# Use of Artificial Intelligence in Forensic Investigations: Legal and Ethical Challenges in India

## Authors

**Virendra Kumar[1], Mansi Srivastava[2], Devyani Chaudhary[3], Priyanshi[4]**

[1]Assistant Professor, Royal College of Law, Ghaziabad

[2]Research Scholar, School of Legal Studies, COER University, Roorkee

[3]B.A.LL.B., School of Legal Studies, Jigyasa University, Dehradun

[4]B.A.LL.B., School of Legal Studies, Jigyasa University, Dehradun

**Abstract**

Artificial intelligence is rapidly transforming forensic investigations in India, from cyber-forensics and digital evidence analysis to automated facial recognition and predictive policing. AI tools assist investigators in processing large volumes of data, identifying patterns, and generating leads that were previously impossible or impracticable through manual methods. However, this technological shift raises complex legal and ethical questions concerning admissibility and reliability of AI-generated evidence, standards of expert testimony, privacy and surveillance, algorithmic bias and discrimination, and the accountability of both state and private actors involved in AI-enabled investigations.

The paper first outlines the conceptual and technological contours of AI use in forensic investigations in India, including cyber-forensics, automated facial recognition systems (AFRS), AI-driven surveillance, and pattern-recognition tools used by police and forensic laboratories. It then analyses the existing legal framework—particularly the Information Technology Act, 2000; the Digital Personal Data Protection Act, 2023; and the Bharatiya Sakshya Adhiniyam, 2023—together with constitutional jurisprudence post-Justice K.S. Puttaswamy (Retd.) v. Union of India, to assess how far these norms regulate AI-based forensic practices. The paper identifies key legal and ethical challenges: opacity of AI systems and explainability of algorithms; chain of custody and evidentiary integrity; privacy, surveillance and mass data-collection; algorithmic bias and unequal impact; and the absence of a dedicated AI statute or sector-specific safeguards for forensic use.

Drawing on comparative insights from the European Union's AI Act and global debates on "responsible AI", the paper argues for a risk-based and rights-oriented regulatory approach tailored to forensic and law-enforcement contexts. It proposes doctrinal and policy reforms including: statutory standards for admissibility and probative value of AI-generated evidence; mandatory algorithmic audits and impact assessments; privacy-by-design and data-minimisation in investigative deployments; clear allocation of liability among state agencies, vendors, and experts; and institutional mechanisms for oversight and redress. The paper concludes that without a coherent regulatory framework reconciling innovation with constitutional guarantees of fairness, equality and privacy, AI's integration into forensic investigations risks undermining due process and public trust in India's criminal justice system.

**Keywords**: Artificial Intelligence; Forensic Evidence; Digital Forensics; Automated Facial Recognition; Surveillance; Privacy; Data Protection; Bharatiya Sakshya Adhiniyam, 2023; Digital Personal Data Protection Act, 2023; Justice K.S. Puttaswamy; India.

## 1. Introduction

AI has become an increasingly central component of criminal investigation and forensic practice in India, particularly in the domains of cyber-crime, digital evidence analysis, and large-scale data analytics. Law-enforcement agencies now use AI-driven tools for tasks such as malware analysis, log-file correlation, crime pattern mapping, and automated image or video analysis in the course of investigations. Automated facial recognition systems (AFRS) are being deployed by police and other state agencies to identify suspects and persons of interest from CCTV footage and image databases, while AI-enhanced surveillance platforms integrate feeds from multiple sources for real-time monitoring.

This expansion of AI in policing occurs in the backdrop of a criminal justice system already grappling with questions of delay, investigative capacity, and the handling of digital evidence. Proponents argue that AI can significantly improve efficiency, reduce backlogs in forensic laboratories, and assist in complex cyber-crime investigations that require sophisticated technical tools. Yet the introduction of AI also challenges foundational legal concepts such as mens rea, evidentiary reliability, and the presumption of innocence, while raising concerns about privacy, mass surveillance, and discriminatory targeting.

India's legal framework is in a transitional phase, with older statutes like the Information Technology Act, 2000 being supplemented by new enactments, including the Digital Personal Data Protection Act, 2023 (DPDP Act) and the Bharatiya Sakshya Adhiniyam, 2023 which replaces the Indian Evidence Act. At the same time, constitutional jurisprudence following the Supreme Court's recognition of privacy as a fundamental right in Justice K.S. Puttaswamy (Retd.) v. Union of India has established robust tests of legality, necessity and proportionality for state actions involving surveillance and data processing. AI-driven forensic practices must therefore be evaluated against both statutory requirements and constitutional limitations.

## 2. Research Question

The central research question guiding this paper is:

How does the deployment of artificial intelligence in forensic investigations in India interact with existing legal and ethical frameworks, and what reforms are necessary to ensure that AI-enabled forensic practices remain consistent with constitutional guarantees and principles of fair trial.

Sub-questions emerging from this inquiry include:

• To what extent do current Indian statutes and evidentiary rules address AI-generated or AI-assisted forensic evidence?

• What are the primary legal and ethical concerns associated with AI-based surveillance, facial recognition, and automated decision-making in investigative contexts?

• How can India reconcile the need for effective law enforcement with the protection of privacy, equality and due process in the context of AI-enabled forensics?

## 3. Scope and Limitations of the Study

This study focuses on AI applications directly connected to forensic investigations and criminal procedure in India, including: digital forensics and cyber-crime investigations; automated facial recognition and surveillance systems used for identification and tracking; pattern-recognition tools for crime analysis; and AI-assisted evidence examination in forensic laboratories. The analysis is confined to Indian law, though selective comparative references (such as to the EU AI Act or foreign privacy regimes) are used to illuminate regulatory options rather than to provide comprehensive comparative law coverage.

The paper primarily examines public-sector use of AI by law-enforcement agencies and related public institutions, though it recognises that private vendors and technology providers play a crucial role in supplying AI tools and may themselves be regulated as data fiduciaries under the DPDP Act. It does not attempt a technical evaluation of specific algorithms or models; rather, it treats AI systems in functional terms (e.g., facial recognition, pattern-matching, anomaly detection) to focus on legal and ethical consequences.

The study is limited by the relative opacity surrounding some law-enforcement deployments—many AI-based surveillance and recognition systems operate without detailed public documentation, making it difficult to fully assess their design, datasets, and internal safeguards. Further, the DPDP Act and accompanying rules are themselves in the process of phased implementation, and judicial interpretation of its provisions in the AI context is still nascent. The analysis therefore necessarily involves some degree of normative and prospective reasoning about how courts and regulators ought to respond to emerging practices.

## 4. Research Methodology

This paper adopts a doctrinal and analytical research methodology, supplemented by comparative and normative perspectives. It relies primarily on statutory texts, case law, government policy documents, and secondary literature including journal articles, policy reports, and expert analyses pertaining to AI, digital forensics, surveillance, and data protection in India. Key sources include academic and policy work on AI in Indian cyber-forensics, AI-driven surveillance, the evidentiary treatment of digital and AI-generated records, and the interpretation of the DPDP Act and related rules.

Comparative materials—particularly on the EU AI Act, EU data-protection frameworks, and foreign approaches to AI accountability—are used to highlight regulatory models that may be adapted to the Indian context, while recognising the specificities of India's constitutional and socio-legal environment. The methodology is normative in that it does not merely describe existing law but evaluates it against constitutional principles, rule-of-law values, and human-rights standards, proposing reforms where gaps or inconsistencies are identified.

## 5. Conceptual Framework: AI and Forensic Investigations

### 5.1 AI Technologies in Investigative Practice

In India, AI tools are being used across a spectrum of investigative and forensic activities. In cyber-forensics, machine learning systems assist in pattern recognition in network traffic, anomaly detection in log files, malware classification, and correlation of disparate data points to reconstruct digital events. These tools help address the exponential growth of cyber-crime, where digital footprints, encrypted communications, and distributed systems make traditional investigative methods inadequate.

Beyond cyber-crime, AI is increasingly used in criminal intelligence and investigation: predictive policing tools attempt to forecast crime hotspots; crime mapping and data-mining systems identify patterns in past offences; and natural language processing aids in processing large volumes of documents, social-media content, or call-detail records. AI-enhanced video analytics can automatically flag suspicious behaviour or recognise objects and individuals in CCTV footage, which is then used to generate leads or corroborate other evidence.

### 5.2 Automated Facial Recognition and Surveillance

Automated facial recognition technology (AFRT) has emerged as one of the most controversial AI applications within Indian law enforcement. Several state police forces and central agencies have procured or deployed facial recognition systems, often linked to large image databases, to identify suspects, trace missing persons, and monitor public spaces. Systems such as the National Automated Facial Recognition System (NAFRS), Delhi Police's AFRS, and platforms used by the Hyderabad Police's Command and Control Centre illustrate this trend.

Studies and policy reports have documented significant concerns regarding the design, accuracy, and deployment of these systems. Research highlights risks of false positives, especially for women, children, and marginalised communities, as well as the absence of clear legal authorisation, public notice, or independent oversight. AFRTs used in law enforcement raise questions about their chilling effect on freedom of movement, protest, and association, given their potential to track individuals across time and space without consent or suspicion.

### 5.3 AI, Evidence and Expert Testimony

AI's role in forensic investigations also implicates core evidentiary concepts. AI systems may generate, transform, or interpret digital records that are later presented in court as inculpatory or exculpatory evidence. Examples include AI-generated match scores in facial recognition, probabilistic inferences in pattern-matching tools, and automated correlation reports linking IP addresses, devices, or accounts to alleged criminal activity.

The probative value of such AI-assisted outputs depends on factors such as the quality and representativeness of training data, error rates, explainability of the model, and the chain of custody of input and output data. These questions intersect with rules on electronic evidence and expert testimony, including how AI systems are to be authenticated, how their reliability is to be assessed, and what level of disclosure is required regarding their internal functioning for cross-examination to be meaningful.

## 6. Existing Legal Framework in India

6.1 Information Technology Act, 2000 and SPDI Rules

The Information Technology Act, 2000 (IT Act) provides the foundational legal framework for electronic records, electronic signatures, and certain categories of cyber-offences in India. Although the Act predates modern AI technologies, it remains relevant for AI-driven investigations insofar as it regulates cyber-crimes, data security obligations, and the admissibility of electronic records. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules) impose data-security and notice-and-consent obligations on body corporates handling sensitive personal data, including biometric information.

However, the IT Act and SPDI Rules do not contain AI-specific provisions; they neither define AI systems nor explicitly regulate algorithmic decision-making, automated profiling, or AI-based surveillance. This creates a regulatory gap in relation to AI tools used by private vendors and, indirectly, by state agencies that procure such tools for forensic investigations.

### 6.2 Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 (DPDP Act) is India's first comprehensive data-protection statute, designed to govern the processing of digital personal data by public and private entities, including cross-border processing of Indian residents' data. It conceptualises individuals as "Data Principals" and entities determining the purposes and means of processing as "Data Fiduciaries," with particularly large or sensitive processors designated as "Significant Data Fiduciaries" (SDFs) subject to enhanced obligations.

AI systems that process personal data—such as facial recognition databases, AI-enhanced surveillance platforms, and predictive policing tools—will typically be governed by the DPDP Act because "processing" is defined broadly to include automated operations performed on digital personal data, including collection, storage, use, and dissemination. The Act's core principles of consent, purpose limitation, data minimisation, and accountability provide a normative framework to evaluate AI-based forensic practices, even though the statute does not explicitly mention AI or algorithmic profiling.

Subordinate legislation and rules under the DPDP Act, including provisions on algorithmic governance and due diligence for SDFs, further require entities using AI to conduct algorithmic risk assessments, ensure that AI systems are not likely to pose risks to the rights of Data Principals, and embed privacy-by-design and auditability across the lifecycle of AI models. These obligations are especially pertinent where AI tools are used for high-stakes decisions in criminal investigations.

### 6.3 Bharatiya Sakshya Adhiniyam, 2023 and Digital Evidence

The Bharatiya Sakshya Adhiniyam, 2023 (BSA) replaces the Indian Evidence Act, 1872 and seeks to modernise evidentiary law for the digital era, including explicit treatment of electronic records. Provisions such as section 63 of the BSA regulate how electronic records are to be proved in evidence, including requirements relating to authentication, integrity, and certificates regarding the manner in which the electronic record was produced. These provisions are directly relevant to AI-generated outputs and logs, which are often stored and transmitted in digital form.

Recent scholarship suggests that Indian evidence law remains under-prepared to address AI-driven evidence, especially in relation to explainability, algorithmic bias, and the appropriate standard of reliability for AI-assisted forensic tools. Questions arise about whether AI systems should themselves be treated as "documents," "devices," or "experts" for evidentiary purposes, and how their output should be presented and challenged in court. Without specific guidance on AI, courts must adapt general provisions on electronic records and expert evidence to an evolving technological landscape.

### 6.4 New Criminal Codes and Procedural Law

India has enacted new criminal codes—the Bharatiya Nyaya Sanhita, 2023 and Bharatiya Nagarik Suraksha Sanhita, 2023—which, among other changes, aim to reflect contemporary realities such as cyber-crime and digital evidence. While these codes do not create a comprehensive AI law, they shape investigative powers, arrest and search procedures, and evidentiary standards within which AI-enabled tools operate.

Legal scholars have argued that these reforms provide an opportunity to embed safeguards for AI-based investigations, including clear limits on surveillance, appropriate judicial oversight for intrusive technologies, and rights to challenge AI-generated inferences. Yet, in their current form, the codes still leave many AI-specific questions unanswered, particularly in relation to systemic surveillance and automated suspicion generation.

6.5 Constitutional Framework: Privacy, Equality, and Due Process

In Justice K.S. Puttaswamy (Retd.) v. Union of India, a nine-judge bench of the Supreme Court unanimously recognised privacy as a fundamental right under Article 21, with informational privacy forming a central component of the right. The Court articulated a tripartite test of legality, legitimate aim, and proportionality (including necessity and balancing) to evaluate state actions that infringe privacy, with subsequent decisions such as Anuradha Bhasin v. Union of India and cases concerning surveillance and internet shutdowns applying this framework to modern technologies.

AI-driven surveillance and forensic investigations, especially when involving large-scale collection and processing of biometric or behavioural data, must therefore satisfy this constitutional test. Moreover, Articles 14 and 19—guaranteeing equality before law and freedoms of speech, assembly, and movement—are implicated when AI tools are deployed in ways that may disproportionately target specific groups, chill democratic participation, or operate in an arbitrary and opaque manner.

## 7. Legal Challenges in AI-Enabled Forensic Investigations

7.1 Admissibility, Reliability and Explainability

One of the foremost legal challenges is determining when and how AI-generated or AI-assisted evidence is admissible in criminal proceedings. Under the BSA and earlier jurisprudence on electronic records, courts must be satisfied regarding the authenticity and integrity of digital evidence, including the reliability of the process by which it was produced. AI systems, particularly those based on complex machine learning models, often function as "black boxes," making it difficult for courts, lawyers, and defendants to understand how a particular output—such as a facial recognition match or anomaly score—was generated.

This opacity complicates the application of evidentiary rules on expert opinion and raises due-process concerns in criminal trials. If neither the underlying training data nor the algorithmic logic is disclosed, cross-examination becomes superficial, and the defence is unable to meaningfully challenge the validity of AI-produced inferences. Further, the probabilistic nature of many AI outputs (e.g., confidence scores) requires careful judicial instruction to avoid undue weight being given to AI evidence at the expense of other material, particularly when jurists lack technical literacy in AI.

7.2 Chain of Custody and Data Integrity

Forensic integrity relies on an unbroken chain of custody documenting how evidence was collected, stored, analysed, and presented. AI systems introduce additional complexity: digital data may be pre-processed, transformed, or filtered through multiple layers of automated tools before generating the final output used in court. Ensuring that each step is logged, reproducible, and insulated from tampering requires robust technical and procedural safeguards, including secure logging, hash-verification, and access controls.

In environments where police forces and forensic laboratories lack adequate technical infrastructure or training, the risk arises that AI tools are used without proper documentation or validation, undermining both evidentiary reliability and defence rights. Cyber-security vulnerabilities in AI systems themselves—

such as susceptibility to adversarial attacks or data poisoning—further complicate the assessment of whether AI-generated evidence can be trusted.

7.3 Allocation of Liability and Accountability

AI-enabled investigations often involve complex relationships between state agencies, private vendors, and technical experts. When an AI system produces an erroneous match leading to wrongful arrest or prosecution, questions arise as to who bears legal responsibility: the investigating officer, the agency that procured the system, the vendor that designed it, or the expert who interpreted its output. India currently lacks a dedicated AI liability framework that clarifies such allocation of responsibility, leading to potential diffusion of accountability.

The DPDP Act imposes duties on Data Fiduciaries and SDFs, including algorithmic due diligence and risk assessment, which may serve as a basis for regulatory sanctions in cases of data misuse or rights-violations. However, these obligations are designed primarily for data-protection and do not directly address wrongful convictions or investigative misconduct arising from reliance on flawed AI tools. Without clear statutory standards, courts will need to adapt general principles of negligence, vicarious liability, and public-law compensation to the AI context, a task that is both doctrinally and practically challenging.

## 8. Ethical Challenges: Surveillance, Privacy, and Bias

8.1 AI Surveillance and the Puttaswamy Proportionality Test

AI-driven surveillance mechanisms—particularly AFRT and real-time monitoring systems—pose acute ethical questions about privacy, autonomy, and democratic freedoms. Scholars have argued that many AI surveillance deployments in India lack a clear legislative basis and are instead grounded in executive orders, tenders, or departmental circulars, falling short of the "legality" requirement of Puttaswamy. Moreover, mass or indiscriminate facial recognition in public spaces raises doubts about whether such measures are "necessary" in a democratic society or whether less intrusive alternatives could achieve comparable security objectives.

The proportionality analysis also requires balancing security benefits against the extent and intensity of rights-infringement. Empirical studies indicate that facial recognition systems can exhibit substantial error rates and demographic biases, calling into question their actual effectiveness as investigative tools relative to their intrusive character. When deployed without clear limits on retention, sharing, and secondary use of biometric data, such systems risk function creep and may gradually transform Indian cities into spaces of pervasive, unaccountable surveillance.

### 8.2 Algorithmic Bias and Discrimination

AI systems trained on historical data risk reproducing and amplifying existing social biases related to caste, religion, gender, and socio-economic status. For instance, predictive policing algorithms built on arrest or crime data reflecting historically over-policed communities may disproportionately flag those same communities as high-risk, creating a feedback loop of enforcement. Similarly, facial recognition algorithms trained on skewed datasets may perform worst on under-represented groups, leading to higher false-positive rates for minorities.

Such discriminatory effects implicate Article 14's guarantee of equality and non-arbitrariness, as well as Articles 19 and 21 where AI-mediated targeting affects expression, association, or bodily integrity. Yet current Indian law lacks explicit provisions addressing algorithmic discrimination or mandating fairness audits, impact assessments, or public disclosure of error rates in AI-enabled law-enforcement tools. The DPDP Act's focus on individual consent and data rights, while important, does not fully capture systemic harms generated by biased AI systems.

### 8.3 Opacity, Consent and Public Trust

Ethical concerns also arise from the opacity of AI deployments in India's criminal justice system. Many surveillance and facial recognition projects have been rolled out with limited public awareness, sparse privacy impact assessments, and minimal avenues for community input or contestation. Individuals often do not know that their images or data are being captured, processed, and linked across databases, undermining meaningful consent and control over their personal information.

This opacity erodes public trust in law enforcement and the justice system, particularly in marginalised communities that may already experience over-policing or discriminatory treatment. Ethical AI frameworks emphasise values of transparency, explainability, and participation, which require not only technical documentation but also accessible communication about the purposes, risks, and safeguards associated with AI tools. Without such measures, AI-enabled forensic investigations risk being perceived as opaque instruments of control rather than tools for justice.

## 9. Comparative and International Perspectives

Global debates on AI regulation provide important reference points for India's evolving approach. The European Union's AI Act, for instance, adopts a risk-based framework that classifies AI systems by risk level, imposing stricter obligations on high-risk applications, including those in law enforcement and critical infrastructure. High-risk systems must satisfy requirements of human oversight, transparency, data-quality, robustness, and post-market monitoring, while certain unacceptable uses, such as real-time remote biometric identification in public spaces for law-enforcement, are tightly constrained or prohibited.

Scholars examining AI-driven surveillance in India argue that similar risk-based and context-sensitive regulation could help reconcile national security interests with privacy and civil liberties. Comparative analyses also highlight practices such as mandatory algorithmic impact assessments, independent oversight bodies, and rights for individuals to seek explanations or contest automated decisions, which may be adapted to India's constitutional framework. Importantly, any transplantation of foreign models must be sensitive to India's socio-economic diversity, policing realities, and institutional capacities.

International human-rights standards, including those articulated by UN bodies on surveillance, privacy, and automated decision-making, reinforce the need to ensure that AI-enabled investigations respect principles of legality, necessity, proportionality, non-discrimination, and effective remedy. These standards can guide Indian courts and policymakers in interpreting domestic law in harmony with global human-rights norms, particularly when dealing with novel issues posed by AI tools.

## 10. Suggestions and Recommendations

10.1 Enact a Dedicated Legal Framework for AI in Criminal Justice

India should consider enacting a dedicated statute or a detailed chapter within existing criminal-procedure or evidence laws specifically addressing AI use in criminal investigations and forensic practice. Such a

framework could define AI and high-risk AI systems, lay down principles for permissible uses in law enforcement, and establish minimum safeguards for applications involving surveillance, biometric identification, and automated decision-making.

This statute should incorporate the Puttaswamy proportionality test and explicitly require legislative authorisation for intrusive AI-based surveillance, rather than relying on executive directives or tender documents. It should also address liability and accountability, clarifying responsibilities of law-enforcement agencies, technology vendors, and experts when AI systems contribute to investigative or evidentiary outcomes.

10.2 Develop Evidentiary Standards for AI-Generated Evidence

The Bharatiya Sakshya Adhiniyam, 2023 should be supplemented, either through amendments or authoritative judicial interpretation, with detailed standards for the admissibility and probative value of AI-generated evidence. These standards should require, at a minimum:

• Disclosure of relevant technical information, including model type, training data characteristics (to the extent feasible), and known limitations or error rates;

• Documentation of the full chain of custody for both input data and AI-generated outputs, including logs of preprocessing steps and algorithmic configurations;

• Validation studies or independent audits demonstrating that the AI tool performs reliably for the population and context in which it is used;

• Clear judicial guidance on the interpretation of confidence scores and probabilistic outputs to avoid undue reliance on AI at the expense of other evidence.

Courts should be empowered to exclude AI-generated evidence where these standards are not met or where the risk of unfair prejudice outweighs probative value.

10.3 Mandate Algorithmic Audits and Impact Assessments

Building on the DPDP Act's provisions for Significant Data Fiduciaries and algorithmic due diligence, India should institutionalise mandatory algorithmic audits and human-rights impact assessments for AI systems used in law enforcement and forensic investigations. These audits should be conducted by independent entities with technical and legal expertise, evaluating issues such as data protection compliance, bias and discrimination, robustness, and security vulnerabilities.

Impact assessments should consider not only privacy risks but also potential effects on equality, free expression, and due process, with specific attention to vulnerable and marginalised communities. The results of such assessments, along with information about oversight mechanisms and complaint procedures, should be made publicly accessible to the greatest extent consistent with legitimate security needs.

10.4 Embed Privacy-by-Design and Data Minimisation

Law-enforcement agencies deploying AI tools must adopt privacy-by-design and data-minimisation principles across the entire lifecycle of AI systems, from procurement and development to deployment and decommissioning. This includes limiting data collection to what is strictly necessary for specified investigative purposes, setting retention limits, anonymising or pseudonymising data whenever feasible, and restricting secondary use or sharing across agencies absent clear legal basis.

Technical safeguards such as differential privacy, secure multi-party computation, and robust access-control mechanisms can reduce privacy risks while still enabling legitimate investigative functions. Privacy-by-design also entails incorporating features that facilitate transparency and accountability, such as logging mechanisms, user-friendly notices, and interfaces that allow authorised oversight bodies to review system performance.

10.5 Regulate AI-Driven Surveillance and Facial Recognition

Given the particularly intrusive nature of AI-driven surveillance, India should establish a specific regulatory framework for AFRT and similar technologies. This framework might include:

• A moratorium or strict limitations on real-time, wide-area facial recognition in public spaces, except under clearly defined circumstances subject to judicial authorisation;

• Statutory requirements for necessity and proportionality assessments before deploying surveillance AI, including evaluation of less intrusive alternatives;

• Transparency obligations such as public registers of surveillance systems, impact assessments, and information about locations and purposes of deployment;

• Strong safeguards for retention and sharing of biometric data, with criminal penalties for unauthorised access or misuse.

Courts should apply strict scrutiny to AI-based surveillance in light of Puttaswamy and related privacy jurisprudence, particularly where such systems are used to monitor protests, political events, or sensitive locations.

10.6 Address Algorithmic Bias and Promote Fairness

Regulatory measures should explicitly address algorithmic bias and discrimination in AI-enabled forensic tools. Possible interventions include:

• Requiring fairness assessments and demographic performance analysis for AI systems prior to deployment and at regular intervals thereafter;

• Prohibiting training or tuning models in ways that exploit sensitive attributes (such as caste or religion) unless strictly necessary and proportionate for a legitimate aim, and even then subject to strong safeguards;

• Providing defendants with access to relevant data and documentation needed to challenge claims of fairness or neutrality in AI outputs;

• Encouraging inclusive design processes that involve stakeholders from affected communities and civil-society organisations in evaluating AI tools intended for law-enforcement use.

Courts should recognise that algorithmic tools can perpetuate structural inequalities and should be open to expert testimony and empirical evidence on algorithmic bias when assessing the weight to be given to AI-generated inferences.

10.7 Capacity-Building and Institutional Oversight

Effective regulation of AI in forensic investigations requires not only legal rules but also institutional capacity. Police forces, prosecutors, defence lawyers, and judges need training in the basics of AI, data protection, and digital evidence to engage critically with AI-generated material. Forensic laboratories and

investigative agencies must build technical expertise to validate and audit AI tools, rather than relying entirely on vendor claims.

India should also establish or strengthen independent oversight bodies—such as data-protection authorities, human-rights commissions, or specialised AI regulators—with powers to investigate complaints, conduct inspections, and issue binding directions regarding AI use in law enforcement. These bodies should coordinate with courts and civil-society organisations to ensure that regulatory decisions reflect both technical realities and constitutional values.

### 11. Conclusion

AI's integration into forensic investigations in India presents a double-edged sword: it promises enhanced investigative capacities and more efficient processing of complex digital evidence, but simultaneously threatens to erode fundamental rights and distort evidentiary standards if deployed without adequate safeguards. The existing legal framework—comprising the IT Act, the DPDP Act, and the Bharatiya Sakshya Adhiniyam, 2023—offers important building blocks, yet remains incomplete and fragmented when confronted with the specific challenges of AI-enabled forensics, particularly in areas of explainability, bias, surveillance, and accountability.

Constitutional jurisprudence post-Puttaswamy requires that any AI-based interference with privacy and liberty satisfy rigorous standards of legality, necessity, and proportionality, while also respecting equality and non-arbitrariness. AI-driven surveillance practices, especially automated facial recognition and large-scale data analytics, will often struggle to meet these standards unless embedded within clear legislative frameworks and subject to robust oversight. The normative thrust of India's constitutional order thus demands a cautious, rights-oriented approach to AI in criminal justice, rather than a purely efficiency-driven one.

This paper has argued for a multi-pronged reform agenda: enacting dedicated legal standards for AI use in investigations; articulating detailed evidentiary rules for AI-generated outputs; mandating algorithmic audits and impact assessments; embedding privacy-by-design and data minimisation; regulating AI-based surveillance with particular care; addressing algorithmic bias; and investing in capacity-building and institutional oversight. Comparative experiences, such as the EU AI Act's risk-based framework, provide valuable guidance but must be adapted to India's constitutional and socio-legal context. Ultimately, the legitimacy of AI in forensic investigations will depend on whether it enhances, rather than undermines, the fairness, transparency, and human-rights orientation of India's criminal justice system.

## References

1. Cruz Joshna I & Layasri B, Artificial Intelligence in Indian Cyber Forensics, Int'l J. Legal Leaders & Res. (2025).
2. Yash G. Mahalle, Cybercrime, Artificial Intelligence, and Forensic Evidence Law in India: Reassessing Legal Standards in the Digital Age, Lawful Legal (Dec. 30, 2025), https://lawfullegal.in.
3. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).
4. Anuradha Bhasin v. Union of India, (2020) 3 S.C.C. 637 (India).
5. Digital Personal Data Protection Act, No. 22 of 2023, INDIA CODE (2023).

6. Information Technology Act, No. 21 of 2000, INDIA CODE (2000).
7. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Gazette of India, G.S.R. 313(E).
8. Bharatiya Sakshya Adhiniyam, No. 23 of 2023, INDIA CODE (2023).
9. Bharatiya Nyaya Sanhita, No. 21 of 2023, INDIA CODE (2023).
10. Constitution of India, 1950.
11. Bharatiya Nagarik Suraksha Sanhita, No. 22 of 2023, INDIA CODE (2023).
12. Indian Law Enforcement's Ongoing Usage of Automated Facial Recognition Technology – Ethical Risks and Legal Challenges, Vidhi Centre for Legal Policy (Aug. 15, 2021), https://vidhilegalpolicy.in.
13. MM Abraham, AI-Driven Surveillance in India: Reconciling Privacy, National Security and Legal Oversight, 8 J. Data Prot. & Privacy 183 (2025).
14. Right to Privacy Under Article 21 Versus AI Surveillance, Int'l J. Eng'g Dev. & Res. (2026), https://rjwave.org/ijedr/papers/IJEDR2601236.pdf.
15. The Algorithmic Accountability Paradox Under India's DPDP Act, 2023: Regulating Significant Data Fiduciaries, Bhatt & Joshi Assocs. (Dec. 23, 2025), https://bhattandjoshiassociates.com.
16. AI and Data Protection: Challenges in Automated Decision-Making, Indian Inst. of Soc. Sci. & Pub. Pol'y Res. (Feb. 27, 2025), https://iisppr.org.in.
17. AI and Data Protection in India: DPDP Act 2023 Explained, Complinity (Jan. 6, 2026), https://complinity.com.
18. Data Privacy Considerations Surrounding AI Use in India, Law.asia (May 8, 2025), https://law.asia/ai-and-data-protection.
19. India – Increasing Use of AI Across the Justice System, Tech & Justice Lab, Univ. of Oxford (Oct. 1, 2025), https://www.techandjustice.bsg.ox.ac.uk/research/india.
20. Legal Challenges in the Age of Artificial Intelligence, Int'l J. Found. & Multidisciplinary Res. (2025), https://www.ijfmr.com/papers/2025/5/58572.pdf.