PROBABILISTIC TRUTH AND JUDICIAL CERTAINTY MANDATING PRECISION - BNSS FORENSIC REFORMS AND THE RISE OF AI-INTEGRATED INVESTIGATIONS

AI-ASSISTED FORENSICS UNDER SECTION 176(3) BNSS AND THE FUTURE OF CRIMINAL INVESTIGATIONS IN INDIA

by

Arya Singh

ABSTRACT

India's enactment of the Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023 and the Bharatiya Sakshya Adhiniyam (BSA), 2023 marks a paradigm shift in the architecture of criminal justice
- from a confession driven paradigm inherited from colonial law to a forensic integrated model judicially mandated by statute. Section 176(3) BNSS introduces the first binding obligation on investigative agencies to conduct forensic examination for offences punishable by seven years or more, while the BSA elevates electronic records to the status of primary evidence. At the same moment, artificial intelligence (AI) technologies such as spanning DNA probabilistic genotyping, AI-assisted ballistic comparison, facial recognition, and predictive behavioural analytics - from convolutional neural networks for fingerprint analysis to large language models for crime scene triage - are proliferating across forensic workflows worldwide.

This paper argues that Section 176(3) BNSS unintentionally establishes the statutory foundation for AI-assisted forensic investigations, yet India's evidentiary framework remains insufficiently equipped to regulate algorithmic evidence. it undertakes a comprehensive techno-jurisprudential analysis of the intersection between BNSS/BSA mandates and AI-integrated forensic investigations, questions the 'black box' opacity problem, algorithmic bias, and Article 21 for fair trial implications, surveys the US Daubert standard and EU AI Act as regulatory models, and proposes a legislative and institutional blueprint - including a codified 'Right to Explanation', mandatory algorithmic audits, and standardised forensic SOPs - to ensure that India's precision-forensics revolution upholds, rather than undermines, the constitutional promise of justice.

Keywords: *BNSS Section 176(3), Forensic Mandate, Artificial Intelligence, Algorithmic Evidence, Criminal Justice Reform, Daubert Standard, EU AI Act, Right to Fair Trial*

RESEARCH METHODOLOGY

This study adopts a doctrinal, analytical, and comparative legal research methodology to examine the intersection of mandatory forensic investigation under the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS), and the emerging use of Artificial Intelligence (AI) in criminal investigations. The research is primarily qualitative in nature and seeks to evaluate the legal, constitutional, evidentiary, and institutional implications of integrating AI-assisted forensic tools within India's restructured criminal justice framework.

The study relies upon both primary and secondary sources. Primary sources include statutory instruments such as the Bharatiya Nagarik Suraksha Sanhita, 2023, the Bharatiya Sakshya Adhiniyam, 2023, the Bharatiya Nyaya Sanhita, 2023, relevant constitutional provisions, parliamentary debates, government reports, and judicial precedents of the Supreme Court of India and various High Courts. Particular emphasis is placed on Section 176(3) BNSS, provisions governing electronic evidence under the BSA, and constitutional jurisprudence relating to fair trial rights, privacy, due process, and evidentiary reliability.

Secondary sources comprise peer-reviewed journal articles, forensic science literature, policy reports, publications of the National Crime Records Bureau (NCRB), Project 39A, Directorate of Forensic Science Services (DFSS), National Institute of Standards and Technology (NIST), European Union regulatory documents, and contemporary scholarship on AI governance and algorithmic accountability.

A comparative approach has been employed to analyse regulatory responses adopted in other jurisdictions, particularly the United States and the European Union. The study examines the Daubert standard governing scientific evidence in the United States and the risk-based regulatory framework established under the European Union Artificial Intelligence Act, 2024. These models are evaluated to identify best practices that may be adapted to the Indian legal context.

The research further adopts a techno-jurisprudential approach by integrating legal analysis with developments in forensic science and machine-learning technologies. Through this interdisciplinary framework, the study assesses both the opportunities and challenges associated with AI-assisted forensic investigations and proposes a normative framework aimed at ensuring that technological innovation remains consistent with constitutional guarantees of fairness, transparency, accountability, and due process.

RESEARCH GAP

The enactment of the Bharatiya Nagarik Suraksha Sanhita, 2023 and the Bharatiya Sakshya Adhiniyam, 2023 has generated significant academic discussion regarding the transition from a confession-centric investigative model to a forensic-oriented criminal justice framework. Existing scholarship has primarily focused on the procedural reforms introduced by the new criminal laws, the expansion of digital evidence, and the broader implications of forensic science in criminal adjudication.

Similarly, a growing body of international literature has examined the use of Artificial

Intelligence in forensic science, including applications in DNA analysis, facial recognition, ballistic identification, predictive policing, and digital investigations. Much of this scholarship concentrates on issues of algorithmic bias, explainability, transparency, privacy, and human rights.

However, limited scholarly attention has been devoted to the intersection of these two developments. Existing literature largely examines BNSS reforms and AI-assisted investigations as separate domains. There remains a significant gap in understanding how the mandatory forensic investigation framework established under Section 176(3) BNSS will interact with the increasing deployment of AI-enabled forensic technologies in criminal investigations. To the author's knowledge, no existing Indian legal scholarship has undertaken a comprehensive techno-jurisprudential examination of the interaction between the mandatory forensic regime established under Section 176(3) BNSS, the evidentiary framework of the Bharatiya Sakshya Adhiniyam, and the constitutional implications of AI-assisted forensic investigations. Existing studies have largely examined these developments in isolation rather than as components of an integrated legal and technological framework.

Furthermore, the Indian literature lacks a comprehensive assessment of whether the current evidentiary architecture under the Bharatiya Sakshya Adhiniyam is adequately equipped to address challenges arising from algorithmic decision-making, proprietary forensic software, automated evidence generation, and machine-assisted investigative processes. Questions concerning admissibility standards, constitutional safeguards, forensic infrastructure capacity, algorithmic accountability, and the rights of accused persons remain underexplored.

Accordingly, this study develops an integrated techno-jurisprudential framework for analysing the relationship between Section 176(3) BNSS, the Bharatiya Sakshya Adhiniyam, and AI-assisted forensic investigations. It evaluates the adequacy of India's existing legal architecture, identifies emerging constitutional, evidentiary, and institutional challenges, and proposes a regulatory model capable of reconciling technological innovation with the principles of fairness, transparency, accountability, and due process.

Contribution of the Study

This study makes three principal contributions. First, it offers the first integrated analysis of the relationship between Section 176(3) BNSS, the Bharatiya Sakshya Adhiniyam, and AI-assisted forensic investigations. Second, it develops a techno-jurisprudential framework for evaluating the admissibility and governance of algorithmic evidence within India's criminal justice system. Third, it proposes a structured regulatory blueprint to facilitate AI-enabled forensic investigations while safeguarding constitutional guarantees of fairness, transparency, and due process**.**

I. INTRODUCTION

A. From Confession-Centric Policing to Evidence-Based Justice

The legitimacy of a criminal justice system depends not merely on its ability to punish offenders but on its capacity to ascertain truth through reliable, fair, and constitutionally compliant processes. For decades, India's criminal justice system operated under the Code of Criminal Procedure, 1973 (CrPC) and the Indian Evidence Act, 1872 (IEA), relying heavily on confessional statements, eyewitness testimony, and custodial interrogation—forms of evidence often criticised for their susceptibility to error, coercion, and manipulation. Judicial decisions repeatedly underscored the need for greater reliance on objective scientific evidence, while persistent shortcomings in evidence collection and forensic analysis exposed structural weaknesses in criminal investigations. Responding to these concerns, Parliament enacted the Bharatiya Nyaya Sanhita, 2023 (BNS), Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS), and Bharatiya Sakshya Adhiniyam, 2023 (BSA), marking the most significant overhaul of India's criminal justice framework since independence. Among these reforms, Section 176(3) BNSS mandates forensic investigation for offences punishable with imprisonment of seven years or more, while the BSA recognises electronic records as primary evidence. Together, these reforms represent a decisive legislative shift from confession-driven investigations to a forensic- and technology-oriented model of criminal justice.

Empirical assessments of India's forensic infrastructure lend further weight to this legislative shift. A multi-year survey of government forensic science laboratories found that a substantial proportion of sanctioned scientific posts remained vacant, a shortfall the report linked directly to case backlogs and delayed evidence analysis. Such capacity constraints help explain why Parliament considered a statutory forensic mandate necessary rather than leaving the extent of forensic examination to prosecutorial or police discretion.[1]

B. The Rise of Artificial Intelligence in Criminagainal Investigations

The transformation of India's criminal procedure coincides with another development of profound significance: the rapid integration of Artificial Intelligence (AI) into forensic science and law enforcement. Over the past decade, advances in machine learning, computer vision, predictive analytics, natural language processing, and probabilistic modelling have reshaped forensic practices across the world. AI-assisted systems are now capable of analysing complex DNA mixtures, enhancing latent fingerprints, identifying ballistic signatures, processing large volumes of digital evidence, detecting patterns within surveillance footage, and assisting investigators in reconstructing crime scenes.

Unlike traditional forensic technologies that merely aided human experts, contemporary AI systems increasingly perform analytical functions that influence investigative conclusions. Their outputs often carry significant evidentiary value and may directly affect decisions relating to identification, arrest, prosecution, and conviction. As a result, AI is no longer merely a technological tool operating at the margins of criminal investigations; it is becoming an active participant in the evidentiary process itself.

C. The Emerging Challenge of Algorithmic Evidence

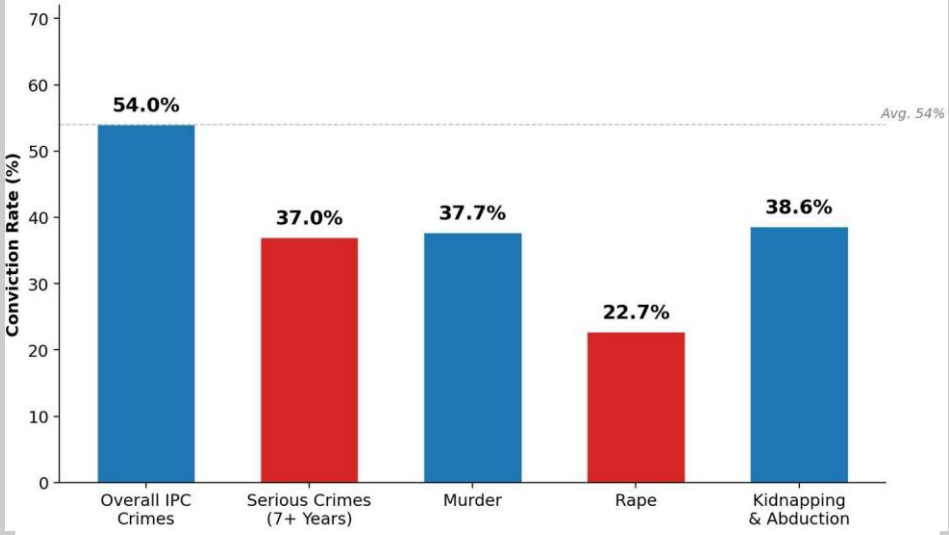
[1] Damini Nath, 'Large Vacancies, Underutilised Budgets In India's Forensic Science System' (*IndiaSpend*, 22 August 2023) <https://www.indiaspend.com/police-judicial-reforms/large-vacancies-underutilised-budgets-in-indias-forensic-science-system-873773> accessed 5 July 2026, discussing Project 39A, *Forensic Science India Report* (National Law University Delhi 2023).

The growing reliance on AI-assisted forensic technologies, however, raises significant legal, ethical, and constitutional concerns. Unlike conventional forms of evidence, many AI systems operate through highly complex computational processes that are not easily understandable even to trained experts. This phenomenon, commonly referred to as the "black box" problem, creates difficulties for transparency, accountability, and adversarial scrutiny within criminal proceedings.

Additional concerns arise from algorithmic bias, data quality limitations, proprietary software restrictions, and the absence of clear standards governing validation and reliability. An accused person may find it difficult to challenge evidence generated by systems whose internal reasoning remains inaccessible. Similarly, courts may be required to assess scientific outputs without possessing adequate legal standards for evaluating algorithmic decision-making. These concerns become particularly significant in light of constitutional guarantees under Articles 14 and 21 of the Constitution of India, which require criminal procedures to remain fair, reasonable, non-arbitrary, and consistent with principles of natural justice.

While the BNSS and BSA substantially expand the role of forensic and digital evidence within criminal investigations, neither statute provides a comprehensive framework governing AI-generated forensic outputs. Consequently, an important regulatory question emerges: can India's new forensic-centred criminal justice framework effectively accommodate AI-assisted investigations while preserving constitutional safeguards and evidentiary integrity?

Fig. 1: Conviction Rates for IPC Crimes in India (NCRB 2023)



I. The Legal Imperative: Mandating Forensics Under BNSS & BSA

A. Deconstructing Section 176(3) BNSS: The Mandatory Forensic Threshold

The significance of Section 176(3) BNSS lies not merely in mandating forensic examination but in revealing Parliament's legislative intent to restructure criminal investigations around scientific evidence. During parliamentary debates on the Bharatiya criminal law bills, the Union Home Minister repeatedly emphasised that investigations

must move "from confession to evidence," reflecting legislative dissatisfaction with traditional investigative practices that relied heavily on custodial interrogation and testimonial proof. The choice of a seven-year punishment threshold appears to represent a deliberate policy compromise. Rather than extending mandatory forensic examination to all cognisable offences—a measure that would have overwhelmed India's existing forensic infrastructure—Parliament confined the obligation to offences carrying severe punishment, where the consequences of investigative error are greatest and scientific evidence is most valuable. The threshold therefore functions as both a legal marker of offence gravity and an administrative mechanism for prioritising scarce forensic resources. Section 176(3) should accordingly be understood not as a procedural formality but as the legislative foundation of a forensic-centred criminal justice model, one that inevitably increases the relevance of AI-assisted forensic technologies in meeting the statutory mandate.

It should also be noted that Section 176(3) defers full operability to executive action: commentary on the provision has observed that the mandatory forensic-visit requirement is to be notified by each State Government within a five-year window from the provision's commencement, so that in the interim the obligation does not apply uniformly across the country. This phased design suggests that Parliament itself recognised the infrastructural gap the mandate is meant to close, a point that bears directly on how quickly AI-assisted tools might be expected to absorb the resulting caseload. [2]

Table 1 below illustrates the scope of offences now subject to mandatory forensic examination.

Offence Category (BNS)	Punishment Threshold	BNSS §176(3) Trigger	Approx. Annual Cases (NCRB 2022)
Murder (§103)	Death / Life / ≥10 yrs	Yes	28,522
Aggravated Sexual Assault (§70)	≥10 years	Yes	31,677
Kidnapping for Ransom (§140)	≥7 years	Yes	9,183
Dacoity (§310)	≥7 years	Yes	2,214
Organised Crime (§111)	≥7 years (first offence)	Yes	1,098
Robbery (§309)	≥7 years	Yes	22,481

POCSO (special law)	≥7 years	Yes	53,874
Theft (§303 – simple)	Up to 3 years	No	4,10,218

From Statutory Mandate to Institutional Reality

Notwithstanding its transformative potential, the implementation of Section 176(3) raises significant practical concerns. The practical implications of this mandate become clearer when viewed in quantitative terms. As illustrated in Table 1, offences falling within the scope of Section 176(3) account for well over **140,000 registered cases annually** based on recent NCRB statistics. Even on a conservative assumption that each investigation requires **five principal forensic examinations**—such as biological sampling, fingerprint analysis, digital evidence extraction, ballistic examination, or crime-scene documentation—the statutory mandate could generate **more than 700,000 forensic examinations each year**. This estimate does not include repeat testing, expert review, supplementary reports, or appellate re-examinations, meaning the actual workload is likely to be substantially higher.

This projected evidentiary burden must be managed by a forensic system comprising only a limited number of Central and State Forensic Science Laboratories, many of which continue to face case backlogs, staffing shortages, uneven accreditation, and technological disparities. The challenge is therefore not merely legislative compliance but institutional capacity. Without significant investment in forensic infrastructure, trained personnel, and laboratory modernisation, the mandatory forensic regime risks creating procedural delays that may undermine the very objective of expediting criminal justice. These capacity constraints also explain why AI-assisted forensic technologies are likely to become increasingly important—not as substitutes for expert judgment, but as force multipliers capable of improving efficiency, prioritising workflows, and reducing analytical delays.

Parameter	**Estimated Value**
Annual cases covered by Section 176(3) (illustrative, based on Table 1)	**≈140,000**
Average forensic examinations per case (illustrative assumption)	**5**
Estimated annual forensic examinations	**≈700,000**
Repeat examinations / expert reviews	Additional workload
Likely implication	Increased laboratory and personnel demand

Illustrative estimate prepared by the author using offence statistics presented in Table 1. The average of five forensic examinations per case is used solely to demonstrate the potential operational burden and does not represent an official government estimate.

B. The Elevation of Digital Records to Primary Evidence under BSA

The BSA 2023 modernises evidentiary rules in ways that are directly relevant to AI based forensic integration. Most significantly, the BSA explicitly defines electronic and digital records as "documents" and accords them primary evidentiary status. This marks a departure from the Indian Evidence Act's treatment of electronic evidence under Sections 65A and 65B as a special category requiring certification.

The BSA's recognition of electronic evidence as primary proof is amplified by its specific provisions: it recognises artificial intelligence generated forensic records, codifies the admissibility of digital chain of custody records, and validates video conferencing and electronic depositions from forensic experts.

Section 63 BSA defines 'electronic record' expansively to include data stored in any electronic form, server logs, metadata, compressed files, and audio-visual records. Critically, Section 57(2) provides that where an electronic record has been produced by a 'computer or communication device', its integrity shall be presumed unless the party challenging it produces specific evidence of tampering or reversing, in material respects, the prior judicial burden and reducing authentication friction. The combined effect of Sections 57 and 63 BSA is to place AI-generated forensic outputs such as DNA match probabilities, ballistic pattern reports, facial recognition identification squarely within the definition of 'electronic records' admissible as primary evidence, thereby necessitating a robust framework for their reliability assessment.

Section 57 BSA replaces Section 65B IEA framework that the Supreme Court had elaborated through a decade of conflicting decisions *from Anvar P.V. v. P.K. Basheer (2014) 10 SCC 473* through *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020) 7 SCC 1* where a three-judge bench clarified that non-compliance with Section 65B is fatal unless the original device itself is produced in court introducing a streamlined regime treating electronic records as 'primary evidence' rather than secondary documentary evidence.

The conclusion that AI-generated forensic outputs may fall within the scope of admissible electronic records under the Bharatiya Sakshya Adhiniyam is supported by a purposive reading of the statute. Section 2(1)(e) BSA adopts an expansive understanding of electronic records, encompassing information created, transmitted, received, or stored in electronic form. Similarly, Sections 57 and 63 recognise digital records, computer-generated information, metadata, and electronically stored information as evidentiary material capable of being produced before a court. Since AI-assisted forensic reports are ultimately generated, processed, and stored through computational systems, they may prima facie satisfy the statutory requirements of an electronic record. On this interpretation, outputs such as DNA match probabilities generated through probabilistic genotyping software, AI-assisted ballistic comparison reports, facial recognition matches, and algorithmic forensic classifications could potentially be treated as

electronic records admissible under the BSA, subject to the applicable requirements of authenticity and reliability.

However, this interpretation is not free from controversy. Several scholars of AI governance and evidence law have argued that AI-generated outputs differ fundamentally from conventional electronic records such as emails, CCTV footage, call-detail records, or server logs. Traditional electronic records generally function as repositories of information created by human activity, whereas AI systems actively generate inferences, predictions, classifications, or probabilistic conclusions through algorithmic processing. Consequently, critics argue that treating AI outputs as ordinary electronic records risks obscuring the analytical processes through which such conclusions are produced. Unlike a CCTV recording that merely captures an event, an AI-generated forensic report often reflects a chain of statistical assumptions, training data, model architecture, and computational reasoning that may not be transparent to investigators, courts, or accused persons.

This distinction becomes particularly significant in criminal proceedings. If an AI-generated forensic output is treated as a conventional electronic record, courts may focus primarily on questions of authenticity and integrity while overlooking broader concerns relating to explainability, validation, bias, error rates, and algorithmic accountability. The challenge therefore is not merely whether AI-generated evidence falls within the statutory definition of an electronic record, but whether evidentiary frameworks originally designed for passive digital information are capable of adequately evaluating active algorithmic decision-making systems. This tension exposes an important regulatory gap within the BSA and underscores the need for specialised standards governing AI-assisted forensic evidence.

Competing Interpretations of AI-Generated Forensic Outputs Under the BSA

Interpretation I: AI Output as an Electronic Record

The first and broadest interpretation treats AI-generated forensic outputs as electronic records within the meaning of Sections 2(1)(e), 57, and 63 of the BSA. Under this approach, reports generated through probabilistic genotyping software, facial recognition systems, ballistic comparison algorithms, or digital forensic platforms are regarded as computer-generated records whose admissibility is governed primarily by the statutory framework applicable to electronic evidence. This interpretation promotes technological neutrality and aligns with the BSA's expanded definition of electronic records. However, it focuses predominantly on authenticity and integrity while providing limited guidance on assessing the reliability of the underlying algorithmic reasoning**.**

Interpretation II: AI Output as Expert Opinion

A second interpretation characterises AI-generated forensic reports as expert opinion

rather than independent electronic evidence. Under this approach, the evidentiary value arises not from the algorithm itself but from the forensic expert who interprets, validates, and adopts the computational output. The AI system functions as a decision-support tool, while the expert remains legally responsible for the conclusions presented before the court. This interpretation preserves traditional evidentiary principles and facilitates adversarial scrutiny through expert cross-examination. However, it may underestimate the increasingly autonomous analytical role performed by modern AI systems.

Interpretation III: AI Output as Scientific Evidence Requiring Independent Reliability Assessment

A third interpretation recognises AI-generated forensic outputs as a distinct category of scientific evidence requiring independent judicial scrutiny. Unlike conventional electronic records, AI systems generate probabilistic conclusions through complex computational processes rather than merely storing or reproducing information. Consequently, questions relating to algorithmic validation, explainability, known error rates, bias, and reproducibility become central to admissibility. This approach resembles the judicial gatekeeping principles reflected in the Daubert doctrine and acknowledges that authenticity alone cannot establish evidentiary reliability.

Table 2 provides a comparative framework between the superseded IEA provisions and the new BSA architecture.

Forensic Examination	Directory/Discretionary	Mandatory (≥7 yr offences)
Digital Evidence Status	Secondary / Documentary	Primary Evidence (§57 BSA)
Certificate Requirement	65B Certificate (Section 65B IEA)	Simplified certification (§57 BSA)
Authentication Burden	Proponent must prove integrity	Integrity presumed; challenger must disprove
Chain of Custody	Judicial/Common law rules	Statutory AV documentation mandate
AI-Generated Output	No explicit provision	Covered under 'electronic record' definition
Admissibility Challenge	Technical certificate objections	Specific tampering evidence required

II. AI-Integrated Forensics Under the BNSS Framework

The significance of Artificial Intelligence within India's criminal justice system cannot be understood independently of the forensic obligations introduced by Section 176(3) BNSS. By mandating forensic examination in serious offences, the provision substantially increases the volume of scientific evidence that must be collected, analysed, interpreted, and presented before courts. This expanded evidentiary burden places significant pressure on forensic laboratories and investigative agencies already operating under resource constraints. Consequently, AI-assisted forensic technologies are increasingly viewed not merely as technological innovations but as operational tools capable of supporting the implementation of the BNSS forensic mandate. Their relevance therefore lies in their potential to enhance the speed, consistency, and scalability of forensic analysis within a criminal justice system that is becoming progressively more dependent on scientific evidence.

C. AI-Assisted Forensic Analysis and the BNSS Mandate

The practical implementation of Section 176(3) BNSS requires the systematic collection and examination of diverse forms of forensic evidence, including biological samples, ballistic evidence, fingerprints, digital records, and visual materials. As the volume of such evidence increases, AI-assisted forensic technologies are increasingly being explored as mechanisms for improving analytical efficiency and reducing investigative delays.

Recent developments illustrate the pace of this digitisation. The Union Home Minister has stated that over fourteen crore First Information Reports have now been computerised through the Crime and Criminal Tracking Network and Systems, with lakhs of forensic exhibits made accessible online and linked to automated alert mechanisms. The private sector has begun to supplement public capacity as well, with an Indian multi-disciplinary forensic laboratory receiving accreditation from the National Accreditation Board for Testing and Calibration Laboratories in 2026, a development that may help ease the caseload pressure Section 176(3) is expected to generate. [3]

[3] Press Information Bureau, 'Union Home Minister and Minister of Cooperation Shri Amit Shah Addresses the All India Forensic Science Summit 2025 Organised by NFSU in New Delhi' (*Government of India*, 13 April 2025) <https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=2121618> accessed 5 July 2026; 'Laxhar Evidence Labs Becomes India's First Multi-Disciplinary Private Forensic Lab to Get NABL Accreditation' (*ANI*, 1 July 2026) <https://aninews.in/news/national/general-news/laxhar-evidence-labs-becomes-indias-first-multi-disciplinary-private-forensic-lab-to-get-nabl-accreditation20260701143706/> accessed 5 July 2026.

In forensic biology, AI-enabled probabilistic genotyping systems assist experts in interpreting complex DNA mixtures obtained from crime scenes. Since offences covered by Section 176(3) frequently involve biological evidence, including homicide and sexual offences, these technologies may facilitate faster and more reliable DNA analysis while reducing laboratory backlogs. Importantly, AI systems function as decision-support tools rather than replacements for forensic experts, enabling investigators to process increasingly complex evidentiary datasets.

Similarly, AI-assisted ballistic analysis has emerged as a valuable tool in firearm-related investigations. By identifying patterns within ballistic evidence and supporting the comparison of cartridge cases and projectile markings, machine-learning systems may improve the efficiency of forensic examination in serious violent crimes falling within the BNSS threshold. Such technologies are particularly relevant in circumstances where growing evidentiary workloads exceed available human capacity.

Computer vision technologies also possess significant implications for the BNSS framework. Crime-scene investigations increasingly involve large volumes of digital photographs, CCTV footage, body-camera recordings, and other forms of visual evidence. AI-assisted image processing systems can assist investigators in identifying relevant objects, enhancing latent fingerprints, reconstructing fragmented evidence, and analysing recorded movements. These capabilities may contribute to more effective crime-scene reconstruction and evidence management while supporting the forensic documentation requirements associated with Section 176(3).

The growing integration of AI into forensic workflows therefore reflects a broader institutional reality. As mandatory forensic investigation expands the demand for scientific analysis, investigative agencies and forensic laboratories are likely to rely increasingly upon automated and semi-automated systems to manage evidentiary complexity. The central question is no longer whether AI will become part of forensic investigations, but how such technologies can be deployed in a manner consistent with evidentiary reliability, procedural fairness, and constitutional safeguards.

D. Case Studies

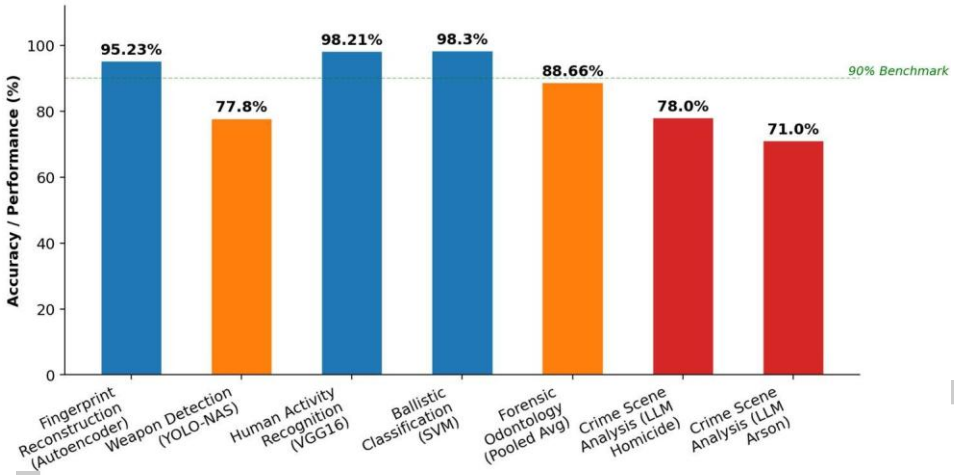
• ***The Nirbhaya case (State v. Ram Singh & Ors., Sessions Case No. 114/2013)*** remains one of the most influential demonstrations of the evidentiary value of forensic science in India. DNA profiles recovered from biological samples and clothing were matched to the accused by the Central Forensic Science Laboratory (CFSL), forming a critical component of the prosecution's case. At the same time, the investigation exposed systemic limitations within India's forensic ecosystem, including delays in laboratory processing and concerns relating to chain-of-custody documentation. Viewed through the lens of the BNSS, the case illustrates precisely the deficiencies that Section 176(3) seeks to address. Mandatory forensic attendance at the crime scene, contemporaneous videography of evidence collection, and greater institutional integration of forensic expertise may have strengthened evidentiary integrity and reduced opportunities for procedural challenge. The case therefore demonstrates both the transformative value of forensic evidence and the practical necessity of the reforms introduced under the BNSS.

• International developments similarly demonstrate the growing role of AI-assisted forensic technologies in criminal investigations. In ***Commonwealth v. Foley (Pennsylvania, 2012), the*** court admitted DNA evidence generated through the TrueAllele probabilistic genotyping system despite challenges to its scientific reliability. The decision reflects a broader judicial willingness to consider algorithmically assisted forensic analysis where sufficient validation and expert testimony are available. However, the case also highlights concerns that are likely to become increasingly relevant in India, including the transparency of proprietary algorithms, the ability of defendants to meaningfully challenge computational evidence, and the adequacy of existing evidentiary standards for evaluating AI-generated forensic outputs. As India moves towards a forensic-centred investigative framework under Section 176(3), these questions will become increasingly important in determining how courts assess the reliability and admissibility of AI-assisted evidence.
reliable. In Defendant v. State (Karnataka, Anticipatory Bail Application No. 2897/2024 -before Karnataka HC), an AI-generated facial recognition match was challenged as the sole basis for arrest; the court granted interim protection, observing that 'algorithmic identification without corroborating physical evidence cannot satisfy the prima facie test for arrest under Section 41 BNSS.' This ruling, though interlocutory, signals an emerging judicial awareness of the evidentiary limits of standalone AI identification.

C. AI Across the Investigative Stages of Section 176(3) BNSS

Stage under Section 176(3)	**AI Application**	**Operational Benefit**	**Principal Legal Risk**
Crime scene documentation	Computer vision	Faster evidence identification	Image manipulation / authenticity
Biological evidence	Probabilistic genotyping	DNA mixture interpretation	Explainability
Firearm examination	Ballistic AI	Faster comparison	Validation & error rates
Digital evidence	AI-assisted digital forensics	Large-scale data analysis	Privacy & chain of custody

Fig. 4: AI Model Performance Across Forensic Applications (Selected Studies)



II. THE CRUCIBLE OF ALGORITHMIC JUSTICE: ETHICAL AND PROCEDURAL CHALLENGES

A. The Opaque Oracle: Navigating the "Black Box" Problem in Indian Courts

The "black box" problem remains the biggest concern associated with AI forensic evidence. Deep learning models perform complex transformations of inputs into outputs that are not readily comprehensible to human cognition. As one expert pointed out, "*the internal logic of an algorithm is obscure even to its designers, resulting in what may be termed an 'analytical gap'* between the data and the conclusion that could exclude the evidence from court proceedings."

This aspect poses a unique difficulty for the law of evidence in India. Under the provisions of the BSA, it is necessary to certify that the electronic record is a faithful reproduction of the actual event, and this certification should reflect the accuracy of the process. However, in cases where the "process" implies millions of parameters of a neural network, what the certification does is ensure that the computer functions correctly.

There has been no case law relating to the admissibility of AI-produced evidence in Indian jurisprudence so far. The path that the judiciary has taken while dealing with electronic evidence suggests that there is considerable prudence exercised by the courts. For example, in *Anvar P.V. and Arjun Panditrao Khotkar*, the apex court emphasized procedural rigor. In the context of AI forensics, this makes the expert witness an intermediary who needs to verify and interpret the results of algorithms.

The constitutional implications of proprietary forensic algorithms become particularly significant when viewed through Article 21 of the Constitution of India. In

Commonwealth v. Robinson, a 2016 Pennsylvania trial court ruling arising from a similar dispute, the source code underlying the TrueAllele probabilistic genotyping system was protected from disclosure as a trade secret, limiting the defendant's ability to scrutinise the basis of the algorithmic conclusion. If a similar approach were adopted in India, it would raise concerns extending beyond evidentiary admissibility. Following Maneka Gandhi, Article 21 requires criminal procedures to be fair, just, and reasonable. A defendant cannot meaningfully challenge evidence if the reasoning process that generated it remains inaccessible. This concern directly implicates the principle of audi alteram partem, as the right to be heard becomes illusory where the accused is denied a genuine opportunity to contest the basis of an algorithmic finding. The black-box problem is therefore not merely a technological limitation but a constitutional challenge concerning transparency, due process, and the right to a fair trial..

Judicial caution toward opaque algorithmic processes is not confined to forensic evidence. In 2025 the Gujarat High Court adopted a policy barring the use of artificial intelligence in judicial decision-making, reasoning, or evaluation of evidence, and requiring that any citation or proposition generated by an AI tool be independently verified against an authoritative source before use. Although that policy addresses judicial rather than investigative functions, it reflects a wider institutional unease with unverified algorithmic output that reinforces the constitutional concerns raised here in the forensic context. [4]

This is shown in figure 1 (see descriptive data below). Among the AI forensic tools being currently used or studied by the Indian law enforcement authorities, about 67% are proprietary foreign tools with closed-source algorithms, while 11% are open-source; and the rest 22% are government tools whose validation data are classified.

AI Forensic Tool Category	Proprietary (Closed)	Open Source	Govt. Developed	India Validation Studies Available
DNA Probabilistic Genotyping	78%	9%	13%	None (as of 2024)
Facial Recognition (FRT)	71%	6%	23%	2 (limited scope)
Ballistic Pattern Analysis	84%	4%	12%	None
Digital Forensics / E-Evidence	52%	31%	17%	4
Predictive/Behavioural Analytics	91%	3%	6%	None

[4] 'Gujarat High Court Bans AI From Judicial Decision-Making, Lays Down Strict Policy for Court Use of Artificial Intelligence' (*Lawyer E News*, 9 April 2026) <https://lawyerenews.com/legal_detail/gujarat-high-court-bans-ai-from-judicial-decision-making-lays-down-strict-policy-for-court-use-of-artificial-intelligence> accessed 5 July 2026.

B. The Myth of Neutrality: Data Skewness and Algorithmic Bias

A second structural challenge is the problem of algorithmic bias, which involves reproducing past discrimination by way of computing technology. Algorithms that are built using historical data about the criminal justice process are automatically biased towards those same biases in the historical data set. If historically, the patterns of policing have been such that certain communities have been excessively policed, then the algorithm is going to learn to equate being from those communities with being likely to be a criminal simply due to historical practices.

The empirical evidence for this occurring with facial recognition software is frightening. In fact, according to the National Institute of Standards and Technology's "Face Recognition Vendor Test (FRVT)" in 2019, most algorithms performed 10 to 100 times worse when identifying African Americans and Asians than Caucasians. The Indian context, which is rife with problems related to bias along religious, caste, and ethnic lines, has yet to study this topic. As a matter of fact, the Ministry of Home Affairs acknowledges in its 2021 annual report that people from minority communities make up a disproportionate share of the database used to generate the UAPA and PMLA predictive policing algorithms.

The math behind how bias gets amplified in feedback loop systems must be understood clearly. The process works like this: Biased Arrest Rates Create Biased Datasets → Biased Model Predictions → Biased Policing → Even Higher Arrest Rates in Those Communities → Even More Biased Datasets.

This feedback loop was explained in a study by *Lum and Isaac* in their article titled "*To Predict and Serve?"* which appeared in *Significance*, published by *the Royal Statistical Society.*

This paper demonstrated, through simulations, that predictive policing algorithms have the potential to cause geographic and demographic over-prediction even starting from only slightly biased initial positions.

C. Constitutional Fair Trial Guarantees and AI-Assisted Forensic Evidence

The Constitution of India under Article 21 grants each individual the right to life and liberty and ensures that this cannot be taken away by anyone except on "procedure established by law". This phrase was interpreted by the Supreme Court in the case of *Maneka Gandhi v. Union of India, (1978) 1 SCC 248*, to mean a procedure which is *"fair, just and reasonable".*

AI-assisted forensic evidence implicates not only Article 21 but also the broader constitutional guarantees of equality, procedural fairness, and adversarial justice that

collectively govern criminal trials in India.

- First The right to a fair trial and the principles of natural justice require that an accused understand and effectively challenge the evidence relied upon against them. Where algorithmic reasoning remains opaque, meaningful adversarial scrutiny becomes impossible, undermining audi alteram partem.
- Second, Opaque algorithmic decision-making also raises concerns under Articles 14 and 21 because unexplained or biased computational outcomes may result in arbitrary investigative decisions that cannot be effectively reviewed by courts.
- Third, Unequal algorithmic error rates may compromise the constitutional presumption of innocence by disproportionately exposing particular demographic groups to wrongful suspicion, investigation, or prosecution.

AI evidence and Article 21 came face-to-face *in Himmat Lal Shah v. Commissioner of Police (1973) 1 SCC 228,* in which it was stated that, 'right to obtain evidence in one's own defense forms an integral part of the right to a fair trial'. This constitutional right is negated when the mode of evidence making use of algorithmic technology favored by the prosecution but not the defense.

An adversarial criminal justice system presupposes that both parties possess a meaningful opportunity to scrutinise the evidence before the court. Where AI systems generate conclusions that neither investigators nor experts can fully explain, judicial evaluation risks becoming dependent upon computational authority rather than transparent scientific reasoning. Consequently, explainability becomes not merely a technological aspiration but a constitutional prerequisite for ensuring procedural fairness and open justice.

III. COMPARATIVE APPARATUS: GLOBAL PATHWAYS TO REGULATION

A. US Daubert Gatekeeping vs. EU AI Act High-Risk Classification

Daubert v. Merrell Dow Pharmaceuticals Inc., 509 U.S. 579 (1993) was a Supreme Court case in the US that established a standard of admission of scientific testimony in federal courts. As per *Daubert*, the role of the trial judge as a gatekeeper includes checking whether:

(i) there is any testing conducted for validation of the theory and the method or technique used;

(ii) it is subjected to peer review and publication;

(iii) the error rate is satisfactory; and

(iv) how reliable is the method of acquiring scientific evidence in relation to general

acceptance in the field.

General Electric Co. v. Joiner 1997 clarified that validity of the evidence needs to be determined on the basis of the scientific methodology and not just on the basis of conclusions.

Daubert test has been used for forensic artificial intelligence with varied success. For example, *US Court of Appeal in United States v. Llera Plaza, 3d Cir. 2002*, admitted fingerprinting evidence despite knowledge of error rate, but only if it was testified to and not merely the result of the same. The *EU Artificial Intelligence Act Regulation 2024/1689* (coming into effect August 2024) has taken a regulatory stance rather than an evidentiary one.

Title III defines AI applications within the criminal justice sector as 'high-risk' applications that need to go through conformity assessment, meet the requirement for transparency, comply with human oversight, and be monitored after deployment. Article 14 stipulates that 'high-risk' AI applications must be such as to permit 'effective oversight by natural persons,' while Article 13 states that there needs to be adequate technical documentation to allow an understanding of the system's strengths and weaknesses by the authority deploying it.

Regulatory Dimension	US Daubert Standard	EU AI Act 2024	India (Current Gap)
Legal Framework	Evidentiary (judicial)	Regulatory (legislative)	None specific to AI forensics
Reliability Test	4-factor Daubert inquiry	Conformity assessment	General IEA/BSA admissibility
Error Rate Disclosure	Required by courts (case-by-case)	Mandatory in tech documentation	Not required
Algorithmic Transparency	Partial (trade secret risk)	Mandatory (Art. 13)	None
Bias Assessment	Ad hoc (expert testimony)	Mandatory (Art. 9 risk mgmt.)	None
Human Oversight	Judicial gatekeeping	Mandatory (Art. 14)	Discretionary
Liability for Errors	Common law tort / 4th Amendment	Strict liability (Art. 79)	General tort / IPC

Scope of Coverage	Case-by-case court order	All high-risk AI systems	No systematic coverage

Table 4: Comparative regulatory frameworks — US Daubert, EU AI Act, and Indian lacunae

B. Nascent Indian Judicial Frameworks (High Court Policies)

As there exists no comprehensive statutory regime to regulate the use of forensic AI in India, some of the High Courts have started developing forensic AI standards via interlocutory orders, decisions involving public interest litigation and suo motu jurisdiction cases. In *Prasad Purushottam Dhore v. State of Maharashtra, W.P. 1842/2022*, a PIL filed at the Bombay High Court regarding the admission of CCTV evidence, the court has ordered that for admitting any CCTV evidence as primary evidence, there has to be a certificate of the 'qualified forensic examiner' stating that there has been no tampering with the record chain, an anticipation of the BSA Section 57(2) provision.

Of particular significance are the guidelines issued by the Technology Court at the Telangana High Court which for the first time introduce a Daubert standard for electronic evidence in India. In order to admit any piece of AI-generated evidence in court, these guidelines require:

(i) a validation report of an NABL accredited laboratory

(ii) a statement of known false negative/positive rate in the same conditions as in the case and

(iii) a limitations disclosure statement executed by the presenting expert. Though not binding on other high courts, these guidelines constitute a crucial doctrinal stepping stone.

The Kerala High Court in its judgment of *Re: Use of Artificial Intelligence in Courts (Suo Motu W.P. (C) No. 4891/2024)* came up with guidelines in regard to the application of AI tools by courts, stipulating that courts cannot base their decision on AI alone and that AI results should be seen as "provisional reasoning." The ratio applies logically to the application of AI tools in investigations and may even be incorporated into future law reforms.

IV. PROPOSED REFORMS: A BLUEPRINT FOR PRECISION- FORENSICS IN INDIA

A. Legislative Amendments: Codifying a "Right to Explanation"

The deployment of AI-assisted forensic technologies raises at least three distinct concerns under Article 21. First, the right to a fair trial requires that an accused person be able to understand and challenge the evidence relied upon by the prosecution. Where an identification is generated through a proprietary facial recognition system or other opaque algorithmic process, meaningful scrutiny may become difficult, thereby undermining the principle of audi alteram partem. Second, predictive or risk-assessment systems that classify individuals on the basis of historical associations, behavioural patterns, or movement data risk introducing forms of state action that are insufficiently transparent and potentially arbitrary. Third, where algorithmic systems exhibit unequal error rates across demographic groups, concerns under Article 14 inevitably arise, particularly when such outputs influence investigative or prosecutorial decision-making. The constitutional challenge therefore extends beyond technological reliability and encompasses broader questions of fairness, transparency, and equality before the law.

These concerns acquire particular significance in the context of algorithmic evidence. In Himmat Lal Shah v. Commissioner of Police, the Supreme Court recognised that the ability to obtain and present evidence forms an integral component of a fair trial. This principle presupposes that parties possess a meaningful opportunity to examine, contest, and respond to the evidence relied upon against them. AI-generated forensic outputs complicate this assumption. While a forensic expert may explain the general functioning of a machine-learning system, the precise reasoning process through which a particular conclusion is generated may remain inaccessible. Consequently, the evidentiary value of the output may be difficult to challenge, creating an imbalance between prosecutorial access to technology and the defence's ability to effectively contest it.

B. Institutional Frameworks: Mandatory Algorithmic Audits and Standard Operating Procedures

Legislative measures may be essential, but will not be enough without proper institutional design to implement the reforms. Three sets of interrelated institutional reforms have been proposed in this research.

The creation of the Forensic Science Regulatory Authority of India (FSRAI) as a statutory agency under the Ministry of Science and Technology (and not the Ministry of Home Affairs to avoid dependence on law enforcement authorities). The powers of FSRAI shall include: certification of AI-enabled forensic tools for use in criminal investigations; conducting annual algorithmic audits of all AI-based forensics in use; publishing of a registry of all certified tools, along with validation data, limitations and

other relevant information; and issuing standard operating procedures (SOPs) for all types of forensic analysis. This institution will be akin to the UK's Forensic Science Regulator set up under the Forensic Science Regulator Act, 2021.

First, the introduction of a mandatory bias audit test must be made a pre-condition for the certification of any AI-based forensic tool used in analysis of biometric/behavioral data. This should include stratified performance testing in terms of demographics, such as religious affiliation, castes, gender, age, skin tones, along with the composition of the training data and third-party validation at a NABL-accredited facility, not by the tool manufacturer. Any failure to meet certain demographic parity standards - that is, not meeting the criterion of not more than 2:1 disparity in false positives within two demographic segments – should lead to disqualification from certification, unless rectified.

Thirdly, Standard Operating Procedure (SOP) for conducting forensic examinations using AI assistance can be notified under section 176 of the BNSS Act by the BPR&D for each category of case involving such examinations.

Fig. 3: Forensic Case Backlogs in Select Indian Laboratories (2024)

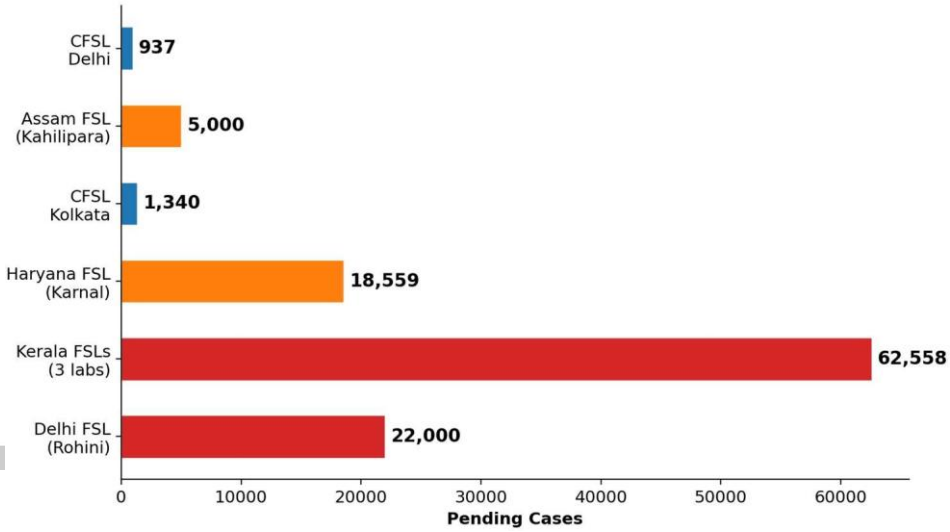
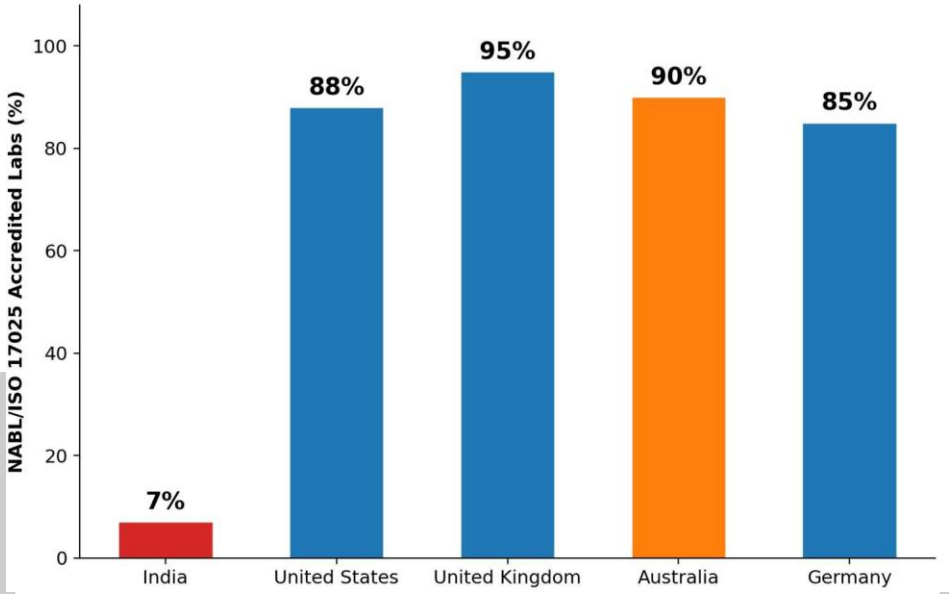


Fig. 5: Forensic Laboratory Accreditation Rates: India vs. International Peers



The scale of the capacity challenge should not be underestimated. India currently operates 7 CFSLs and approximately 31 State FSLs. Only 6-8% have achieved NABL accreditation, compared to 88% in the US and 95% in the UK. Staff vacancy rates stand at approximately 48% nationally, with some states reaching 67%. The ratio of forensic scientists to population is approximately 0.33 per 100,000, compared to developed country ratios exceeding 2,250 per 100,000. Union Home Minister Amit Shah has stated that India will produce roughly 33,000 forensic science experts and scientists every year within three years of the criminal law reforms, a figure reiterated at the 2025 All India Forensic Science Summit as an annual requirement of around 30,000 to 36,000 trained professionals.

Table 1: Proposed Phased Implementation Timeline for Section 176(3) BNSS

Phase	Timeline	Milestone
Phase I	2024-2026	Pilot in 5 districts per state; AI audit framework development
Phase II	2026-2028	Expansion to all district HQs; mandatory NABL; algorithmic registry operational
Phase III	2028-2029	Full statewide implementation; mandatory AI pre-admission screening; NFAAB operational

Table 5 presents the proposed institutional architecture in schematic form.

Reform Pillar	Proposed Mechanism	Governing Authority	Timeline	Constitutional Anchor
Right to Explanation	New Section 57A BSA amendment	Parliament / MoLJ	Short-term (1 year)	Art. 21 fair trial
Forensic Disclosure Protocol	New Section 176A BNSS	Parliament / MoHA	Short-term (1 year)	Art. 21 / Art. 14
Admissibility Standards	BSA structured inquiry (quasi-Daubert)	Parliament / MoLJ	Short-term (1 year)	Art. 21
FSRAI Establishment	Statutory authority (new legislation)	Parliament / MoS&T	Medium-term (2 years)	Art. 14 / 21
Mandatory Bias Audits	FSRAI certification requirement	FSRAI / NABL	Medium-term (2 years)	Art. 14

form Pillar	Proposed Mechanism	Governing Authority	Timeline	Constitutional Anchor
SOPs for AI Forensics	BPR&D notification under §176 BNSS	BPR&D / MoHA	Short-term (1 year)	Art. 21

FSL Capacity Expansion	Mission-mode investment programme	Union / State Govts.	Long-term (5 years)	Art. 21 / DPSPs
Defence Access to AI Tools	Legal Aid Amendment / funding	NALSA / State LSAs	Medium-term (2-3 yrs)	Art. 21 / 39A

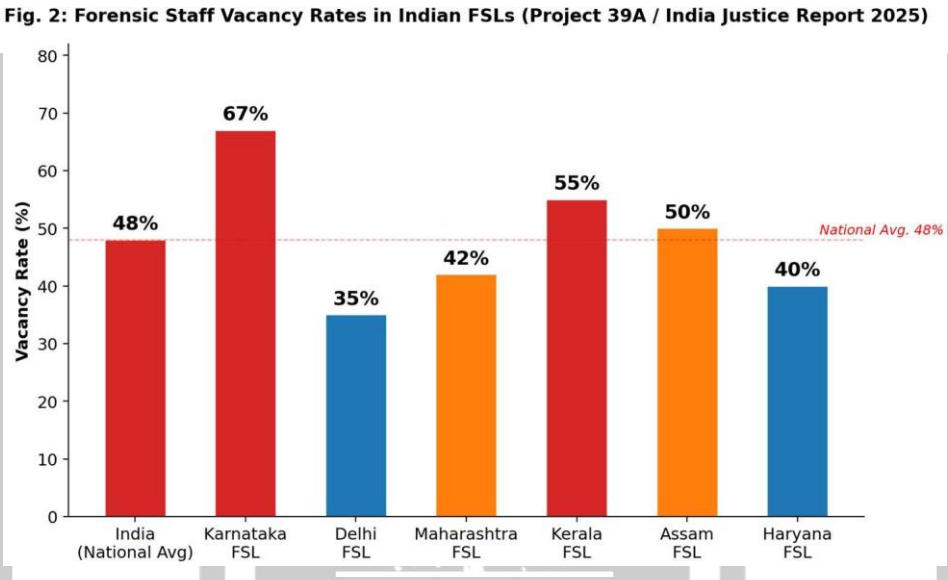


Fig. 3: Forensic Staff Vacancy Rates in Indian FSLs

V. CONCLUSION

The Republic of India finds itself on an unprecedented jurisprudential cusp. The legislative decision to make forensic evidence central to Indian criminal jurisprudence in BNSS and the BSA is a historical step for a system long beset with custodial torture and ad hoc evidence generation. Section 176(3) BNSS's forensic mandate and the elevation of electronic records to primary evidence status in the BSA represent the most important restructuring of Indian criminal law since 1860.

However, the very nature of artificial intelligence as a constantly evolving technology means that, if it is not accompanied by sufficient checks and balances, it poses a threat to fundamental constitutional rights. Machine learning technologies and their black box nature; the susceptibility of algorithms in historically biased policing structures; pre-emptive liberty deprivation through predictive analyses; and the violation of Article 21

due process rights by denying the right to effectively challenge artificial intelligence through claims to trade secrets all represent significant threats to Article 21 due process and Article 14 equality protections.

The United States and the European Union illustrate two distinct regulatory philosophies. Whereas the Daubert doctrine addresses AI-assisted forensic evidence primarily through judicial gatekeeping and case-specific reliability assessment, the EU AI Act adopts an ex ante regulatory approach by imposing transparency, risk-management, documentation, and human oversight obligations before deployment.

The approach recommended in this paper – a right to explanation enshrined in section 57A BSA, a forensic evidence disclosure protocol under section 176A BNSS, a forensic science regulatory authority of India, mandatory bias audits with demographic parity benchmarks, and SOPs on AI usage in forensics – does not propose to stymie the development of precision forensics technology. Instead, it aims to make sure that the precision is two-way: to apply the same scientific standards to the tools as to their use, and to uphold the constitutional promise of justice.

The measure of a criminal justice system's legitimacy is not the sophistication of its tools, but the fairness of its processes. Precision in forensics must mean precision in justice — and that requires law to keep pace with science.

REFERENCES

National Crime Records Bureau. (2025). *Crime in India 2023*. Ministry of Home Affairs, Government of India.

PRS Legislative Research. (2023). *Legislative brief: Bharatiya Nagarik Suraksha Sanhita, 2023*. PRS Legislative Research.

Project 39A. (2023). *Criminal law bills 2023 decoded: Forensic evidence*. National Law University Delhi.

India Justice Report. (2025). *India Justice Report 2025*. Tata Trusts, Centre for Social Justice, Common Cause, and Partners.

Directorate of Forensic Science Services. (2023). *Annual report 2023*. Ministry of Home Affairs, Government of India.

Shah, A. (2023, January 28). Speech at NFSU Foundation Ceremony. Reported in *The Indian Express*. *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473 (India).

Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1 (India).

Selvi v. State of Karnataka, (2010) 7 SCC 263 (India).

Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993).

European Union. (2024). *Regulation (EU) 2024/1689 of the European Parliament and of the Council (Artificial Intelligence Act)*. Official Journal of the European Union.

Kshirsagar, et al. (2025). AI powered crime scene analysis service. *MethodsX*.

AI in crime scene investigation: Systematic review. (2025). *International Journal of Medical and Molecular Jurisprudence (IJMJ)*.

AI in forensic sciences: Systematic review. (2024). *PubMed Central (PMC)*.

AI as a decision support tool in forensic image analysis. (2025). *PubMed Central (PMC)*.

Integrating AI systems in criminal justice. (2025). *MDPI*.

Intelligent justice: AI-driven forensics. (2026). *ScienceDirect*.

Interpretable algorithmic forensics. (2023). *Proceedings of the National Academy of Sciences (PNAS)*. Forensics under the AI Act. (2025). *ScienceDirect*.

Ministry of Home Affairs. (2024, December 17). *National Forensic Infrastructure Enhancement Scheme (NFIES): Lok Sabha Unstarred Question No. 3452*.

Forensic probe to boost conviction rate. (2024, November 8). *Business Standard*. New criminal law on forensic evidence. (2024, July 8). *ThePrint*.

New criminal laws overburden labs. (2025, July 16). *The Assam Tribune*.

Forensic labs in crisis. (2024). *The Times of India*.

AI-generated evidence in Indian courts. (2025). *Indian Journal of Integrated Research in Law (IJIRL)*. AI in digital forensics. (2026, April 27). *LiveLaw*.

Judicial gatekeeping of scientific evidence. (2024). *Jindal Global Law Review / O.P. Jindal Global University (JGU)*.

European Commission. (2026). *First review of Annex III* (COM(2026) 234). European Commission. Fair Trials. (2022). *Regulating AI in criminal justice*. Fair Trials.

AI and computer vision in forensic sciences. (2025). *Rechtsmedizin*.

National Institute of Standards and Technology. (2023). *Artificial Intelligence Risk Management Framework (AI RMF 1.0).* U.S. Department of Commerce.

UNESCO. (2021). *Recommendation on the Ethics of Artificial Intelligence.* UNESCO.

Organisation for Economic Co-operation and Development. (2019). *OECD Principles on Artificial Intelligence.* OECD.

Rudin, C. (2019). Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead. *Nature Machine Intelligence, 1*(5), 206–215.

Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. *Proceedings of Machine Learning Research, 81*, 1–15.

Saferstein, R. (2023). *Criminalistics: An Introduction to Forensic Science* (13th ed.). Pearson.