Artificial Intelligence Driven Forensic Evidence: Shift from Human Experts to Machine Testimony

Dr. C.E. Pratap[1], D. Harini[2]

[1]Government Advocate (Criminal Side), High Court, Chennai

[2]IV year B.A., LL.B (Hons), Jindal Global Law School, O.P. Jindal Global University, Sonipat, Haryana

DOI: https://doi.org/10.51244/IJRSI.2026.13010026

Received: 01 January 2026; Accepted: 06 January 2026; Published: 23 January 2026

INTRODUCTION

Forensic science has been traditionally grounded in the assumption that objective scientific analysis, as carried out by human experts, can help the criminal justice system in uncovering the truth. From fingerprint analysis and handwriting comparison to DNA profiling and ballistic analysis, courts across various jurisdictions rely on expert interpretation of scientific expert opinion to establish guilt or innocence. However, this reliance has become increasingly constrained in an era marked by exponential data growth, complex digital manipulation and inherent limits in human cognitive and analytical capacity. In response, Artificial Intelligence (AI) has begun playing an expanding role in forensic processes.[1] Machine learning systems, used in a variety of investigations such as voice identification, crime scene reconstruction, deepfake detection or digital forensics, offer the promise of enhanced speed, efficiency and analytical ability. These characteristics that are especially attractive to country like India where over-burdened criminal system is a common phenomenon.

The introduction of AI, however, alters the very epistemology of forensic evidence. Unlike traditional forensic expert testimony that can be explained, scrutinised and cross-examined, AI systems that often operate as opaque "black boxes", not fully intelligible even to its designers, challenge the foundations of our established justice system.[2] In addition, these systems are likely to exemplify data, assumptions or social contexts that shaped their development, thereby negating the contentions that they are neutral. Notwithstanding these challenges, the fact is, the Indian legal system currently has no overarching legislation governing the use of these systems. The present evidentiary provision of these systems takes a human-oriented perspective, which says little about Algorithmic Evidence. This paper, thus, aims to examine the scientific, legal and institutional challenges posed by forensic AI and argues for a principled governance framework to ensure accountability, fairness and due process.

The Architecture of Forensic Artificial Intelligence

Artificial Intelligence in forensic science is not merely a single technology but a series of complex systems, designed to carry out specific tasks that were historically performed by human experts or believed to be beyond the capacity of such experts. It is thus important to test Forensic AI as not just a monolithic tool,[3] but rather analyse it through its major scientific domains. The architecture of Forensic AI can be discussed in detail with specific reference to various divisions of Forensic Science.

Pattern Recognition and Comparative Forensic Analysis

This comprises one of the most wide-spread use of AI in forensics where it is routinely applied to tasks below mentioned.

[1] Paul W Grimm, Maura R Grossman and Gordon V Cormack, 'Artificial Intelligence as Evidence' (2021) 19 JTIP 9 <https://scholarlycommons.law.northwestern.edu/njtip/vol19/iss1/2/> accessed 19 December 2025.

[2] Shaswat Anand and Shailja Thakur, 'Challenges and Limitations of AI in Forensic Science: A Critical Review' (2025) 6(1) IJRPR 5621 <https://ijrpr.com/uploads/V6ISSUE1/IJRPR38264.pdf> accessed 19 December 2025.

[3] Francesco Sessa and others, 'Artificial Intelligence and Forensic Genetics: Current Applications and Future Perspectives' (2024) 14(5) *Applied Sciences* 2113.

i) Fingerprint Analysis: Deep learning systems help analyse patterns, distortions and fragmentary prints that human examiners may overlook and match latent fingerprints with databases of registered fingerprints with increased levels of accuracy

ii) Ballistic Analysis: AI systems identify impact signatures left by firearms based on their striations and provide comparison reports of the evidence against the existing repositories more quickly and accurately than manual comparison

iii) Bloodstain Pattern Analysis: Tools that automate bloodstain identification, classification (like impact vs. swipe) and measurement, reducing subjectivity and increasing accuracy.[4]

DNA Interpretation and Probabilistic Genotyping

Unlike clean, direct samples of DNA that permit straightforward matching, crime scenes tend to often produce complex samples of DNA. AI-assisted Probabilistic Genotyping systems use statistical algorithms and machine learning to interpret such mixtures and determine contributor likelihood.[5]

Behavioural and Linguistic Predictive Patterns

AI systems are relied upon not just to analyse evidence but to infer and predict behaviour or intent.[6] Tools such as Natural Language Processing (NLP) for threat assessment, AI based Neuro-Prediction and other predictive policing tools go beyond mere analysation of data to a further step of predicting future conduct in helping shape the investigative direction and provide leads on criminal pattern.

Digital Forensics and Media Authentication

With the increased use and dependence on digital technology, this is one of the most rapidly evolving domains of Forensic AI.[7] Deep learning algorithms and Artificial Neural Networks are used for detecting deepfakes, facial recognition and gait analysis in video/image evidence, voice recognition and speaker identification, reconstruction of damaged audio/video, metadata analysis and in cyber-forensics.

Toxicology and estimating Post-mortem interval

In forensic toxicology and post-mortem interval estimation,[8] AI and machine learning models are applied to analyse biochemical markers, tissue degradation patterns, environmental variables and autopsy data to assist in estimating the time since death, identifying toxic substances and determining metabolic interactions that may not be apparent through a conventional approach.

Shift in Forensic Authority: From Human Experts to Machine Testimony

Historically, human experts have acted as interpreters of forensic evidence. Since courts are open to not just the evidence itself, but also an expert's reasoned explanation of the evidence, the traditional human-centric forensics, grounded on trained professionals and established methodology, provides a stable model that takes into account transparency, reproducibility and ethical accountability. The submissions and opinions of such experts are further open to scrutiny and challenge during cross-examination, which forms an important part of an adversarial criminal system.

[4] Muhammad Arjamand and others, 'The Role of Artificial Intelligence in Forensic Science: Transforming Investigations through Technology' (2024) 7(5) IJMRAP 67.

[5] Jill R Presser and Kate Robertson, *Executive Summary, AI Case Study: Probabilistic Genotyping DNA Tools in Canadian Criminal Courts* (Law Commission of Ontario, Toronto, June 2021) <https://www.lco-cdo.org/wp-content/uploads/2021/06/AI-PG-Case-Study-Exec-Summary-EN-Final-June-2021-.pdf> accessed 19 December 2025

[6] Saurav Yadav, Shalini Yadav, Preeti Verma, Smriti Ojha and Sudhanshu Mishra, 'Artificial Intelligence: An Advanced Evolution in Forensic and Criminal Investigation' (2023) 1 *Current Forensic Science* e190822207706 <https://doi.org/10.2174/2666484401666220819111603> accessed 19 December 2025.

[7] Sowmya G, 'AI in Digital Forensics: Detecting Deepfakes and Synthetic Media Attacks' (2025) 13(2) IJSET 1.

[8] C.E. Pratap, *Forensic Application of Scientific Expert Evidence in Criminal Trials* (Ph.D Thesis submitted to The Tamil Nadu Dr. Ambedkar Law University, Chennai, February 2024), p.331.

Over the recent years however, with the growth and expansion of technology, the use of AI has spread and seeped into the field of forensic science just as it has managed to do so in various other fields.[9] Many jurisdictions, including India though without explicit policy are in a hybrid stage where AI is used to do preliminary analysis that is then verified or signed off by human experts. This places the responsibility on the experts even if they did not technically perform the analysis, thus, trying to strike a balance between the rapid changes of a developing society with its accompanying data explosion and adhering to the conventional norms that ensures transparency and accountability.

This transition marks the beginning of an era in which machine forensics takes centre stage, where the analysis and interpretation of evidence increasingly depend on algorithmic reasoning.[10] While the formal responsibility may lie with the human experts, there is an underlying shift in the substantive authority to automated systems and devices whose reasoning processes remain arcane.

Legal Compatibility Issues concerning AI based Evidence

The integration of AI in forensic processes presents Indian Evidence Law with a fundamental doctrinal tension- the law of evidence is designed on human authorship, human perception and human accountability, whereas forensic outputs produced through AI are a result of autonomous computational processes. While certain provisions of the BSA, 2023 and the erstwhile Indian Evidence Act, 1872, seem to prima facie accommodate digital and electronic form of evidence, these provisions were not framed to manage algorithmic interpretation. Consequently AI-generated or AI-processed forensic evidence falls into a doctrinal vacuum partially compatible with statutory rules but structurally irreconcilable with the foundations of Evidence Law.

Surface Compatibility: Appearance of Admissibility

Section 61 of BSA (earlier Section 65B of IEA) recognises electronic evidence as admissible documents.[11] This means that AI outputs such as deepfake analysis reports, pattern recognition results, voice analysis outputs, etc., can technically be produced in court if accompanied by the necessary certification.

Further, AI-driven forensic systems can often track every access event, timestamp each analytical step, prevent tampering and generate audit logs, thus seemingly improving evidentiary integrity by strengthening the Chain of Custody.

Structural Incompatibility

While the lack of explicit prohibition makes AI outputs compatible at a procedural level, such compatibility is superficial- limited to the form of the evidence, not its nature.

i) Absence of Explainability

The assessment of evidence submitted before Indian Courts is based on intelligible reasoning, demonstrable methodology and reproducible results. However, AI systems, particularly neural networks and probabilistic genotyping tools, cannot provide explanations for their outputs (black box of calculations that are inaccessible to the experts themselves).[12] Additionally, even for the AI-systems which grant access to their reasoning process, the lawyers and judges in court do not possess sufficient technical know-how to understand or comprehend, much less challenge those reasonings.[13]

ii) Collapse of Cross-Examination

The adversarial system is built on the right to question. The origin of the evidence, its scientific authenticity, or its relevance to the proceedings, all evidence is subject to cross-examination. The lack of a human author for AI

[9] Grimm, Grossman and Cormack, ‘Artificial Intelligence as Evidence’.

[10] Archak Das, ‘AI in Legal Evidence Analysis: Ethical and Legal Implications’ (2024) 2 IJLRA 5.

[11] Section 61 Bharatiya Sakshya Adhiniyam 2023; Section 65B Indian Evidence Act 1872.

[12] Richard J Allen, ‘Artificial Intelligence and the Evidentiary Process: The Challenges of Formalism and Computation’ (2001) 9 *Artificial Intelligence and Law* 99.

[13] Eftychia Bampasika, ‘Artificial Intelligence as Evidence in Criminal Trial’ (2020) *Proceedings of the WAIEL Conference*, Athens.

evidence to provide justifying reasoning or defending arguments makes it impossible to cross-examine such evidence in a meaningful way, thus undermining the principle of equality of arms and the right to a fair trial.[14]

iii) Reliability cannot be tested under existing Statutes

Unlike human experts, AI-generated inference cannot be replicated manually, may change with software updates, vary across different versions or models and depends on undisclosed training data.[15] Since the Evidence Laws in India were never designed for probabilistic or algorithmic reasoning, courts have no statutory basis to evaluate any dataset bias, inbuilt errors, model drift or false positives/negatives.[16]

Doctrinal Gaps in Indian Law

Indian law lacks foundational definitions for AI-Generated definitions, algorithmic inference, machine testimony or any kind of automated forensic analysis. Treating the provisions of Section 61 of BSA or Section 65B of IEA as the basis for admitting AI evidence would be equivalent to placing AI outputs in the same shelf as CCTV or computer printouts.[17] Such characterisation of AI as mere "electronic record" would amount to a flagrant misclassification that fails to take into account the complex, opaque and distinct nature of an AI as opposed to other simple digital documents. Indian legislations fails to make distinction between static digital evidence and dynamic AI generated outputs.

Lack of Accountability

In traditional forensic science, the human expert is held accountable for the evidence and opinion so provided. Their opinion is open to critique, and any negligence is directly traceable. However, in AI-generated forensics, various stakeholders come into play. The developer denies responsibility, vendors claim proprietary secrecy, mere operation of the tool by police, experts signing reports they likely did not author and the court accepting the results without a proper foundational understanding. This complex sequence makes it extremely difficult to trace accountability for wrongful convictions resulting from any errors or negligence. The lack of a liability framework in the Indian law for such evidence makes AI errors effectively unchallengeable.

Constitutional Limitations: Rights of an Accused *vis-à-vis* use of AI evidence

All persons, regardless of guilty or innocent, have a right to fair trial which includes components such as equality of arms, right to explanation, right to cross-examine or right to challenge evidence. The use of AI evidence, however, strips them of most these basic rights. It would not be possible to explain to all the accused or even their representatives how the algorithm works, why it produced the result or what data influenced the conclusion. Without such explanation it becomes impossible to challenge the evidence,[18] especially given the lack of access to the AI's source code, training datasets and algorithm logic in most instances. Further, AI is not the most conventional witness. The operators, not being the actual authors of the device, would likely not understand the entire functionality of the devices themselves and it would not be feasible to order the appearance of the developer before the court for each case.

Beyond that, AI-driven biometric evidence, in areas pertaining to voice, face, gait or behavioural pattern recognition, blurs the line drawn between testimonial and physical evidence. Since these systems draw an inferential conclusion from bodily and behavioural data, their compulsory use risks indirectly compelling testimonial evidence,[19] thereby raising concerns about possible violation of the right against self-incrimination.[20]

[14] The Constitution of India, Article 21.

[15] Jenna Burrell, 'How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms' (2016) 3 *Big Data & Society* 1.

[16] Deepanker Singhal and Pragya Narang, 'AI-Generated Evidence in Indian Courts: Admissibility, Reliability and the Chain of Custody Challenge' (2023) 5(5) *Indian Journal of Integrated Research in Law* 186.

[17] Shruthika S, 'The Use of Artificial Intelligence in Criminal Trials' (2025) 7 IJLSI 414.

[18] Bampasika, 'Artificial Intelligence as Evidence in Criminal Trial'.

[19] Deepanker Singhal and Pragya Narang, 'AI-Generated Evidence in Indian Courts: Admissibility, Reliability and the Chain of Custody Challenge' (2023) 5(5) IJIRL 186.

[20] The Constitution of India, Article 20(3).

Scientific and Ethical risks

While the adoption of AI in forensic science is often justified through claims of accuracy, efficiency and neutrality, in reality, these claims tend to obscure various profound scientific and ethical risks that arise upon the use of automated systems in criminal evidence.

Algorithmic bias

AI systems learn from datasets that reflect historical policing practices, surveillance patters, demographic skews and investigative biases.[21] As a result, it risks encoding past injustices into its decision making. Pre-existing biases such as over-representation of certain communities in police datasets, historically skewed arrest data, mislabelled training sets, socio-economic markers embedded in biometric datasets, can easily enter forensic AI resulting in false positives, misidentification and discriminatory risk assessments.[22] Since the outputs are numerical or algorithmically generated, they give an appearance of neutrality while in fact reinforcing structural injustices.

Automation bias

It is in human nature to assume that computers/algorithms are more objective and accurate and hence, statistical outputs are authoritative. This phenomenon of 'Automation bias' gives rise to some serious risks in AI forensics. Automation bias can manifest in various ways- investigators following AI-generated leads even when inconsistent with physical evidence, prosecutors relying on algorithmic matches without independent corroboration or judges treating probability scores as scientific proof. This aura of infallibility that is attached to AI-generated evidence can thus be legally devastating.

Jurisdictional Issues

Usage of foreign-controlled AI software in forensic investigations has the potential to create complicated jurisdictional issues,[23] especially with regard to data sovereignty and admissibility of evidence.

i) Conflicting laws: Data processed by AI algorithms is usually stored in clouds across multiple countries, thus making it liable to the legislation of all relevant jurisdictions. Conflicting laws in these jurisdictions can give cross-border issues wherein complying with data request from one country may end up violating the stringent data protection laws of another.

ii) Data Localization Requirements: Some nations require that sensitive data be processed and stored physically within their borders. A tool that is foreign-owned and processes data outside the country may infringe such data localization requirements.

Concerns on Human Dignity, Surveillance and Technological Overreach

Apart from the evidentiary issues surrounding forensic AI, it also raises ethical questions regarding human dignity as well as proportionality. Continuous monitoring through biometrics, predictive profiling, and mass collection of data in a systemic manner risks normalising intrusive state scrutiny.[24] When deployed without strict necessity or oversight, such technologies threaten to transform forensic investigation into a mechanism of surveillance rather than a tool for justice.

Towards a Forensic AI Governance Model for India

[21] Doris Skaramuca, 'Evaluating the Admissibility of AI Evidence in Criminal Proceedings: Legal Standards and Ethical Implications' (2025) 2025 *SPLITLAW – International Doctoral and Postdoctoral Conference in the Law and Law Related Fields* 155–177.

[22] Shubham Handa and Dr.Shailja Thakur, 'Role of Artificial Intelligence in Admissibility of Electronic Evidence' (2024) 5 IJRPR 1324.

[23] Schellman & Company, 'Cross-Border AI Governance and Jurisdictional Conflicts' <https://www.schellman.com/blog/ai-services/cross-border-ai-governance-and-jurisdictional-conflicts>
accessed 19 December 2025.

[24] Vidushi Marda, 'Artificial Intelligence Policy in India: A Framework for Engaging the Limits of Data-Driven Decision-Making' (SSRN, 29 August 2018) <https://ssrn.com/abstract=3240384> accessed 19 December 2025.

From the foregoing analysis, it is clear that the issues presented by forensic AI evidence cannot be remedied by traditional evidentiary rules alone. Though the Indian judiciary enjoys wide discretion to deal with expert evidence and electronic evidence, issues of reliability, transparency, and accountability, triggered by forensic AI evidence, demand a separate framework. A coherent governance model must therefore recalibrate both evidentiary classification and institutional oversight, rather than relying on post hoc judicial evaluation.[25]

Reclassification of AI as 'Algorithmic evidence' from mere 'Electronic record'

Indian evidence law should abandon the assumption that AI outputs are functionally equivalent to ordinary electronic records.[26] Forensic AI, unlike static digital documents, interpret data actively to generate inferential conclusions. Accordingly, such outputs have to be recognised as a form of 'Algorithmic evidence' distinct from passive recording tools. Such reclassification would help ensure that AI-generated evidence is subject to more rigorous tests for admissibility in court.

Pre-Admissibility Reliability Screening

Courts should conduct a mandatory screening to determine the reliability of the AI-generated output for admission as evidence.[27] There must be a formal assessment of whether the system has been scientifically validated for the specific forensic task it performs including a disclosure of error rates, conditions of deployment and known limitations. Additionally, the screening should not just be limited to the accuracy claims but should also examine the integrity of the data pipeline such as the verification of training data, susceptibility to manipulation and continuity of the evidentiary custody from data collection to the generation of algorithmic output. Such screening prevents court from relying on opaque and unverified tools and ensure that the chain of custody does not lose its significance in cases of AI evidence.

Establishing a Forensic AI Certification Authority

Institutional oversight should go beyond internal forensic laboratories. The establishment of an independent National Certification Authority for Forensic AI tools would provide accountability at an ex-ante stage. The authority could assess the systems before their deployment, ensure periodic audits of bias and performance degradation and maintain an accessible registry of the approved tools. This will help reduce arbitrary procurement of proprietary tools and ensure accountability at an institutional level.

Rights of Accused to Contest Algorithmic Evidence

Procedural safeguards for the accused should specifically be improved. For the accused persons to exercise their right to confrontation and equality of arms, they cannot possibly do so without access to the required information about the algorithmic evidence. Whilst a full disclosure of source code may not be feasible on technical considerations, they ought to be provided with access to some basic data with regards to the validation set, error rate, and independent expert services so as to validate the outputs of the AI. Simultaneously, courts should also mandate a human-in-the-loop requirement,[28] ensuring that AI outputs remain corroborative in nature, with the final forensic opinion resting in the capable hands of experts amenable to cross-examination.

Additionally, India can also draw valuable guidance from comparative approaches. The EU's risk-based classification and regulation of high-risk AI-systems and the USA's emphasis on scientific reliability in AI evidence demonstrate that algorithmic tools in criminal justice demand heightened scrutiny.[29] Adapting these principles to India's framework would allow the criminal justice system to benefit from AI while ensuring that the principles of transparency, accountability and fairness are not sacrificed.

[25] Ram Krishna Mani Tripathi, 'AI in Judicial Decision-Making: Opportunities and Challenges' (2025) 8(4) IJLMH 2274–2289.

[26] Singhal and Narang, 'AI-Generated Evidence in Indian Courts'.

[27] European Commission High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI* (European Commission 2019) <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai> accessed 21 December 2025.

[28] ibid.

[29] Sabine Gless, 'AI in the Courtroom: A Comparative Analysis of Machine Evidence in Criminal Trials' (2020) 51(2) *Georgetown Journal of International Law* 233–274.

Interface between AI and Forensic Evidence: Case Studies in India

The following cases in India indicate that the need for changes is urgent:

• **Delhi riots (2020):** The Delhi Police made use of facial recognition technology to identify suspects, with little disclosure as to accuracy or error rates.

• **Deepfake evidence in Maharashtra (2021):** The courts were probing how to assess manipulated videos as evidence under Section 65B opening to doctrinal holes.

• **Aadhaar authentication logs:** The logs were first introduced as evidence against main accused in criminal trials, notwithstanding significant concerns, related to the unreliability of biometric recognition systems as contained within Indian Supreme Court judgements.93 As evidenced by the cases, the courts were improvising with the straitjacket contained in the wording of Section 65B of Indian Evidence Act, 1872.

CONCLUSION

Artificial Intelligence is increasingly transforming the field of forensics through its innovative application in the generation, interpretation and presentation of evidence in a court of law. As this paper has shown, AI-based approach in forensic evidence occupies an uneasy position in the Indian criminal justice system. While such tools are frequently considered to be procedurally admissible, an analysis of the current evidentiary framework reveals a structural vacuum which fails to align the attributes of forensic AI with foundational assumptions of Indian law that is built on human reasoning, accountability and contestability.

The gaps in the Indian law, as exacerbated by scientific risks, ethical concerns and legal inconsistencies, highlight the need for a critical assimilation of algorithmic inference into the legal framework. This requires a calibrated response rooted in governance, not prohibition, by re-envisioning forensic AI as algorithmic expert evidence and introducing appropriate provisions of screening, oversight and defence, whereby Indian law can discipline the use of AI without abandoning its benefits. Ultimately, criminal trial is an essentially moral and constitutional exercise. If Artificial Intelligence is to have a role in forensic evidence, it must remain subordinate to human judgment, legal accountability and the requirement of due process.