

ARTIFICIAL INTELLIGENCE IN CRIMINAL INVESTIGATIONS: ISSUES OF TRANSPARENCY, ACCOUNTABILITY AND DUE PROCESS

AUTHOR – NEGA.N, LL.M STUDENT AT THE TAMIL NADU DR. AMBEDKAR LAW UNIVERSITY

BEST CITATION – NEGA.N, ARTIFICIAL INTELLIGENCE IN CRIMINAL INVESTIGATIONS: ISSUES OF TRANSPARENCY, ACCOUNTABILITY AND DUE PROCESS, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 6 (9) OF 2026, PG. 765-773, APIS – 3920 – 0001 & ISSN – 2583-2344.

INTRODUCTION

Artificial Intelligence (AI) has emerged as a transformative force in modern criminal investigations, significantly reshaping traditional methods of policing, surveillance, evidence analysis, and crime prevention. Technologies such as facial recognition systems, predictive policing algorithms, biometric surveillance, digital forensics, automated decision-making tools, and machine learning systems are increasingly used by law enforcement agencies to identify suspects, analyze large volumes of data, and improve investigative efficiency. While AI offers advantages such as speed, accuracy, and enhanced crime detection capabilities, its growing integration into criminal justice systems has also raised serious legal, ethical, and constitutional concerns. Issues relating to algorithmic opacity, lack of transparency, biased decision-making, wrongful identification, and misuse of surveillance technologies challenge the principles of accountability, fairness, and due process. Furthermore, the extensive collection and monitoring of personal data through AI-driven systems raise concerns regarding privacy, equality, and protection against arbitrary state action, particularly in the absence of comprehensive legal regulation. In India, the increasing adoption of AI technologies in policing and criminal investigations highlights the urgent need for a balanced legal framework that ensures effective law enforcement while safeguarding constitutional rights and democratic values. This research paper therefore critically examines the role of Artificial Intelligence in criminal investigations with specific focus on the issues of transparency, accountability, and due process, while also analysing the need for regulatory safeguards and ethical AI governance in the digital age.

CONCEPT OF ARTIFICIAL INTELLIGENCE

Artificial Intelligence (AI) refers to the capability of computer systems and machines to perform tasks that normally require human intelligence, such as learning, reasoning, problem-solving, decision-making, and data analysis. AI operates through technologies such as machine learning, algorithms, natural language processing, and biometric recognition systems, enabling machines to analyse large volumes of information and generate predictive or automated outcomes. In recent years, AI has emerged as a transformative force in modern criminal investigations, significantly reshaping traditional methods of policing, surveillance,

evidence analysis, and crime prevention. Technologies such as facial recognition systems, predictive policing algorithms, biometric surveillance, digital forensics, and automated decision-making tools are increasingly used by law enforcement agencies to identify suspects, analyze evidence, and improve investigative efficiency. While AI offers advantages such as speed, accuracy, and enhanced crime detection capabilities, its growing use has also raised serious legal, ethical, and constitutional concerns relating to transparency, accountability, privacy, algorithmic bias, and due process. The absence of comprehensive legal regulation further increases the risks of wrongful identification, discriminatory policing,

misuse of surveillance technologies, and violation of fundamental rights.

APPLICATION OF AI IN CRIMINAL INVESTIGATIONS

Artificial Intelligence has become an important part of modern criminal investigations by improving crime detection, evidence analysis, and public security measures. Law enforcement agencies increasingly use AI-driven technologies such as facial recognition systems, predictive policing tools, biometric surveillance, data analytics, and automated decision-making systems to investigate cybercrime, terrorism, organized crime, and financial offences.

1) Facial Recognition Technology

Facial Recognition Technology (FRT) is a biometric AI system used to identify or verify individuals by analysing facial features through photographs, CCTV footage, and video recordings. Law enforcement agencies use FRT for suspect identification, criminal tracking, border security, missing person detection, and public surveillance. In India, AI-based facial recognition systems are increasingly used for policing and national security purposes.

2) Predictive Policing

Predictive policing refers to the use of AI algorithms and data analytics to predict possible criminal activities based on historical crime data and behavioural patterns. These systems help law enforcement agencies identify crime hotspots, allocate police resources efficiently, and prevent crimes before they occur. Predictive policing is commonly used in cases involving organized crime, gang violence, and drug trafficking.

3) Biometric Surveillance Systems

Biometric surveillance systems use AI technologies to identify individuals through fingerprints, iris patterns, voice recognition, and facial features. These systems assist law enforcement agencies in suspect identification, identity verification, and criminal tracking. Technologies such as automated fingerprint identification systems are widely used in criminal

investigations and security operations. In India, initiatives such as the National Automated Fingerprint Identification System (NAFIS) demonstrate the growing use of biometric technologies in policing.

4) Data Analytics and Digital Evidence Examination

AI-driven data analytics and digital forensic tools play a major role in examining electronic evidence such as emails, mobile phone records, social media content, and financial transactions. AI technologies help investigators analyse large volumes of digital data, detect suspicious activities, recover deleted files, and identify criminal networks. These tools are especially useful in cybercrime, terrorism, financial fraud, and money laundering investigations. AI-based digital evidence examination improves investigative speed and accuracy by reducing human effort and identifying hidden connections within large datasets.

5) Automated Decision-Making Tools

Automated decision-making tools use AI algorithms to assist law enforcement agencies in suspect prioritization, risk assessment, threat analysis, and resource allocation. Certain jurisdictions also use AI systems in bail decisions, sentencing recommendations, and parole evaluations. These systems improve efficiency by processing complex information rapidly and supporting investigative decision-making.

TRANSPARENCY ISSUES IN AI BASED CRIMINAL INVESTIGATIONS

The increasing use of Artificial Intelligence in criminal investigations has improved the efficiency of law enforcement agencies by enabling faster data analysis, suspect identification, and evidence examination. However, the growing dependence on AI technologies has also raised serious concerns regarding transparency. Many AI systems operate through complex algorithms and machine learning models that are difficult to understand, even for authorities using them. This

lack of transparency creates challenges in assessing the fairness, reliability, and legality of AI-generated outcomes. When AI systems are used for suspect identification, predictive policing, and evidence analysis, investigators, judges, lawyers, and accused persons may struggle to understand or challenge algorithmic decisions. Such opacity may undermine due process and reduce public trust in criminal justice systems.

a) Algorithmic Opacity and “Black Box” Systems

Algorithmic opacity refers to the inability to clearly understand how AI systems process information and produce decisions. Many AI technologies used in criminal investigations function as “black box” systems, where the internal decision-making process remains hidden or difficult to interpret. For example, facial recognition systems may identify suspects without clearly explaining how the identification was made or why a particular individual was matched with a criminal database. This lack of transparency creates serious legal and ethical concerns because accused persons may be unable to effectively challenge AI-generated conclusions. Judges and legal professionals may also lack the technical expertise required to assess complex algorithms. Furthermore, private technology companies often protect AI source codes as trade secrets, limiting independent scrutiny. Opaque systems may additionally conceal algorithmic biases and errors, leading to wrongful identification, discriminatory policing, and unequal treatment under the law.

b) Lack of Explainability in AI Decisions

Explainability refers to the ability of AI systems to provide understandable reasons for their decisions and outputs. In criminal investigations, explainability is essential because investigative decisions directly affect the liberty, dignity, and constitutional rights of individuals. However, many AI systems based on machine learning and deep learning technologies cannot clearly explain how conclusions are reached. The lack of explainability undermines due process

because accused persons may not know the basis of allegations or investigative findings against them. It also weakens accountability, as investigators may rely on algorithmic outputs without understanding their reliability or fairness. Courts may face difficulties in assessing the credibility and admissibility of AI-generated evidence, while the public may become sceptical of AI-driven investigations. To address these concerns, experts have emphasized the importance of “Explainable AI” (XAI), which aims to make AI systems more transparent and understandable.

c) Challenges in Verification and Reliability of AI Evidence

AI-generated evidence raises important concerns regarding accuracy, verification, and reliability in criminal investigations. AI systems are increasingly used to analyse CCTV footage, identify suspects, examine digital evidence, and generate predictive assessments. However, flawed algorithms, biased datasets, or inaccurate data inputs may produce incorrect results, false identifications, and wrongful conclusions. Verification of AI-generated evidence becomes difficult because many AI systems operate through proprietary and confidential software, limiting access for courts and defence lawyers. Reliability issues also arise because machine learning systems continuously evolve, making it difficult to ensure consistency and reproducibility of outcomes.

ACCOUNTABILITY CONCERNS IN THE USE OF AI

The increasing use of Artificial Intelligence in criminal investigations has created important accountability concerns within modern criminal justice systems. Although AI technologies improve investigative efficiency and assist in crime detection, their growing influence over investigative decisions raises questions regarding responsibility, fairness, and legal oversight. Since criminal investigations directly affect individual liberty and constitutional rights, accountability remains an essential principle of justice.

a) Algorithmic Bias and Discrimination

Algorithmic bias is one of the most serious accountability concerns associated with AI in criminal investigations. AI systems depend on the quality and neutrality of the datasets used for training. If biased or discriminatory data is used, AI systems may produce unfair outcomes based on race, ethnicity, gender, religion, or socio-economic background. Predictive policing systems, for example, may disproportionately target communities that have historically experienced excessive policing. Facial recognition technologies have also been criticized for producing inaccurate results, particularly in identifying women and minority groups, thereby increasing the risk of wrongful arrests and discriminatory treatment. Since algorithmic decisions often appear objective and scientific, law enforcement agencies may rely on them without recognizing hidden biases.

b) Wrongful Identification and Investigative Errors

AI technologies used in criminal investigations may result in wrongful identification and investigative errors due to technical limitations, inaccurate data, or algorithmic flaws. Facial recognition systems and biometric technologies may incorrectly identify innocent individuals because of poor image quality, database inaccuracies, or biased algorithms. Similarly, predictive policing systems may wrongly classify individuals or communities as high-risk, resulting in harassment, reputational damage, and unfair suspicion. Another major concern is “automation bias,” where investigators excessively rely on AI-generated outputs without independently verifying their accuracy. Such overreliance may weaken human judgment and increase the possibility of wrongful arrests and miscarriages of justice.

c) Responsibility of Law Enforcement Agencies and Developers

The use of AI in criminal investigations creates complex questions regarding legal

responsibility and liability. When AI systems produce harmful or discriminatory outcomes, accountability may involve multiple parties, including law enforcement agencies, government authorities, software developers, and private technology companies. Law enforcement agencies remain primarily responsible for ensuring that AI technologies are used lawfully, fairly, and ethically. Authorities cannot avoid accountability by claiming that decisions were made by automated systems. Similarly, developers and private companies are responsible for designing reliable, transparent, and unbiased AI systems. However, assigning liability becomes difficult because AI systems continuously evolve through machine learning processes, and companies often protect algorithms as trade secrets.

d) Ethical Concerns in AI Deployment

The deployment of AI in criminal investigations raises several ethical concerns relating to privacy, fairness, human dignity, and democratic freedoms. AI-powered surveillance systems, facial recognition technologies, and biometric databases enable continuous monitoring of individuals, which may lead to mass surveillance and invasion of privacy. Excessive monitoring without adequate safeguards may restrict personal liberty and create fear within society. Ethical concerns also arise from discriminatory outcomes, overreliance on automated decision-making, and misuse of surveillance technologies by authorities. AI systems may reinforce social inequalities if biased datasets are used, while excessive dependence on algorithmic decisions may reduce human judgment and empathy in criminal justice processes. Furthermore, AI technologies may be misused for political monitoring or suppression of dissent if proper safeguards are absent.

6. DUE PROCESS AND CONSTITUTIONAL CHALLENGES

The increasing use of Artificial Intelligence in criminal investigations has created important constitutional and due

process challenges within modern legal systems. Although AI technologies improve investigative efficiency and assist in crime detection and prevention, their growing role in policing and decision-making raises concerns regarding the protection of fundamental rights and liberties. Since criminal investigations directly affect individual freedom, dignity, and reputation, AI-based systems must operate in accordance with constitutional principles, procedural fairness, and human rights standards.

a) Right to Privacy and Surveillance Concerns

AI-powered surveillance technologies raise serious concerns regarding the right to privacy, which has been recognized as a fundamental right under Article 21 of the Constitution of India in *Justice K.S. Puttaswamy v. Union of India*. AI systems enable law enforcement agencies to collect and analyse large amounts of personal data through facial recognition systems, biometric databases, CCTV networks, and digital surveillance tools. Facial recognition and biometric surveillance technologies may identify and monitor individuals without their knowledge or consent, thereby creating risks of mass surveillance, privacy violations, and misuse of sensitive information. Continuous monitoring may also affect freedom of movement, expression, and association. In the absence of comprehensive legal safeguards, unrestricted AI surveillance may lead to arbitrary state action and excessive intrusion into private life, making privacy protection one of the most significant constitutional challenges in AI-based investigations.

b) Right to Fair Trial and Procedural Fairness

The right to a fair trial is a fundamental principle of due process that ensures individuals are treated fairly and given equal opportunity to defend themselves. However, AI technologies used in criminal investigations may undermine procedural fairness due to lack of transparency and explainability in algorithmic decision-making. Many AI systems function as black box

models, making it difficult for accused persons, lawyers, and judges to understand how conclusions are reached. Proprietary AI systems developed by private companies often restrict access to algorithms and technical details, limiting independent examination of AI-generated evidence. Additionally, automation bias may cause investigators and judges to rely excessively on algorithmic outputs without properly questioning their limitations.

c) Presumption of Innocence and Automated Profiling

The presumption of innocence guarantees that every individual is considered innocent until proven guilty before a court of law. However, predictive policing systems and automated profiling technologies may threaten this principle by identifying individuals as potential offenders based on data analysis and behavioural predictions rather than actual criminal conduct. AI-driven predictive systems analyse historical crime data, social behaviour, and geographic patterns to identify “high-risk” individuals or areas. Such technologies may result in persons being monitored or targeted without sufficient evidence, thereby creating suspicion based on speculative assessments. Biased datasets may also disproportionately target marginalized communities, leading to discrimination and unequal treatment.

d) Human Rights Implications of AI-Based Investigations

The use of AI in criminal investigations has broader human rights implications relating to equality, dignity, liberty, freedom of expression, and protection against discrimination. Biased AI systems may disproportionately target marginalized communities based on race, ethnicity, gender, religion, or socio-economic background, thereby violating principles of equality and non-discrimination. AI-powered surveillance technologies may also create a chilling effect on democratic freedoms because individuals who are constantly monitored may hesitate to participate in protests, political activities, or public discussions. Excessive

reliance on automated systems may further reduce human involvement in decisions affecting liberty and justice. Additionally, governments may misuse AI technologies for political surveillance, suppression of dissent, or arbitrary state control. Therefore, AI deployment in criminal investigations must be guided by principles of transparency, accountability, proportionality, fairness, and human rights protection to ensure compliance with constitutional and international legal standards.

INDIAN LEGAL FRAMEWORK GOVERNING AI AND CRIMINAL INVESTIGATIONS

India does not presently have a comprehensive legislation specifically regulating Artificial Intelligence in criminal investigations. However, several constitutional provisions, statutory laws, judicial decisions, and governmental initiatives indirectly govern the use of AI technologies within policing and criminal justice systems.

The Constitution of India provides important safeguards relevant to AI-based investigations. Article 14 guarantees equality before law and protection against arbitrary state action, while Article 21 protects the right to life and personal liberty, including the right to privacy recognized in *Justice K.S. Puttaswamy v. Union of India*. Any use of AI technologies by law enforcement agencies must therefore comply with constitutional principles of fairness, proportionality, and due process.

The primary procedural laws governing criminal investigations in India include the Bharatiya Nagarik Suraksha Sanhita, 2023 and the Bharatiya Sakshya Adhiniyam, 2023. These laws regulate investigation procedures, admissibility of electronic evidence, and evidentiary standards relevant to AI-generated materials. Electronic records, digital evidence, and forensic reports generated through AI technologies may be admissible subject to statutory requirements regarding authenticity and reliability.

The Information Technology Act, 2000 also plays a significant role in regulating digital evidence, cybercrime investigations, electronic records, and data-related offences. Provisions relating to data security, unauthorized access, and cyber offences indirectly affect AI-assisted criminal investigations, particularly in cases involving cybercrime and digital surveillance. The enactment of the Digital Personal Data Protection Act, 2023 represents an important step toward data protection and privacy regulation.

India has also introduced technological initiatives such as the Crime and Criminal Tracking Network and Systems (CCTNS), the National Automated Fingerprint Identification System (NAFIS), and facial recognition projects to modernize policing and criminal investigation mechanisms. These initiatives reflect increasing governmental reliance on AI-driven technologies for law enforcement and public security purposes.

However, significant regulatory gaps continue to exist. India currently lacks a dedicated AI governance law establishing standards for transparency, accountability, algorithmic fairness, and oversight in criminal investigations.

INTERNATIONAL FRAMEWORK ON AI AND CRIMINAL INVESTIGATION

The European Union has emerged as one of the leading jurisdictions in AI regulation. The EU has proposed comprehensive AI governance measures emphasizing human rights, transparency, and risk-based regulation. Under the EU approach, certain high-risk AI systems used in law enforcement and criminal justice are subject to strict regulatory obligations, including transparency requirements, human oversight, and conformity assessments. The EU has also imposed significant restrictions on real-time biometric surveillance and facial recognition technologies in public spaces.

The United States follows a comparatively decentralized approach toward

AI regulation. Various federal and state authorities have adopted differing standards relating to facial recognition technologies, predictive policing, and surveillance systems. Some states and cities have restricted or banned facial recognition technologies due to concerns regarding privacy and racial discrimination, while others continue to permit extensive law enforcement use of AI systems.

The United Kingdom has increasingly utilized AI-driven surveillance and facial recognition technologies within policing systems. However, British courts and regulatory authorities have emphasized the need for proportionality, legality, and protection of privacy rights. Public debates continue regarding the ethical implications of AI surveillance technologies and automated policing systems.

Countries such as China have adopted extensive AI-based surveillance systems involving facial recognition, biometric monitoring, and large-scale public surveillance networks. While these technologies are promoted for public security and social stability, they have attracted criticism from international human rights organizations regarding mass surveillance and suppression of civil liberties.

NEED FOR REGULATORY REFORMS AND SAFEGAUARDS

The increasing use of Artificial Intelligence in criminal investigations has improved policing, surveillance, crime detection, and evidence analysis. Technologies such as facial recognition systems, predictive policing, biometric surveillance, and automated decision-making tools have enhanced investigative efficiency and public security. However, the rapid expansion of AI has also created serious concerns relating to privacy violations, algorithmic bias, lack of transparency, wrongful identification, and threats to due process and constitutional rights. In the absence of comprehensive legal regulation, AI systems may lead to misuse of surveillance powers,

discriminatory practices, and excessive state control.

Therefore, strong regulatory reforms and safeguards are necessary to ensure the ethical and accountable use of AI in criminal investigations. Legal frameworks should ensure transparency, explainability, accountability, human oversight, and protection of fundamental rights. Independent audits, judicial oversight, data protection measures, and mechanisms to challenge AI-generated decisions must also be established. At the same time, AI governance should balance technological advancement with democratic values, privacy, equality, and procedural fairness so that AI strengthens criminal justice systems without undermining constitutional freedoms and human rights.

SUGGESTIONS AND RECOMMENDATIONS

1) Enactment of Comprehensive AI Legislation –

India should introduce a comprehensive legal framework regulating the use of AI in criminal investigations. The law should define permissible uses of AI technologies and establish safeguards relating to transparency, accountability, privacy, and due process.

2) Establishment of Independent Oversight Mechanisms –

Independent oversight bodies comprising judicial authorities, data protection agencies, and technical experts should monitor the use of AI systems. Regular audits and reviews are necessary to ensure fairness, accuracy, and compliance with legal standards.

3) Ensuring Transparency and Explainability –

AI systems used in criminal investigations should provide clear and understandable explanations for their decisions. Transparency is essential to allow judicial scrutiny and enable individuals to challenge AI-generated conclusions.

4) Mandatory Human Oversight –

AI technologies should assist rather than replace human decision-making. Critical decisions relating to arrest, detention, surveillance, and prosecution must remain subject to meaningful human supervision and verification.

5) Prevention of Algorithmic Bias and Discrimination – AI systems should be trained using fair and representative datasets to prevent discriminatory outcomes. Regular testing and auditing are necessary to identify and eliminate algorithmic bias in policing and surveillance systems.

6) Strengthening Data Protection and Privacy Safeguards – Strong privacy and data protection measures should regulate the collection, storage, and use of personal information. Surveillance practices must follow principles of legality, necessity, and proportionality.

7) Development of Ethical AI Guidelines – Governments and law enforcement agencies should adopt ethical AI frameworks based on fairness, accountability, transparency, and respect for human rights. AI should not be used for arbitrary surveillance or discriminatory practices.

8) Capacity Building and Technical Training – Judges, police officers, prosecutors, and legal professionals should receive technical training regarding AI technologies and AI-generated evidence. This would improve institutional competence and judicial evaluation of automated systems.

9) Judicial Guidelines for AI-Based Evidence – Courts should establish clear standards regarding the admissibility, reliability, and verification of AI-generated evidence. Judicial oversight is necessary to protect due process and prevent wrongful convictions.

10) International Cooperation and Comparative Learning – India should study international approaches and adopt global best practices relating to ethical AI governance, privacy protection, and accountability in criminal investigations.

11) Public Participation and Democratic Accountability – Governments should promote public awareness and encourage democratic discussions regarding AI deployment in policing

and criminal justice systems. Public participation would improve transparency and public trust.

12) Balancing Security and Fundamental Rights

– While AI technologies strengthen crime prevention and public safety, regulatory frameworks must balance technological advancement with protection of privacy, equality, liberty, and procedural fairness. AI should function as a supportive tool for justice rather than a means of unchecked surveillance or arbitrary state power.

CONCLUSION

AI based technologies enable law enforcement agencies to process vast amounts of data efficiently and enhance investigative accuracy and public security. However, despite these advantages, the increasing use of AI has also raised serious legal, ethical, and constitutional concerns relating to transparency, algorithmic bias, wrongful identification, privacy violations, surveillance misuse, and reliability of AI-generated evidence. Excessive dependence on opaque AI systems may undermine due process, procedural fairness, presumption of innocence, and other fundamental rights guaranteed under constitutional and human rights frameworks. The study highlights that, particularly in India, the absence of comprehensive AI-specific legal regulation and accountability mechanisms creates significant risks within criminal justice administration. Therefore, while AI has the potential to strengthen criminal investigations and public safety, its use must remain subject to transparency, human oversight, accountability, ethical governance, and protection of fundamental rights. A balanced and rights-oriented regulatory framework is essential to ensure that Artificial Intelligence functions as a supportive tool for justice rather than an instrument of arbitrary surveillance or discrimination, thereby upholding the principles of fairness, rule of law, and constitutional governance in the digital age.

REFERENCES

- 1) Danielle Keats Citron and Frank Pasquale, "The Scored Society," (2014) Washington Law Review Vol. 89.
- 2) Sandra Wachter, Brent Mittelstadt & Luciano Floridi, "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation," (2017) International Data Privacy Law Vol. 7.
- 3) Ryan Calo, "Artificial Intelligence Policy: A Primer and Roadmap," (2017) University of California Davis Law Review Vol. 51.
- 4) Aziz Huq, "Racial Equity in Algorithmic Criminal Justice," (2019) Duke Law Journal Vol. 68.

Indian Legislations

- 1) Constitution of India.
- 2) Information Technology Act, 2000.
- 3) Digital Personal Data Protection Act, 2023.
- 4) Bharatiya Nagarik Suraksha Sanhita, 2023.
- 5) Bharatiya Sakshya Adhiniyam, 2023.

Case laws

- 1) Justice K.S. Puttaswamy v. Union of India.
- 2) Selvi v. State of Karnataka.
- 3) Carpenter v. United States.
- 4) Bridges v. South Wales Police

Reports and International Documents

- 1) UNESCO, Recommendation on the Ethics of Artificial Intelligence (2021).
- 3) European Union, Artificial Intelligence Act (Proposed Regulation).
- 4) NITI Aayog, National Strategy for Artificial Intelligence (2018).
- 5) United Nations, Guidance on Human Rights and Artificial Intelligence.
- 6) National Crime Records Bureau, reports on Crime and Criminal Tracking Network and Systems (CCTNS).