criminal justice, these technologies are increasingly used in policing, surveillance, criminal investigation, and even in bail, sentencing, and risk assessment decisions. Law enforcement agencies and governments use AI to become more efficient, forecast crime patterns, and use resources to allocate funds more efficiently.

In Western countries, AI-powered applications like predictive policing software in the United States, algorithmic risk evaluation in the United Kingdom and Europe, are applied to determine and predict places of crime and the potential of recidivism. Nonetheless, it has been demonstrated that these systems can support the existing social and racial bias in crime statistics and casting significant doubts on transparency and responsibility.¹ The increasing application of AI is extremely dangerous due to legal and ethical issues, especially when it comes to the criminal liability. The classical criminal law is established on the human notions of intention, knowledge and personal responsibility. AIs on the other hand can be autonomous or semi-autonomous and it can be challenging to identify who is to be held accountable when an AI-based decision triggers harm or injustice. This brings out the primary question of this paper:

¹ Richard A. Berk, "Artificial Intelligence, Predictive Policing, and Risk Assessment for Law Enforcement," 4 *Annual Review of Criminology* 209–37 (2021).

1. Does AI-based crime control threaten constitutional rights and procedural fairness?
2. Can existing legal safeguards adequately regulate AI-driven policing and surveillance?
3. What regulatory framework best balances innovation and human rights protection?

Understanding AI in Crime Control

Artificial Intelligence (AI) in crime control refers to the use of computer systems that can analyse data, identify patterns, and support or make decisions that affect criminal justice processes. To readers with a legal background, one should realize that AI is not like human reasoning. It, rather, is based on data-driven models that learn the previous information and make predictions or recommendations. This conceptual framework explains the nature of AI and how it operates within modern crime control systems.

There are two commonly recognized types of AI namely: Narrow AI and General AI. "Narrow AI is programmed to be able to carry out certain functions", e.g. face recognition, crime hotspots prediction, or risk score. Every AI system in policing and criminal justice is of this type at the moment. "General AI, the one that would be endowed with the ability to think like humans and autonomous thought, is an unrealistic thing and is not applied to crime control".² Algorithms in criminal justice are a major characteristic of AI, which is a feature of algorithmic decision-making. Algorithms are used on a large scale of data, which may be crime records, arrest records or CCTV footage.³ It generates outputs affecting policing or judicial judgements. These results can come out as objective yet are influenced with quality, scope and bias of data used.⁴

The AI systems can also be differentiated into assistive and autonomous. Assistive systems are designed to help human decision-makers to make suggestions whereas autonomous systems are designed to work with limited human involvement. Most AI tools in crime control are officially supportive but as a matter of fact, their suggestions are highly influential, evoking fears of less human control and responsibility.

AI Applications in Crime Control

Predictive Policing: It is one of the significant uses of AI, where algorithms are used to analyse previous crime data to determine likely times and occurrences of crimes. In the United States and the United Kingdom, such systems are used to allocate police resources. However, empirical research shows that predictive policing may reproduce enforcement biases, particularly against disadvantaged communities.⁵

Facial Recognition Technology: Facial recognition is used in the identification of suspects and missing persons by the police forces in the UK and India. Certain states in India use AI-based facial recognition technology that uses criminal databases and this raises concerns regarding accuracy, privacy, and consent.⁶

Surveillance and Crime Mapping: The other area of AI application in crime mapping and surveillance is the integration of CCTV, drone, and digital data to track the people in the streets. Such practices have been the focus of regulatory debate in the European continent, raising the demand to make high-risk AI systems transparent and explainable.⁷

² Wim Naudé and Nicola Dimitri, "The race for an artificial general intelligence: implications for public policy," 35 *AI & SOCIETY* 367–79 (2020).

³ Camino Kavanagh, *New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft Smarter Responses?* (Carnegie Endowment for International Peace, 2022).

⁴ Richard A. Berk, "Artificial Intelligence, Predictive Policing, and Risk Assessment for Law Enforcement," 4 *Annual Review of Criminology* 209–37 (2021).

⁵ Victor Rotaru et al., "Event-level prediction of urban crime reveals a signature of enforcement bias in US cities," 6 *Nature Human Behaviour* 1056–68 (2022).

⁶ Zubair Ahmed Khan and Asma Rizvi, "AI-based facial recognition technology and criminal justice: issues and challenges," 12 *Turkish Journal of Computer and Mathematics Education* 3384–92 (2021).

⁷ Zubair Ahmed Khan and Asma Rizvi, "AI-based facial recognition technology and criminal justice: issues and challenges," 12 *Turkish Journal of Computer and Mathematics Education* 3384–92 (2021).

Algorithmic Risk Assessment: Risk assessment tools assist courts in bail and sentencing decisions by estimating the likelihood of reoffending⁸.

Automated Forensic Systems: Automated forensic analysis, such as AI-assisted fingerprint or DNA matching, is used to speed up investigations⁹.

While these applications improve efficiency, they also shift critical decision-making power to algorithms, thereby directly influencing outcomes in liberty, fairness, and justice. Understanding how AI functions in crime control is essential to assessing its legal and ethical consequences, particularly its impact on accountability and criminal liability.

Ethical and Human Rights Challenges

The use of Artificial Intelligence (AI) in crime control raises serious ethical concerns that go beyond formal legal rules.

Algorithmic Bias and Discrimination: While AI promises efficiency and objectivity, its deployment in policing, surveillance, and criminal justice decision-making directly affects fundamental values such as fairness, privacy, accountability, and human dignity. The ethical analysis is hence imperative to the general societal effects of the AI-based crime-control systems. Ethical reasoning on AI in crime control commonly features the concept of algorithmic decision-making as an approach to minimize human bias.¹⁰ This statement should be subject to doubt, though.

Democratic Accountability: Artificial intelligence systems do not remove bias, often they simply re-package past and structural injustices in a technical way and thus become more difficult to identify and dispute.¹¹ When ethical governance focuses narrowly on performance metrics such as accuracy or cost reduction, it obscures deeper concerns about fairness and democratic accountability.¹²

Transparency and Explainability: The increasing unease with this type of ethical trade-off can be characterized by judicial and regulatory interventions. In SyRI (District Court of The Hague, Netherlands), a welfare fraud detection algorithm was ruled invalid due to breaches of the principles of transparency and proportionality, even though it is alleged to be efficient in its administration.¹³ This court stressed that non-transparent algorithmic systems deprive citizens of the capacity to challenge state action and consequently erode the confidence of people in the state institutions. Even though the case occurred in the context beyond criminal law, its logic could be more applied to AI-controlled crime control when the outcomes regarding individual liberty are even more drastic.¹⁴

Moral Assessment of Criminal Responsibility: needs to be morally assessed Additionally, the possibility of eroding normative principles of criminal justice through the moral transfer of moral judgement to machines is an ethical threat of automation. Other legal scholars have pointed out that criminal responsibility needs to be morally assessed, not simply a recognition of pattern, and ethical models, which give technological optimization first priority, would automatically encourage the acceptance of anti-moral decisions.¹⁵ Such a criticism is especially applicable in places like India and the United States, where AI tools are being actively implemented with no statutory direction, and ethical protection relies on organizational will and not enforceable standards.

Due Process and Procedural Fairness: Even though efficiency, speed and predictive accuracy are often discussed as the reasons to implement Artificial Intelligence to control crimes, in many cases, these priorities are fulfilled at the cost

⁸ John Logan Koepke and David G Robinson, "Danger ahead: Risk assessment and the future of bail reform," 93 *Wash. L. Rev.* 1725 (2018).

⁹ Meghya Nayak, "Ai-enhanced digital forensics: Automated techniques for efficient investigation and evidence collection," 20 *J. Electrical Systems* 211–29 (2024).

¹⁰ Tejas Kumar B Modi, "Artificial Intelligence Ethics and Fairness: A study to address bias and fairness issues in AI systems, and the ethical implications of AI applications," 3 *Revista Review Index Journal of Multidisciplinary* 24–35 (2023).

¹¹ Richard A. Berk, "Artificial Intelligence, Predictive Policing, and Risk Assessment for Law Enforcement," 4 *Annual Review of Criminology* 209–37 (2021).

¹² Xavier Ferrer et al., "Bias and discrimination in AI: a cross-disciplinary perspective" *arXiv preprint arXiv:2008.07309* (2020).

¹³ John Thibaut et al., "Procedural justice as fairness," 26 *Stan. L. Rev.* 1271 (1973).

¹⁴ Ali Noor Mohamed, "Journalism and activist democratic theory and ethics: when the 'chilling effects' of libel can lose effect," 21 *Journalism* 1212–28 (2020).

¹⁵ Thomas Franke et al., "Initial port integration concept for EC and NB systems in EU DEMO tokamak," 146 *Fusion Engineering and Design* 1642–6 (2019).

of procedural guarantees and personal justice. AI systems are likely to lend more towards standardization of decision-making since they are based on probabilistic assessment and not contextual assessment.¹⁶ This change threatens turning the criminal justice system to more of a system based on administrative convenience than one founded on moral judgement. Algorithms and prospective policing (as well as risk assessment) have been subjected to empirical and normative criticism that these tools tend to institutionalize suspicion instead of fostering fairness, and that they target already disadvantaged groups disproportionately.¹⁷ The blind prioritizing of efficiency over legality has been opposed more and more by the courts. European Court of human rights, in *H. W. v Germany* (ECtHR)¹⁸, restated that technological convenience is not able to weaken procedural assurances in cases of liberty. On the same note, a number of jurisdictions have also warned that, although algorithmic predictions can be statistically sound, they cannot replace the personalized evaluation demanded by due process.

These changes imply that efficiency by itself cannot be a normative purpose in using AI in crime control; efficiency should be included as a secondary measure to legality, proportionality, and accountability

Comparative Legal Approaches

The adoption of Artificial Intelligence (AI) in crime control has been very quick, and thus various jurisdictions have taken different legal stances regarding it. With the growing role of AI systems in policing, surveillance, and criminal justice decision-making, lawmakers and courts have the difficulty of negotiating between technology innovation and adherence to the basic rights of privacy, equality, fairness, and due process. The comparison and international overview of AI-related risks demonstrate an increasing understanding of the associated risks, but there is no universal global regulation of AI usage, and also no consistent criminal responsibility when AI-related harm takes place.

European Union: - The resolution to create an AI Artificial Intelligence Act will have a risk-based structure, categorizing AI systems based on their capacity to endanger fundamental rights. AI systems in the fields of law enforcement, predictive policing, facial recognition, and criminal justice decision-making are classified as high-risk and must be closely adhered to all the requirements of transparency, explainability, human oversight, and accountability.¹⁹ The General Data Protection Regulation (GDPR) further strengthens this framework by limiting fully automated decision-making and recognizing data protection and privacy as fundamental rights. The given model is in line with the ethical principles of proportionality, fairness and protection of human rights in criminal justice. On the contrary, the United States has a sector-based and piecemeal regulatory strategy. The federal legislation on AI in crime control does not exist in its full form. Rather, there is governmental regulation of AI use using constitutional laws, laws on civil rights, state laws and internal policing policies.

United Kingdom: - UK assumes a common-law system of AI regulation based on principles. Though no specific AI law exists that regulates the control of crime, the current legal principles like legality, proportionality, and procedural fairness are used to evaluate AI use in the police and surveillance. Courts are at the center of assessing the existence of AI tools.²⁰ The Court of Appeal in the top case on the application of algorithmic and AI-facilitated surveillance of R (Bridges) v Chief Constable of South Wales Police²¹, determined that the use of live facial recognition by the police was illegal. Court stressed that the use of technological means in the policing process should be in accordance with the law, proportionality, and procedural fairness as part of the human rights. Similar to the example of *R (Miller) v College of Policing*²², the Court of Appeal concluded that the “guidance under which no crime hates incidents operated” was unlawful because it had a disproportionate effect on freedom of expression and did not contain any explicit safeguards.

¹⁶ Meena Rani, “Impacts and ethics of using Artificial Intelligence (AI) by the Indian Police,” 27 *Public Administration and Policy* 182–92 (2024).

¹⁷ Matthew Browning and Bruce Arrigo, “Stop and risk: Policing, data, and the digital age of discrimination,” 46 *American Journal of Criminal Justice* 298–316 (2021).

¹⁸ “European Court of Human Rights (ECHR): *K.-H. W. v. Germany*,” 40 *International Legal Materials* 773–810 (2001).

¹⁹ Georgios Pavlidis, “Unlocking the black box: analysing the EU artificial intelligence act’s framework for explainability in AI,” 16 *Law, Innovation and Technology* 293–308 (2024).

²⁰ Ulrike Franke, *Machine Politics: Europe and THE AI Revolution*. (European Council on Foreign Relations, 2022).

²¹ [2020] *EWCA Civ 1058*

²² [2021] *EWCA Civ 1926*

The ruling supports the fact that algorithmic or data-driven policing practices should not work arbitrarily or chilling to fundamental rights, and it is crucial to have clear legal standards.

This model is based on the human rights law and judicial control and is flexible and adaptable. Nevertheless, researchers believe that the principles of common law might be not enough to resolve the technical opaque, scale, and complexity of the AI systems in the contemporary crime control.²³

India: - India has a rather reactive strategy, as protection mechanisms are built up over time due to the policy provisions and judicial rulings, as opposed to wholesale legislation. The Supreme Court case of *Anuradha Bhasin v Union of India*²⁴, considered the limitations on the access of the internet and reminded the executive that discretion cannot be arbitrary even in the areas of security. The Court believed that the limitations on the essential rights should be reasonable, proportionate, and liable to the judiciary review. The rationale is very applicable to AI-assisted crime control decision-making, in which algorithm-driven systems can be used without being transparent and justifiable. The current form of regulation is based on constitutional rights, judicial interpretation, and general criminal and administrative laws.²⁵

USA: - The recourse to post-hoc litigation and judicial review implies that the harms generated by the AI systems are considered only once the rights have been harmed. This paradigm has trouble with the systemic risks of accumulated prejudice and ubiquitous surveillance because single-user suing is poorly configured to take cultural algorithmic procedures to task. As a result, the US approach maintains discretion but creates large holes in criminal justice practices where there are high risks. The majority of jurisdictions do not accept the idea of AI acquiring legal personhood but rather have human actors as the ones responsible. International responses are growing in response to ethical governance, openness, data confidentiality, and cybersecurity.²⁶

Predictive policing and algorithmic risk assessment tools are widely used, but accountability is typically addressed after harm has occurred, through litigation or judicial review. Scholars note that although AI is promoted as efficient and objective, serious concerns remain regarding racial bias, transparency, and unequal impacts on marginalized communities.²⁷ This reflects a reactive liability model, where criminal responsibility depends on proving causation and fault on a case-by-case basis rather than through systemic safeguards.

Recommendations and Regulatory Safeguards

Human-in-the-Loop Oversight: Artificial Intelligence systems used in crime control should function strictly as decision-support tools rather than autonomous decision-makers. Human oversight must remain mandatory in high-stakes areas such as surveillance, predictive policing, arrests, bail, and sentencing. Final authority should rest with accountable human officials to ensure that moral judgement, proportionality, and constitutional safeguards are not replaced by automated decision-making. Human supervision is essential to preserve due process and prevent arbitrary reliance on algorithmic outputs.

Algorithmic Audits and Transparency: AI systems deployed in criminal justice should be subject to regular algorithmic audits and impact assessments to identify biases, discriminatory outcomes, and systemic errors. Transparency and explainability should be treated as mandatory legal standards, particularly for high-risk AI systems affecting individual liberty. The European Union's proposed AI Act emphasizes explainability and traceability to ensure accountability in algorithmic governance. Transparent systems enable judicial review, public scrutiny, and procedural fairness while preventing opaque and unchallengeable decision-making.

²³ Nadjia Madaoui, "The Impact of Artificial Intelligence on Legal Systems: Challenges and Opportunities," 1 *Problems of legality* 285–303 (2024).

²⁴ (2020) 3 SCC 637

²⁵ Meena Rani, "Impacts and ethics of using Artificial Intelligence (AI) by the Indian Police," 27 *Public Administration and Policy* 182–92 (2024).

²⁶ Michael R King, "The future of AI in medicine: a perspective from a Chatbot," 51 *Annals of Biomedical Engineering* 291–5 (2023).

²⁷ Richard A. Berk, "Artificial Intelligence, Predictive Policing, and Risk Assessment for Law Enforcement," 4 *Annual Review of Criminology* 209–37 (2021).

Rights-Based AI Governance: AI governance frameworks must prioritize constitutional rights and ethical principles over administrative convenience or efficiency. The deployment of AI in crime control should comply with standards of legality, proportionality, non-discrimination, privacy protection, and human dignity. In *Justice K.S. Puttaswamy v. Union of India*,² the Supreme Court recognized privacy as a fundamental right, reinforcing the need for safeguards against excessive surveillance and data misuse. Ethical guidelines should therefore require fairness, accountability, and respect for human rights in all AI-assisted criminal justice processes.

International Regulatory Cooperation: Given the transnational nature of AI technologies, international cooperation is necessary for developing consistent legal and ethical standards. Comparative approaches adopted in the European Union, the United Kingdom, and other jurisdictions demonstrate the importance of harmonized principles relating to accountability, transparency, and human oversight. Collaborative regulatory frameworks can help establish global standards for responsible AI governance while ensuring that technological innovation remains consistent with democratic values and the rule of law.

Conclusion

The increasing integration of Artificial Intelligence into crime control systems has transformed contemporary policing, surveillance, and criminal justice administration. AI-driven technologies such as predictive policing, facial recognition, algorithmic risk assessment, and automated surveillance offer significant advantages in efficiency, speed, and data analysis. However, their deployment also raises serious concerns relating to privacy, transparency, discrimination, due process, and democratic accountability. The use of opaque algorithmic systems in high-risk criminal justice functions may reinforce existing social biases and undermine constitutional protections if left unchecked.

Comparative regulatory approaches demonstrate that while jurisdictions such as the European Union emphasize risk-based governance and human oversight, countries like India and the United States continue to rely largely on reactive and fragmented safeguards. This highlights the urgent need for coherent legal frameworks capable of balancing technological innovation with human rights and procedural fairness.

Therefore, AI should not function as an autonomous authority in criminal justice processes. Instead, it must remain a supportive tool operating under strict human supervision, constitutional safeguards, and ethical regulation. Mandatory transparency, algorithmic audits, impact assessments, and rights-based governance are essential to ensuring accountability and preventing arbitrary state action. Ultimately, the legitimacy of AI in crime control depends upon preserving human judgement, rule of law, and the foundational principles of justice in the digital age.
