Canadian Journal of Marketing Research
ISSN: 0829-4836
https://canadian-jmr.com/index.php/cjmr

Research Article

Artificial Intelligence in Modern Criminal Forensics in India: Opportunities and Challenges

Mohd. Faizan Khan[1*], Dr. Sunita Sharma[2] and Ms. Riya Khurana[3]
[1,2]Academician of Law, DPG Law College, Affiliated to Maharishi Dayanand University, Rohtak, Haryana, India
[3]Assistant Professor of Law, DPG Law College, Affiliated to Maharishi Dayanand University, Rohtak, Haryana, India

***Corresponding Author**
Faizan Khan

Article History
Received: 21.08.2026
Accepted: 16.09.2026
Published: 10.10.2026

DOI: 10.61336/cjmr.1604.06

Abstract: Artificial Intelligence (AI) is rapidly transforming the field of criminal forensics in India by enhancing the efficiency, speed and accuracy of criminal investigations. AI-powered technologies such as facial recognition systems, predictive analytics, biometric identification, digital surveillance and machine learning algorithms are increasingly being used by investigative agencies to analyse evidence, identify suspects and detect criminal patterns. In the context of rising cybercrimes, organized crimes and digital offences, AI has emerged as a significant tool for modernizing forensic science and strengthening the criminal justice system. Despite its advantages, the use of AI in criminal forensics also raises several legal, ethical and constitutional concerns. Issues relating to privacy, data protection, algorithmic bias, lack of transparency and reliability of AI-generated evidence pose serious challenges to the Indian legal framework. The absence of comprehensive legislation regulating AI usage in criminal investigations further creates uncertainty regarding accountability and admissibility of AI-based evidence in courts. Additionally, overdependence on automated systems may threaten fundamental rights and procedural fairness if proper safeguards are not implemented. This paper critically examines the opportunities and challenges associated with the application of AI in modern criminal forensics in India. It explores the technological advancements, their impact on forensic investigations and the need for a balanced legal and regulatory framework that ensures both effective crime detection and protection of individual rights in a society.

Keywords: Artificial Intelligence (AI), Criminal Forensics, Digital Evidence, Cybercrime Investigation, Indian Criminal Justice System

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 for non-commercial use (NonCommercial, or CC-BY-NC) provided the original author and source are credited.

INTRODUCTION

The rapid advancement of Artificial Intelligence (AI) has transformed the methods through which criminal investigations are conducted across the world. Traditionally, criminal forensics relied upon human expertise, manual examination of evidence and conventional investigative techniques. However, the increasing volume of digital data, the rise of cybercrime and the growing sophistication of criminal activities have necessitated the adoption of advanced technological tools capable of assisting law enforcement agencies in detecting, preventing and investigating offences more effectively. In this context, Artificial Intelligence has emerged as a significant force in modern criminal forensics.

AI technologies are increasingly being deployed in forensic investigations through facial recognition systems, biometric identification tools, predictive analytics, machine learning algorithms, digital surveillance systems and automated evidence analysis. These technologies enable investigators to process vast quantities of information within a short period, identify hidden patterns, link criminal activities across jurisdictions and generate actionable intelligence. As a result, AI has the potential to significantly enhance the efficiency, speed and accuracy of criminal investigations while reducing the burden on investigative agencies.

The importance of AI-assisted forensic investigation has become particularly evident in the digital age. Contemporary crimes frequently involve electronic devices, social media platforms, encrypted communications, financial transactions and other forms of digital evidence. Traditional investigative methods often struggle to cope with the scale and complexity of such information. AI-powered systems can analyse digital evidence, identify suspicious behavioural patterns, detect cyber threats and assist investigators in uncovering critical links that may otherwise remain unnoticed. Consequently, AI has become an increasingly valuable tool in combating cybercrime, financial fraud, organized crime, terrorism and other technologically sophisticated offences.

Despite these advantages, the growing reliance on AI within criminal forensics raises significant legal, ethical and constitutional concerns. AI systems are not infallible. Errors in algorithmic processing, biased training datasets, inaccurate facial recognition matches and opaque decision-making processes may produce outcomes that adversely affect individuals. The deployment of AI-driven surveillance and investigative tools also raises concerns regarding privacy, data protection and the potential misuse of personal information. Furthermore, excessive reliance on automated systems may undermine procedural fairness if human oversight is diminished.

The constitutional implications of AI-assisted criminal investigations are particularly significant in India. The right to privacy recognized by the Supreme Court in Justice K.S. Puttaswamy v Union of India has established important safeguards against arbitrary state intrusion into personal liberty. Simultaneously, criminal investigations must remain consistent with principles of due process, fairness and the rule of law. The increasing use of AI-generated evidence therefore raises important questions concerning reliability, transparency, accountability and admissibility before courts of law.

The legal framework governing AI in criminal forensics remains fragmented. While statutes such as the Bharatiya Sakshya Adhiniyam [1] provide rules relating to electronic evidence, India does not yet possess a comprehensive legislative framework specifically regulating the use of AI technologies in criminal investigations. Consequently, uncertainty persists regarding standards of reliability, evidentiary value, accountability and judicial scrutiny of AI-assisted forensic tools.

Against this backdrop, this paper critically examines the opportunities and challenges associated with the application of Artificial Intelligence in modern criminal forensics in India. It analyses the technological advancements transforming forensic investigations, evaluates the constitutional and legal concerns arising from their use and explores the evidentiary implications of AI-generated information. The paper argues that while AI possesses immense potential to strengthen criminal investigations and improve forensic efficiency, its deployment must be accompanied by appropriate legal safeguards, transparency requirements and institutional oversight mechanisms capable of protecting individual rights and preserving public confidence in the criminal justice system.

The discussion proceeds in seven parts. The next section introduces the conceptual foundations of AI-driven criminal forensics and examines the principal technologies currently used in investigative processes. The paper then analyses the opportunities created by AI-assisted investigations before evaluating the constitutional, ethical and legal challenges associated with their deployment. Subsequently, it explores the admissibility of AI-generated evidence under Indian law, examines comparative international approaches and proposes a balanced regulatory framework for India. The paper concludes by emphasizing the need to harmonize technological innovation with constitutional values in the administration of criminal justice.

Research Problem

The integration of Artificial Intelligence (AI) into criminal forensic investigations has significantly transformed the manner in which crimes are detected, investigated and prosecuted in India. AI-enabled technologies such as facial recognition, biometric identification, predictive policing, automated digital evidence analysis and machine learning algorithms have substantially enhanced investigative efficiency and forensic accuracy. With the rapid increase in cybercrimes, financial frauds, digital offences and technologically sophisticated criminal activities, investigative agencies increasingly rely upon AI-driven forensic tools to process vast quantities of electronic evidence and identify complex criminal patterns. While these technological advancements strengthen law enforcement capabilities, they simultaneously raise significant concerns regarding privacy, procedural fairness, transparency, accountability and the admissibility of AI-generated evidence within the criminal justice system.

The enactment of the Bharatiya Nyaya Sanhita [2], Bharatiya Nagarik Suraksha Sanhita [3], Bharatiya Sakshya Adhiniyam [1] and the Digital Personal Data Protection Act [4] has substantially altered India's criminal justice and digital governance framework. The BSA recognizes electronic and digital evidence as an integral component of judicial proceedings, while the DPDP Act introduces principles governing the processing and protection of personal data. Nevertheless, these legislations do not comprehensively regulate the deployment of Artificial Intelligence in criminal investigations or prescribe uniform standards relating to algorithmic transparency, explainability, accountability, judicial scrutiny, or evidentiary reliability. Consequently, the legal status of AI-generated forensic evidence and the constitutional safeguards governing its use remain uncertain.

In light of these developments, there exists an urgent need to critically examine whether the existing legal framework adequately balances technological innovation with constitutional guarantees under Articles 14, 19 and 21 of the Constitution of India. The increasing dependence on AI-assisted criminal investigations demands a coherent legal and regulatory framework capable of ensuring transparency, fairness, human oversight and protection of fundamental rights while preserving the efficiency and effectiveness of modern forensic science. This study therefore seeks to evaluate the opportunities and challenges presented by AI in criminal forensics and proposes a balanced governance framework suitable for India's evolving criminal justice system.

Review of Literature

Babuta *et al*. [5], examine the growing use of machine learning algorithms in police decision-making and analyse the legal, ethical and regulatory issues arising from their deployment. The report discusses how AI-assisted policing enhances investigative efficiency through predictive analytics and data-driven decision-making while simultaneously raising concerns relating to transparency, accountability, algorithmic bias and protection of fundamental rights. Desai and Ambali [6] the authors emphasize that AI should function as a decision-support tool rather than replace human judgment, advocating robust oversight and regulatory safeguards. The report provides an important foundation for understanding the governance challenges associated with AI in law enforcement. However, its primary focus remains on policing models in the United Kingdom and does not examine the implications of India's evolving criminal justice framework under the Bharatiya Nyaya Sanhita, Bharatiya Nagarik Suraksha Sanhita, Bharatiya Sakshya Adhiniyam and the Digital Personal Data Protection Act. Hidayat and Anwar [7] the present study extends this discussion by analysing AI within the contemporary Indian legal framework.

Casey [8] provides one of the most comprehensive analyses of digital evidence and computer forensics, explaining the scientific principles governing the identification, collection, preservation and presentation of electronic evidence. The author highlights the importance of maintaining the integrity, authenticity and reliability of digital evidence while discussing practical forensic techniques used in cybercrime investigations and criminal proceedings. Although the book remains a leading authority on digital forensic science, it predates the widespread integration of Artificial Intelligence into criminal investigations. Desai [9] consequently, it does not address contemporary legal questions concerning AI-generated evidence, algorithmic decision-making, explainability, or the evidentiary implications arising under India's newly enacted criminal laws. This study builds upon Casey's foundational principles while examining the legal challenges posed by AI-assisted forensic technologies.

Ferguson [10] critically analyses predictive policing technologies and their impact on contemporary criminal justice systems. He argues that while predictive policing may improve resource allocation and crime prevention, excessive reliance on algorithmic decision-making risks reinforcing existing social inequalities, discriminatory policing practices and constitutional concerns relating to due process and privacy. Ferguson advocates greater transparency and judicial oversight over predictive policing systems. Rajput [11] the article significantly contributes to the debate surrounding AI-assisted policing but primarily evaluates predictive policing within the United States legal system. It does not analyse the admissibility of AI-generated evidence or the implications of India's recent legislative reforms governing digital evidence and criminal investigations. The present research addresses this gap by evaluating predictive AI within the Indian constitutional and statutory framework.

Garvie *et al*. [12] examine the increasing use of facial recognition technology by law enforcement agencies in the United States and highlight the absence of adequate legal regulation governing its deployment. The report discusses issues of privacy, racial bias, wrongful identification and the lack of transparency associated with facial recognition systems. It argues that unrestricted use of such technologies may undermine constitutional rights and procedural fairness. The report provides valuable insights into the risks associated with AI-powered biometric surveillance. However, its analysis is confined to the American legal landscape and does not consider India's constitutional jurisprudence on privacy or recent statutory developments such as the DPDP Act, 2023 and Bharatiya Sakshya Adhiniyam, 2023. This research expands the discussion by examining similar concerns within the Indian legal context.

Goodfellow *et al.* [13] present a comprehensive explanation of deep learning and modern machine learning techniques that constitute the technological foundation of contemporary Artificial Intelligence systems. The book explains neural networks, pattern recognition, data training methodologies and the functioning of AI algorithms that are widely employed in facial recognition, speech recognition, predictive analytics and image processing. While the book provides an authoritative technical understanding of AI systems, it does not examine their legal, ethical, or constitutional implications within criminal investigations. The present study utilizes these technological concepts as a basis for analysing the evidentiary, constitutional and regulatory challenges associated with AI-assisted criminal forensics in India.

NITI Aayog [14] the National Strategy for Artificial Intelligence prepared by NITI Aayog outlines India's vision for promoting responsible AI across various sectors including healthcare, education, agriculture, governance and public administration. The report emphasizes ethical AI, transparency, accountability, capacity building and innovation while

encouraging the development of a robust regulatory ecosystem capable of supporting responsible AI adoption. Although the strategy acknowledges the importance of ethical governance, it provides limited discussion regarding AI deployment in criminal investigations and forensic science. It also predates India's recent criminal law reforms and the enactment of the Digital Personal Data Protection Act, 2023. The present research therefore evaluates how these subsequent legislative developments influence AI-assisted criminal investigations.

Oswald *et al.* [15] examine algorithmic risk assessment models employed in policing within the United Kingdom and analyse their implications for transparency, accountability, legality and public confidence. The authors argue that while AI-based risk assessment tools may improve investigative efficiency, their deployment requires clear legal standards, human oversight and mechanisms capable of preventing discriminatory or arbitrary outcomes. The study contributes significantly to discussions on responsible AI governance in policing. However, its analysis is limited to British policing practices and does not evaluate the evidentiary treatment of AI-generated material under Indian criminal law. This study extends those principles to India's legal system, particularly considering the BSA, BNSS, BNS and DPDP Act.

Russell and Norvig [16] provide one of the most authoritative and comprehensive works on Artificial Intelligence, covering machine learning, reasoning, knowledge representation, robotics, natural language processing and intelligent decision-making systems. The book explains the theoretical foundations and practical applications of AI technologies across multiple sectors. Although it offers an excellent conceptual understanding of AI, the book does not focus on the legal regulation of AI in criminal justice or the admissibility of AI-generated evidence. The present study builds upon these technological concepts to critically evaluate their implications within India's constitutional and criminal justice framework.

Research Questions:

- What role does Artificial Intelligence play in modern criminal forensic investigations in India?
- Whether the existing legal framework, including the BSA, BNSS, BNS, DPDP Act and Information Technology Act, adequately regulates the use of AI in criminal forensics?
- What are the principal constitutional, legal and ethical challenges arising from the use of AI-generated evidence in criminal investigations?
- What regulatory framework can effectively balance technological innovation, investigative efficiency and protection of fundamental rights in AI-assisted criminal investigations in India?

Research Objectives:

- To examine the application of Artificial Intelligence in modern criminal forensic investigations in India
- To analyse the legal framework governing AI-assisted criminal investigations with reference to the Constitution of India, BSA, BNSS, BNS, DPDP Act and the Information Technology Act
- To evaluate the constitutional, legal, ethical and evidentiary challenges associated with AI-generated evidence in criminal proceedings

To propose a balanced legal and regulatory framework for the responsible use of Artificial Intelligence in criminal forensics while ensuring transparency, accountability and protection of fundamental rights.

Research Methodology

The present study adopts a doctrinal research methodology, as it primarily examines the existing legal framework governing the use of Artificial Intelligence in criminal forensics in India. The research is analytical and descriptive in nature, focusing on the interpretation of statutory provisions, constitutional principles, judicial precedents and legal doctrines relating to AI-assisted criminal investigations, digital evidence, privacy and procedural fairness. The study also undertakes a comparative examination of selected international regulatory approaches to understand emerging global standards concerning Artificial Intelligence in criminal justice.

The research relies upon both primary and secondary sources. The primary sources include the Constitution of India, 1950, the Bharatiya Nyaya Sanhita [2], the Bharatiya Nagarik Suraksha Sanhita [3], the Bharatiya Sakshya Adhiniyam [1] the Digital Personal Data Protection Act [4], the Information Technology Act [17], relevant subordinate legislation and judicial decisions of the Supreme Court and various High Courts concerning electronic evidence, privacy, digital surveillance and constitutional rights. Important judicial precedents such as *Justice K.S. Puttaswamy v. Union of India*, *Anvar P.V. v. P.K. Basheer*, *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* and other relevant cases have been examined to analyse the evolving judicial approach toward digital and AI-assisted evidence.

The secondary sources comprise books, peer-reviewed journal articles, research papers, law commission reports, government publications, policy papers issued by NITI Aayog, reports of international organizations such as the OECD, UNESCO and the United Nations Office on Drugs and Crime (UNODC), as well as comparative legal literature on Artificial

Intelligence and criminal justice. These sources have been critically analysed to identify prevailing legal debates, research gaps and emerging best practices, thereby enabling the formulation of recommendations for an effective legal framework governing AI-assisted criminal forensics in India.

Artificial Intelligence and Criminal Forensics: Conceptual Foundations

Understanding Artificial Intelligence in Criminal Investigations: Artificial Intelligence refers to computational systems capable of performing tasks that traditionally require human intelligence, including pattern recognition, data analysis, prediction, reasoning and decision-making. Modern AI technologies are primarily driven by machine learning algorithms that can analyse vast quantities of information, identify relationships within datasets and generate outcomes based on learned patterns. Unlike conventional software systems that operate according to predetermined instructions, AI systems possess the ability to adapt and improve their performance through exposure to new data.

Within the criminal justice system, AI has emerged as an important tool for assisting law enforcement agencies and forensic experts in the investigation and detection of crime. The growing complexity of criminal activities, coupled with the exponential increase in digital information, has created significant challenges for traditional investigative methods. AI technologies offer the ability to process large volumes of evidence efficiently, detect hidden connections and support investigative decision-making in ways that would be difficult through manual analysis alone.

The integration of AI into criminal investigations represents a broader transformation in forensic science. Contemporary investigations increasingly involve digital evidence obtained from mobile devices, surveillance cameras, social media platforms, financial records and communication networks. AI-powered systems assist investigators by organizing, analysing and interpreting this information, thereby enhancing investigative efficiency and accuracy.

Major AI Technologies Used in Criminal Forensics

Several AI-based technologies are currently employed within modern forensic investigations:

- **Facial Recognition Systems:** Facial recognition technology is among the most widely discussed applications of AI in criminal investigations. These systems analyse facial features and compare them against existing databases to identify individuals or verify identities. Law enforcement agencies increasingly use facial recognition for suspect identification, locating missing persons and analysing surveillance footage. The technology significantly reduces the time required to examine large quantities of visual evidence
- **Biometric Identification:** Biometric systems use unique physiological characteristics such as fingerprints, iris patterns, facial structures and voice samples for identification purposes. AI enhances the accuracy and speed of biometric analysis by enabling automated matching and verification processes. Such technologies have become valuable tools in criminal investigations where rapid identification of suspects is required
- **Predictive Analytics and Crime Mapping:** Predictive policing systems employ machine learning algorithms to analyse historical crime data and identify patterns that may indicate future criminal activity. By examining geographical trends, behavioural indicators and previous incidents, these systems seek to assist law enforcement agencies in allocating resources more effectively. Although predictive analytics may improve efficiency, concerns remain regarding bias and fairness in algorithmic decision-making
- **Digital Evidence Analysis:** Modern criminal investigations frequently involve large volumes of electronic data. AI-powered forensic tools can examine emails, financial records, mobile phone data, internet activity, social media communications and digital documents to identify relevant evidence. Such technologies are particularly important in investigations involving cybercrime, financial fraud, organized crime and terrorism
- **Video Analytics and Surveillance Systems:** AI-driven video analytics enable investigators to process surveillance footage more efficiently. These systems can detect unusual behaviour, track movements, identify objects and recognize individuals across multiple video sources. Given the widespread use of CCTV infrastructure in urban areas, AI-assisted video analysis has become an increasingly significant component of contemporary forensic investigations

Emerging Trends in India

India has witnessed growing adoption of AI technologies within law enforcement and forensic institutions. Digital policing initiatives, smart surveillance systems, biometric databases and cybercrime investigation units increasingly rely upon technological tools to enhance investigative capabilities. The expansion of digital governance and smart city projects has further increased the availability of data that may be utilized in criminal investigations.

The rise of cybercrime has also accelerated the demand for advanced forensic technologies. Offences involving online fraud, identity theft, ransomware attacks, cryptocurrency-related crimes and digital financial fraud often generate vast quantities of electronic evidence. AI-assisted investigative tools provide important support in analysing such information and identifying criminal networks.

At the same time, the growing use of AI within criminal investigations has generated concerns regarding privacy, accountability, transparency and procedural fairness. The increasing reliance on algorithmic systems raises important questions regarding the extent to which investigative decisions should be influenced by automated technologies. These concerns highlight the need for careful evaluation of both the benefits and risks associated with AI-driven criminal forensics.

The Expanding Role of AI in Modern Forensic Science

The integration of AI into criminal forensics reflects a broader shift toward data-driven investigative practices. Traditional forensic methods remain essential to criminal investigations; however, AI increasingly functions as a force multiplier capable of enhancing analytical capacity and improving investigative efficiency. By enabling the rapid processing of information and facilitating the identification of complex patterns, AI has transformed the manner in which evidence is collected, analysed and interpreted.

Nevertheless, the effectiveness of AI technologies must not be assessed solely in terms of operational efficiency. Their legitimacy also depends upon compliance with legal standards, constitutional protections and principles of fairness. As AI assumes a greater role in criminal investigations, it becomes necessary to examine both the opportunities and the challenges associated with its deployment within the criminal justice system.

Opportunities Presented By AI in Criminal Investigations

The increasing adoption of Artificial Intelligence within criminal investigations has significantly enhanced the capabilities of law enforcement agencies and forensic experts. The ability of AI systems to process large volumes of information, identify complex patterns and generate analytical insights has transformed many aspects of modern forensic science. As criminal activities become increasingly sophisticated and technology-driven, AI offers valuable tools for improving investigative efficiency, accuracy and responsiveness. While concerns regarding privacy and accountability remain important, the potential benefits of AI-assisted criminal forensics cannot be ignored.

Enhanced Evidence Analysis and Investigation Efficiency

One of the most significant advantages of AI in criminal forensics is its ability to analyse vast quantities of evidence within a relatively short period. Traditional investigations often require investigators to manually review documents, surveillance footage, communication records, financial transactions and digital devices. Such processes are time-consuming and may delay investigations, particularly in complex cases involving large volumes of data. AI-powered forensic tools can rapidly process and categorize information, identify relevant evidence and establish connections between different pieces of data. Machine learning algorithms can detect patterns that may not be immediately apparent to human investigators, thereby improving both the speed and accuracy of investigations. This enhanced analytical capacity enables law enforcement agencies to focus resources on critical aspects of criminal inquiries.

Strengthening Cybercrime Investigations

The rapid growth of cybercrime has created new challenges for law enforcement agencies across the world. Offences such as phishing attacks, ransomware incidents, identity theft, online fraud, hacking and digital financial crimes generate substantial quantities of electronic evidence that require specialized analysis. AI technologies assist investigators by monitoring network activity, detecting suspicious behaviour, identifying malware patterns and analysing digital footprints left by offenders. Advanced machine learning systems can recognize emerging cyber threats and support investigators in identifying perpetrators more efficiently. In an era where cybercrime frequently transcends geographical boundaries, AI has become an essential tool for digital forensic investigations.

Facial Recognition and Suspect Identification

Facial recognition technology has become one of the most visible applications of AI within criminal investigations. By comparing facial images against existing databases, AI systems can assist investigators in identifying suspects, locating missing persons and analysing surveillance footage obtained from public and private sources.

The technology is particularly valuable in cases involving large volumes of visual evidence. Instead of manually reviewing thousands of hours of video recordings, investigators can use AI-assisted systems to identify relevant individuals and reconstruct movements across multiple locations. Such capabilities significantly improve investigative efficiency and may contribute to faster resolution of criminal cases.

Crime Pattern Detection and Predictive Analysis

AI systems possess the ability to analyse historical crime data and identify recurring patterns that may assist law enforcement agencies in preventing and responding to criminal activity. Predictive analytics tools can examine geographical trends, behavioural indicators, temporal patterns and previous criminal incidents to generate insights regarding potential risks. Although predictive policing remains controversial, the analytical capabilities of AI can assist authorities in resource allocation, crime mapping and strategic planning. When implemented responsibly and subject to appropriate safeguards, such technologies may improve the effectiveness of crime prevention initiatives.

Financial Crime and Fraud Detection

Financial crimes have become increasingly sophisticated due to digital banking systems, online payment platforms, cryptocurrencies and cross-border financial transactions. Traditional investigative methods often struggle to detect complex networks of fraudulent activity involving large volumes of financial data. AI-powered analytical systems can identify suspicious transactions, detect unusual financial patterns and uncover connections between individuals, accounts and organizations. These capabilities are particularly valuable in investigations involving money laundering, tax evasion, corruption, cyber-enabled fraud and organized criminal enterprises. By automating aspects of financial analysis, AI enables investigators to detect irregularities more efficiently and accurately.

Missing Persons and Human Trafficking Investigations

AI technologies have also demonstrated significant potential in locating missing persons and combating human trafficking. Facial recognition systems, biometric identification tools and data analytics platforms can assist authorities in identifying vulnerable individuals and tracking criminal networks involved in trafficking operations. The integration of AI with national databases and surveillance systems may improve the ability of law enforcement agencies to identify missing persons and facilitate timely intervention. Such applications highlight the humanitarian potential of AI-assisted criminal investigations beyond conventional law enforcement objectives.

Improving Forensic Accuracy and Resource Optimization

In addition to enhancing investigative speed, AI contributes to greater forensic accuracy by reducing the likelihood of human error in repetitive analytical tasks. Automated systems can process information consistently, identify anomalies and support evidence evaluation through data-driven analysis. AI also enables more efficient allocation of investigative resources. Law enforcement agencies frequently face constraints relating to manpower, expertise and time. By automating routine analytical functions, AI allows investigators and forensic experts to concentrate on complex tasks requiring human judgment and professional expertise. This combination of technological assistance and human oversight has the potential to improve the overall effectiveness of criminal investigations.

Opportunities and the Need for Caution

The opportunities presented by AI in criminal forensics are substantial. Enhanced evidence analysis, improved cybercrime detection, efficient suspect identification, predictive capabilities and advanced forensic analytics demonstrate the transformative potential of AI within the criminal justice system. However, technological effectiveness alone cannot justify unrestricted deployment. The same technologies that enhance investigative efficiency may also generate risks relating to privacy, surveillance, discrimination and procedural fairness. Consequently, any assessment of AI-assisted criminal forensics must balance its operational advantages against the legal and constitutional challenges associated with its use. These concerns form the focus of the next section.

Legal, Ethical and Constitutional Challenges of AI in Criminal Forensics

The growing integration of Artificial Intelligence into criminal investigations has generated significant legal, ethical and constitutional concerns. While AI technologies offer substantial benefits in terms of efficiency and accuracy, their deployment within the criminal justice system raises complex questions regarding privacy, fairness, accountability and procedural safeguards. Criminal investigations directly affect individual liberty and fundamental rights; consequently, the use of AI-powered forensic tools must be evaluated not only on the basis of technological effectiveness but also in light of constitutional principles and legal standards. The challenge lies in ensuring that technological innovation strengthens criminal justice without compromising the rights and freedoms guaranteed under the Constitution of India.

Privacy and Data Protection Concerns

One of the most significant challenges associated with AI-driven criminal forensics relates to privacy. AI systems often rely upon the collection, storage and analysis of large quantities of personal data, including biometric information, facial images, communication records, location data and online activity. The extensive processing of such information raises concerns regarding state surveillance and unauthorized intrusion into individual privacy.

The constitutional significance of privacy was firmly established by the Supreme Court in *Justice K.S. Puttaswamy v Union of India* [18], where the Court recognized privacy as a fundamental right under Article 21 of the Constitution. The judgment emphasized that any restriction upon privacy must satisfy the requirements of legality, necessity and proportionality. The increasing use of facial recognition systems, predictive policing technologies and AI-assisted surveillance mechanisms therefore necessitates careful scrutiny to ensure compliance with these constitutional standards.

The absence of a comprehensive legal framework specifically regulating AI-assisted investigations further intensifies privacy concerns. Without clear statutory safeguards governing data collection, retention and usage, there exists a risk that investigative technologies may be deployed in a manner inconsistent with constitutional protections.

Algorithmic Bias and Discrimination

AI systems are only as reliable as the data upon which they are trained. If training datasets contain historical biases or inaccuracies, the resulting algorithms may produce discriminatory outcomes. This problem is particularly concerning in criminal investigations where algorithmic decisions may influence suspect identification, risk assessment, or investigative priorities.

Facial recognition technologies have been criticized globally for exhibiting higher error rates when analysing certain demographic groups. Similar concerns arise in predictive policing systems, which may inadvertently reinforce existing patterns of over-policing and social discrimination. Such outcomes undermine the principles of equality and fairness that form the foundation of the criminal justice system. The risk of algorithmic bias demonstrates that technological neutrality cannot be assumed. Human oversight remains essential to ensure that AI-generated outputs do not perpetuate discrimination or produce unjust investigative outcomes.

Lack of Transparency and Explainability

A further challenge arises from the opaque nature of many AI systems. Complex machine learning models often function as "black box" technologies, generating outcomes that may be difficult to explain or interpret even by their developers. This lack of transparency creates significant difficulties within criminal investigations where decisions affecting individual liberty must be capable of justification and scrutiny. Transparency is essential to procedural fairness. If investigators, defence counsel, or courts are unable to understand how an AI system reached a particular conclusion, it becomes difficult to assess the reliability and validity of that conclusion. The inability to explain algorithmic reasoning may therefore undermine confidence in AI-generated evidence and create obstacles for judicial review.

Consequently, explainability should be regarded as a fundamental requirement for the deployment of AI technologies within criminal investigations. Systems that significantly influence investigative outcomes must be capable of meaningful scrutiny by legal institutions.

Reliability and Accuracy of AI-Generated Evidence

The admissibility and evidentiary value of AI-generated information depend largely upon its reliability. While AI systems can process data more rapidly than human investigators, they remain vulnerable to errors arising from flawed datasets, programming defects, inaccurate assumptions, or technical limitations. False positives generated by facial recognition systems provide a notable example of this challenge. Incorrect identification may expose innocent individuals to investigation, surveillance, or prosecution. Similarly, predictive algorithms may generate inaccurate assessments that influence investigative decisions without adequate factual basis.

The risk of technological error is particularly significant in criminal proceedings, where mistakes may result in wrongful accusations or miscarriages of justice. Consequently, AI-generated evidence should not be treated as inherently reliable merely because it originates from advanced technological systems. Judicial scrutiny and independent verification remain essential safeguards.

Surveillance, Civil Liberties and the Risk of Overreach

AI-powered surveillance technologies have significantly expanded the ability of state authorities to monitor public spaces and analyse behavioural patterns. While such capabilities may enhance security and support criminal investigations, they also raise concerns regarding excessive surveillance and erosion of civil liberties. The widespread deployment of facial recognition systems, smart surveillance infrastructure and real-time monitoring technologies may create an environment in which individuals are subject to continuous observation. Such developments have the potential to chill free expression, undermine personal autonomy and alter the relationship between citizens and the state. The challenge is therefore to ensure that surveillance technologies are deployed in a manner consistent with democratic values and constitutional protections. Effective oversight mechanisms are necessary to prevent misuse and ensure proportionality in the exercise of investigative powers.

Accountability and Responsibility

The increasing use of AI in criminal investigations also raises questions regarding accountability. When an AI system generates an inaccurate identification, produces a flawed risk assessment, or contributes to an erroneous investigative decision, determining responsibility may be difficult. Responsibility may potentially be attributed to multiple actors, including software developers, technology providers, law enforcement agencies, forensic experts and government institutions. The absence of clear legal standards governing liability and accountability creates uncertainty regarding how errors should be addressed and remedied. Accountability is particularly important because criminal investigations directly affect individual rights and liberties. The deployment of AI technologies should therefore be accompanied by mechanisms capable of identifying responsible actors and providing remedies when errors occur.

Due Process and Fair Trial Concerns

The use of AI within criminal investigations ultimately raises broader concerns regarding due process and the right to a fair trial. Criminal justice systems are founded upon principles of transparency, impartiality and procedural fairness. Decisions affecting liberty must be based upon evidence capable of challenge, verification and judicial scrutiny. Excessive reliance upon automated systems risks undermining these principles if human judgment is displaced by algorithmic decision-making. Investigative technologies should function as tools assisting human decision-makers rather than substitutes for independent legal evaluation.

Accordingly, the legitimacy of AI-assisted criminal forensics depends upon maintaining meaningful human oversight at every stage of the investigative process. Technological efficiency cannot be permitted to override constitutional guarantees designed to protect individual rights and ensure fairness within the administration of justice.

Balancing Innovation and Constitutional Values

The challenges discussed above do not suggest that AI should be excluded from criminal investigations. Rather, they highlight the need for balanced regulatory approaches capable of harnessing technological innovation while preserving constitutional protections. AI possesses enormous potential to strengthen forensic science and improve investigative outcomes. However, its deployment must remain subject to principles of legality, accountability, transparency, proportionality and fairness.

The future success of AI-assisted criminal forensics in India will therefore depend not merely upon technological advancement, but upon the ability of legal institutions to ensure that innovation remains consistent with constitutional values and the rule of law.

Admissibility of AI-Generated Evidence under Indian Law

The increasing use of Artificial Intelligence in criminal investigations raises important questions regarding the admissibility, reliability and evidentiary value of AI-generated information. While AI systems can assist investigators in identifying suspects, analysing digital records, recognizing patterns and processing large volumes of evidence, their outputs ultimately acquire legal significance only when they are relied upon in judicial proceedings. Consequently, courts must determine the extent to which AI-generated information satisfies the requirements of admissibility and evidentiary reliability under Indian law.

The challenge is particularly significant because AI systems do not merely store information; they actively analyse data and generate conclusions based on algorithmic processing. Unlike conventional documentary or electronic evidence, AI-generated outputs may involve predictive assessments, pattern recognition, probabilistic conclusions and automated decision-making processes. These characteristics raise unique evidentiary concerns regarding authenticity, reliability, transparency and judicial scrutiny.

Electronic Evidence under the Bharatiya Sakshya Adhiniyam [1]

The legal framework governing electronic evidence in India is primarily contained in the Bharatiya Sakshya Adhiniyam, [1], which replaced the Indian Evidence Act, 1872. The legislation recognizes the growing importance of electronic records and digital evidence within modern legal proceedings.

Given that AI systems operate through digital platforms and generate electronic outputs, AI-assisted forensic reports, surveillance records, facial recognition results, biometric analyses and algorithmic assessments are likely to be treated as forms of electronic evidence. Consequently, the admissibility of such material must comply with the statutory requirements applicable to electronic records. The recognition of electronic evidence reflects an important adaptation of evidentiary law to technological developments. However, the increasing sophistication of AI technologies raises questions that extend beyond mere admissibility and require careful consideration of reliability and procedural fairness.

Judicial Approach to Electronic Evidence

The Supreme Court of India has played a significant role in clarifying the evidentiary treatment of electronic records. In *Anvar P.V. v P.K. Basheer*, the Court emphasized the importance of complying with statutory requirements governing electronic evidence and established that electronic records must satisfy prescribed evidentiary conditions before being admitted in judicial proceedings.

Subsequently, in *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal*, the Supreme Court reaffirmed the significance of procedural safeguards relating to electronic evidence and clarified the legal position concerning certification requirements. The judgment underscored the necessity of ensuring authenticity and reliability in digital records presented before courts. Although these decisions did not specifically address Artificial Intelligence, the principles articulated by the Court are highly relevant to AI-generated evidence. They demonstrate the judiciary's recognition that technological evidence requires procedural safeguards capable of ensuring reliability and preventing manipulation.

Reliability of AI-Generated Evidence

Reliability constitutes one of the most important considerations in evaluating AI-generated evidence. Courts traditionally assess evidence on the basis of credibility, authenticity, relevance and probative value. The application of these principles to AI-generated information presents unique challenges.

AI systems frequently operate through complex algorithms that analyse data and generate outputs based upon statistical probabilities and machine learning models. While such systems may achieve high levels of accuracy, they are not immune from error. Incorrect training data, algorithmic bias, software defects, or technical limitations may produce inaccurate conclusions that affect investigative outcomes.

For example, facial recognition systems may incorrectly identify individuals, while predictive analytics tools may generate misleading assessments regarding criminal behaviour. If such outputs are relied upon without adequate verification, the risk of wrongful investigation or prosecution increases significantly. Accordingly, AI-generated evidence should not be treated as automatically reliable merely because it originates from advanced technological systems. Courts must remain vigilant in assessing the methodological integrity and evidentiary value of algorithmic outputs.

Transparency and Explainability as Evidentiary Requirements

The admissibility of AI-generated evidence is closely linked to the issue of transparency. In traditional evidentiary processes, witnesses, experts and investigators can generally explain the basis of their conclusions and be subjected to cross-examination. AI systems, particularly those based upon complex machine learning models, may not always provide comparable levels of explainability.

This lack of transparency presents difficulties for both courts and litigants. Defence counsel may be unable to challenge algorithmic conclusions effectively if the underlying decision-making process remains inaccessible. Similarly, judges may encounter difficulties in evaluating the weight that should be attached to AI-generated evidence where the reasoning process is not fully understood. Consequently, explainability should be regarded as a crucial evidentiary safeguard. AI systems used within criminal investigations should be capable of providing sufficient information regarding the methods, datasets and analytical processes underlying their conclusions. Transparency promotes accountability and enables meaningful judicial scrutiny.

Expert Testimony and Human Oversight

Given the technical complexity of AI systems, expert testimony is likely to play an increasingly important role in judicial proceedings involving AI-generated evidence. Experts may assist courts in understanding the functioning of algorithms, evaluating the reliability of forensic tools and identifying potential limitations within technological systems.

Human oversight remains equally important. AI should function as an investigative aid rather than a substitute for human judgment. Investigators, forensic experts, prosecutors and judges must retain ultimate responsibility for evaluating evidence and making decisions that affect individual rights and liberties. The continued involvement of human decision-makers serves as an important safeguard against excessive reliance on automated systems and helps ensure compliance with principles of fairness and due process.

Towards Evidentiary Standards for AI-Based Forensics

As AI technologies become increasingly integrated into criminal investigations, the development of specialized evidentiary standards will become necessary. Existing rules governing electronic evidence provide a useful foundation, but they may not fully address issues such as algorithmic bias, machine learning opacity, automated decision-making and predictive analysis.

Future legal frameworks should establish standards relating to validation, accuracy testing, auditability, transparency and independent verification of AI systems used in forensic investigations. Such safeguards would strengthen public confidence in AI-assisted criminal justice while ensuring that technological innovation remains consistent with evidentiary fairness and constitutional principles. Ultimately, the admissibility of AI-generated evidence should depend not only upon technical functionality but also upon demonstrable reliability, transparency and accountability. Courts must ensure that the pursuit of technological efficiency does not compromise the integrity of the judicial process or the rights of individuals subjected to criminal investigation.

Comparative Perspectives on AI in Criminal Forensics

The increasing use of Artificial Intelligence in criminal investigations has prompted governments and regulatory authorities across the world to develop legal frameworks aimed at balancing technological innovation with fundamental rights protections. Comparative analysis of international approaches provides valuable insights for India as it seeks to regulate AI-assisted criminal forensics.

United States

The United States has been among the earliest adopters of AI-driven investigative technologies. Law enforcement agencies have increasingly utilized facial recognition systems, predictive policing tools and algorithmic risk assessment models. These technologies have contributed to enhanced investigative efficiency and crime detection capabilities. However, their deployment has also generated significant legal controversy. Civil liberties organizations have raised concerns regarding racial bias, wrongful identification and excessive surveillance. Several jurisdictions have imposed restrictions on facial recognition technologies, while courts have increasingly scrutinized the constitutional implications of algorithmic decision-making. The American experience demonstrates both the benefits and risks associated with rapid technological adoption in criminal investigations.

European Union

The European Union has adopted a rights-based approach toward AI regulation. The recently enacted AI Act classifies certain AI applications used in law enforcement and criminal justice as high-risk systems subject to enhanced regulatory requirements. The framework emphasizes transparency, accountability, human oversight and protection of fundamental rights. Attention has been given to biometric surveillance technologies and facial recognition systems. The European approach reflects a commitment to ensuring that technological innovation remains consistent with privacy rights, data protection principles and procedural fairness. This model offers valuable lessons regarding the importance of regulatory safeguards in AI-assisted criminal investigations.

United Kingdom

The United Kingdom has pursued a relatively balanced approach to AI deployment in policing and forensic investigations. Law enforcement agencies have experimented with facial recognition systems and advanced data analytics while remaining subject to judicial scrutiny and regulatory oversight. Judicial decisions concerning the use of automated facial recognition technologies have emphasized the need for legality, proportionality and accountability. The British experience demonstrates that technological innovation can coexist with legal safeguards when supported by clear oversight mechanisms and institutional accountability structures.

Lessons for India

Comparative experience reveals several common themes. First, human oversight remains essential regardless of technological sophistication. Second, transparency and explainability are increasingly regarded as necessary safeguards for AI systems affecting individual rights. Third, independent auditing and accountability mechanisms play a crucial role in maintaining public confidence. Finally, regulatory certainty is essential for ensuring that AI technologies are deployed consistently and responsibly.

For India, these experiences suggest that the regulation of AI-assisted criminal forensics should not focus solely upon technological effectiveness. Equal importance must be given to constitutional protections, evidentiary reliability, procedural fairness and accountability. A balanced regulatory framework should therefore combine innovation with robust safeguards capable of protecting both public security and individual rights.

Towards An Indian AI Forensic Governance Framework

The preceding discussion demonstrates that AI possesses enormous potential to strengthen criminal investigations while simultaneously creating significant legal and constitutional challenges. To maximize benefits and minimize risks, India requires a coherent regulatory framework capable of governing the use of AI within criminal forensics. This paper proposes an Indian AI Forensic Governance Framework (IAFGF) based upon five interrelated principles.

Human-Centred Decision-Making

AI should function as an investigative aid rather than an autonomous decision-maker. Critical decisions relating to arrest, prosecution, surveillance and evidentiary evaluation must remain subject to meaningful human oversight. Investigators and judicial authorities should retain ultimate responsibility for decisions affecting individual rights and liberties. Human-centred governance ensures that technological outputs are evaluated within the broader context of legal principles, factual circumstances and constitutional safeguards.

Transparency and Explainability

AI systems deployed within criminal investigations should be capable of providing understandable explanations regarding their functioning and conclusions. Investigators, courts, defence counsel and oversight authorities must be able to scrutinize the basis of algorithmic decisions. Transparency promotes accountability and enables effective judicial review. It also strengthens public confidence in the legitimacy of AI-assisted forensic investigations.

Independent Auditing and Validation

Regular auditing of AI systems should be made mandatory. Independent experts should evaluate forensic technologies for accuracy, reliability, bias and compliance with legal standards. Validation procedures should be conducted before deployment and periodically throughout the operational life of the system. Such audits would reduce the risk of discriminatory outcomes and improve the credibility of AI-generated evidence presented before courts.

Privacy and Data Protection Safeguards

The use of AI in criminal investigations must remain consistent with constitutional privacy protections and applicable data protection principles. Clear rules should govern data collection, storage, processing, retention and sharing. Investigative authorities should be required to demonstrate necessity and proportionality when deploying AI-based surveillance or forensic tools. Strong privacy safeguards are essential to preventing misuse and maintaining constitutional legitimacy.

Judicial and Institutional Oversight

Effective oversight mechanisms are critical for ensuring accountability. Judicial review should remain available where AI-assisted investigative measures affect fundamental rights. In addition, specialized oversight bodies may be established to monitor compliance, investigate complaints and develop best practices for AI deployment within the criminal justice system. Institutional coordination between law enforcement agencies, forensic laboratories, judicial authorities and regulatory bodies will be necessary to ensure consistent implementation of governance standards.

Building Trust in AI-Assisted Criminal Justice

The long-term success of AI in criminal forensics depends not only upon technological performance but also upon public trust. Citizens must have confidence that AI systems operate fairly, accurately and within the limits imposed by law. The proposed Indian AI Forensic Governance Framework seeks to achieve this objective by combining innovation with accountability, efficiency with fairness and technological advancement with constitutional values.

CONCLUSION

Artificial Intelligence has emerged as one of the most transformative developments in modern criminal forensics. Through facial recognition systems, biometric identification technologies, predictive analytics, digital evidence analysis and automated investigative tools, AI has significantly enhanced the ability of law enforcement agencies to detect, investigate and prevent crime. The technology offers substantial opportunities for improving investigative efficiency, forensic accuracy and resource utilization in an increasingly digital criminal environment.

At the same time, the deployment of AI within criminal investigations raises complex legal, ethical and constitutional concerns. Issues relating to privacy, algorithmic bias, transparency, reliability, surveillance and accountability challenge traditional assumptions regarding criminal justice and evidentiary fairness. The absence of a comprehensive legal framework governing AI-assisted investigations in India further increases uncertainty regarding admissibility, oversight and protection of individual rights. This paper has argued that the effectiveness of AI in criminal forensics should not be measured solely by its capacity to enhance investigative efficiency. Its legitimacy ultimately depends upon compliance with constitutional values, procedural safeguards and principles of fairness. Technological innovation cannot be permitted to undermine the rights that form the foundation of a democratic legal system.

The future of criminal forensics in India will undoubtedly involve greater reliance upon Artificial Intelligence. However, successful integration requires more than technological adoption. It requires a balanced regulatory framework capable of ensuring transparency, accountability, reliability and respect for fundamental rights. By adopting appropriate governance mechanisms and maintaining meaningful human oversight, India can harness the benefits of AI-assisted criminal investigations while preserving the constitutional values that underpin the rule of law.

REFERENCES

1. Bharatiya Sakshya Adhiniyam, 2023, India.
2. Bharatiya Nyaya Sanhita, 2023, India.
3. Bharatiya Nagarik Suraksha Sanhita, 2023, India.
4. Digital Personal Data Protection Act, 2023, India.
5. Babuta, A. *et al.* Machine Learning Algorithms and Police Decision-Making: Legal, Ethical and Regulatory Challenges. Royal United Services Institute, 2018.
6. Desai, S. and B. Ambali. "Healthcare security with blockchain in India." *ShodhAI: Journal of Artificial Intelligence*, vol. 1, no. 1, 2024, pp. 28-39. https://doi.org/10.29121/shodhai.v1.i1.2024.

7. Hidayat, R. and N. Anwar. "Forensic analysis of web phishing and social engineering using the National Institute of Standards and Technology method: Case study of Facebook account data theft." *Journal of Digital Security and Forensics*, vol. 1, no. 1, 2024, pp. 12-25. https://doi.org/10.29121/digisecforensics.v1.i1.2024.14.
8. Casey, E. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. 3rd Edn., Academic Press, 2011.
9. Desai, A.U. "A review of the applications of machine learning in cybersecurity and its challenges." *Journal of Digital Security and Forensics*, vol. 1, no. 1, 2024, pp. 26-29. https://doi.org/10.29121/digisecforensics.v1.i1.2024.17.
10. Ferguson, A.G. "Policing predictive policing." *Washington University Law Review*, vol. 94, 2017, pp. 1109.
11. Rajput, H. "Biological evidence for crime investigation." *Journal of Digital Security and Forensics*, vol. 1, no. 1, 2024, pp. 34-52. https://doi.org/10.29121/digisecforensics.v1.i1.2024.23.
12. Garvie, C. *et al.* The Perpetual Line-Up: Unregulated Police Face Recognition in America. Georgetown Law Center on Privacy and Technology, 2016.
13. Goodfellow, I. *et al. Deep Learning*. MIT Press, 2016.
14. NITI Aayog. National Strategy for Artificial Intelligence. Government of India, 2018.
15. Oswald, M. *et al.* "Algorithmic risk assessment policing models: Lessons from the United Kingdom." *Information and Communications Technology Law*, 2018.
16. Russell, S. and P. Norvig. Artificial Intelligence: A Modern Approach. 4th Edn., Pearson, 2021.
17. Information Technology Act, 2000, India.
18. Justice K.S. Puttaswamy (Retd.) v. Union of India. 10 SCC 1, 2017.