The Impact of Artificial Intelligence on Forensic Science in Criminal Investigations in India: Technological Transformation, Evidentiary Jurisprudence, and Constitutional Challenges

Sajal Das
Research Scholar, Vikrant University, Gwalior
doi.org/10.64643/IJIRT210935

***Abstract*—The integration of Artificial Intelligence (AI) into forensic science marks a significant structural shift in criminal investigation across India. Historically constrained by severe case backlogs, manual evidentiary processing, and resource deficits across Central and State Forensic Science Laboratories (CFSLs and SFSLs), Indian law enforcement and forensic agencies have increasingly adopted machine learning, deep learning, computer vision, and natural language processing to modernize investigative workflows. Flagship national architectures-including the Crime and Criminal Tracking Network and Systems (CCTNS 2.0), the Inter-Operable Criminal Justice System (ICJS 2.0), the National Automated Fingerprint Identification System (NAFIS), and the e-Sakshya digital evidence platform-exemplify this institutional transformation. Simultaneously, the enactment of the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) and the Bharatiya Sakshya Adhiniyam, 2023 (BSA) has reshaped the procedural landscape by mandating forensic visits for serious offenses and updating the statutory regime governing electronic records. However, deploying opaque, probabilistic AI models in high-stakes criminal adjudication creates acute tensions with constitutional guarantees under Articles 14, 20(3), and 21 of the Constitution of India. This paper examines the technological applications of AI across Indian forensic disciplines, evaluates institutional and statutory reforms, analyses the evidentiary admissibility of AI-generated outputs under the BSA, and proposes a regulatory governance framework grounded in algorithmic transparency, human-in-the-loop oversight, and constitutional due process.**

***Index Terms*—Algorithmic Bias, Artificial Intelligence, Bharatiya Sakshya Adhiniyam (BSA), Criminal Investigation, Digital Forensics, Evidentiary Admissibility, Forensic Science, India.**

I. INTRODUCTION

Background and Context: Criminal justice administration in India has long grappled with a widening gap between the complexity of modern crime and the institutional capacity of traditional forensic science[1]. Over the past decade, rapid digitization, ubiquitous mobile connectivity, and the expansion of digital financial ecosystems have transformed the typology of crime across the country. Offenses increasingly involve multi-jurisdictional cyber frauds, encrypted digital communications, deepfake impersonations, synthetic identity theft, and organized transnational networks[2]. Concurrently, conventional violent and property crimes generate vast volumes of unstructured digital artifacts ranging from closed-circuit television (CCTV) footage and call detail records (CDRs) to cellular tower dumps and geolocation logs that overwhelm traditional manual forensic examination[3].

Historically, India's forensic infrastructure has struggled under chronic pendency, shortages of trained scientific personnel, and reliance on labour-intensive analytical protocols. Traditional forensic examinations in disciplines such as questioned documents, toolmark comparison, ballistics, and visual surveillance review depend heavily on subjective human interpretation,

[1] (Mogali, 2025)
[2] (Kumar, 2025)
[3] (Kumar V. K., 2026)

which is both time-consuming and susceptible to cognitive bias[4]. Against this backdrop, Artificial Intelligence (AI) has emerged as a transformative force capable of automating pattern recognition, triaging massive datasets, enhancing degraded physical and digital traces, and accelerating turnaround times across the investigative lifecycle[5].

Research Problem and Objectives: While AI-assisted forensic tools promise unprecedented speed and analytical scale, their integration into Indian criminal investigations outpaces the development of dedicated statutory standards, validation protocols, and judicial safeguards[6]. The deployment of predictive analytics, Automated Facial Recognition Systems (AFRS), voice biometrics, and automated digital forensics raises foundational legal questions regarding privacy, algorithmic bias, chain-of-custody integrity, and the right to a fair trial. Furthermore, the transition from the Indian Evidence Act, 1872 to the Bharatiya Sakshya Adhiniyam, 2023 (BSA) has modernized electronic record certification without fully resolving how trial courts should evaluate the internal reliability of probabilistic or "black-box" AI systems[7].

This research paper pursues four primary objectives:

- Technological Mapping: To examine how AI, machine learning (ML), and deep learning are deployed across key forensic domains in India, including digital forensics, biometrics, DNA profiling, ballistics, and forensic pathology.
- Institutional and Infrastructure Analysis: To evaluate India's national policing and forensic modernization ecosystem, focusing on CCTNS 2.0, ICJS 2.0, NAFIS, e-Sakshya, and research initiatives led by the National Forensic Sciences University (NFSU).
- Evidentiary and Statutory Assessment: To critically analyse the admissibility, authentication, and probative value of AI-derived forensic evidence under the BSA, 2023 and the BNSS, 2023.
- Constitutional and Regulatory Critique: To evaluate the constitutional risks posed by AI forensics specifically concerning informational privacy, self-incrimination, and algorithmic discrimination and formulate a governance framework tailored to Indian jurisprudence.

II. LITERATURE REVIEW AND CONCEPTUAL EVOLUTION

A. Structural Bottlenecks in Traditional Indian Forensics: Existing scholarship on Indian criminal justice highlights that for decades, forensic science functioned primarily as an ancillary, reactive service rather than an integrated pillar of criminal investigation[8]. Following independence, the establishment of the Central Forensic Science Laboratory (CFSL) in Kolkata in 1957 and subsequent state laboratories laid the institutional foundation for scientific investigation. Yet, structural constraints persisted: low forensic utilization rates in routine criminal prosecutions, high vacancy rates among scientific officers, outdated instrumentation in regional laboratories, and prolonged delays in submitting forensic reports to trial courts.

These bottlenecks frequently contributed to low conviction rates in heinous offenses, as investigating officers relied disproportionately on ocular testimony and custodial confessions, both of which remain vulnerable to witness hostility and judicial scrutiny. Recognizing these systemic weaknesses, the Government of India initiated sweeping criminal law reforms in 2023–2024. Under Section 176(3) of the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS), forensic expert visits to crime scenes became mandatory for all offenses punishable with imprisonment of seven years or more[9]. This legislative mandate immediately multiplied the operational workload of forensic laboratories nationwide, making technological force-multiplication through AI an operational necessity rather than an optional upgrade.

B. Paradigm Shift: From Rule-Based Automation to Machine Learning Forensics: The transition toward computational forensics in India has unfolded in two distinct phases[10]. The first phase, spanning the early

[4] (al., 2024)
[5] (Saikanth, 2025)
[6] (Sharma, 2026)
[7] (Verma, 2026)
[8] (Kumar N. , 2025)
[9] (Acts of Parliament, 2023)
[10] (Saikanth, 2025)

2000s to the mid-2010s, relied on deterministic, rule-based software systems. Early fingerprint databases and basic computer forensic utilities operated on rigid, human-defined parameters such as manual minutiae plotting in dactyloscopy or keyword string searches in hard-drive imaging. While useful for record storage, these systems could not autonomously learn from unstructured data or identify latent patterns across disparate datasets.

The second phase, accelerating over the past decade, represents a paradigm shift toward data-driven Artificial Intelligence[11]. Unlike deterministic software, modern ML and deep neural networks ingest vast repositories of historical forensic data to infer complex feature representations independently[12]. Convolutional Neural Networks (CNNs) extract subtle spatial hierarchies from low-resolution CCTV frames; recurrent architectures and transformers process multilingual audio intercepts; and unsupervised clustering algorithms detect anomalous financial flows in cybercrime investigations. Consequently, AI has transitioned from a passive clerical tool into an active analytical partner that generates investigative leads, triages physical and digital exhibits, and quantifies evidentiary matches[13].

III. METHODOLOGY

This study adopts a doctrinal, comparative, and analytical socio-legal research methodology. Primary sources examined include the Constitution of India, the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS), the Bharatiya Sakshya Adhiniyam, 2023 (BSA), the Digital Personal Data Protection Act, 2023 (DPDPA), landmark judgments of the Supreme Court of India, and official policy directives issued by the Ministry of Home Affairs (MHA), the National Crime Records Bureau (NCRB), and NITI Aayog. Secondary sources comprise peer-reviewed literature in forensic science, computer engineering, and Indian evidentiary jurisprudence, alongside comparative regulatory frameworks including the European Union Artificial Intelligence Act, 2024, the United States Federal Rule of Evidence 702 (Daubert standard), and the United Kingdom Forensic Science Regulator Act, 2021.

IV. CORE APPLICATIONS OF ARTIFICIAL INTELLIGENCE IN INDIAN FORENSIC DISCIPLINES

Digital and Cyber Forensics: Digital forensics represents the most mature and urgently needed domain for AI deployment in India[14]. With exponential growth in Unified Payments Interface (UPI) transactions, mobile banking, and social media usage, cyber-enabled financial fraud and online exploitation generate terabytes of volatile data per investigation. Manual extraction and review of seized smartphones, cloud backups, and network logs are no longer viable within statutory investigation timelines[15].

AI-driven digital forensic suites employed by Indian cybercrime units and CFSLs perform automated disk triage, malware classification, and anomaly detection[16]. Machine learning models scan seized devices to prioritize high-value artifacts-such as hidden partitions, encrypted containers, cryptocurrency wallet addresses, and deleted communications-reducing initial triage times from weeks to hours. Furthermore, Natural Language Processing (NLP) algorithms analyse vast corpora of chat logs, emails, and social media posts to map conspiratorial networks, detect extortion or radicalization patterns, and perform sentiment and intent analysis. Given India's linguistic diversity, AI translation and transcription tools-bolstered by the July 2026 institutional collaboration between the National Forensic Sciences University (NFSU) and the Digital India BHASHINI Division-enable investigators to process voice notes and text evidence across regional Indian languages rapidly[17].

Biometric Identification: Facial Recognition, Fingerprints, and Voice Forensics: Biometric forensics has witnessed the most visible operational integration of AI across Indian policing agencies[18]:

- Automated Facial Recognition Systems (AFRS): State police forces-including those in Delhi,

[11] (Mogali, 2025)
[12] (Saikanth, 2025)
[13] (Sharma, 2026)
[14] (Kumar V. K., 2026)
[15] (A. Kumar, 2025)
[16] (Kumar V. K., 2026)
[17] (Division, 2026)
[18] (Mathapathi, 2025)

Telangana, Uttar Pradesh, Maharashtra, and Tamil Nadu-as well as central agencies utilize AI-powered facial recognition platforms to match suspect imagery from CCTV cameras against criminal registries, missing person databases, and public records. Deep learning architectures compensate for pose variation, occlusion, poor lighting, and aging, enabling law enforcement to identify suspects in crowded public spaces and resolve cold cases.

- Automated Fingerprint and Palmprint Identification: Managed by the National Crime Records Bureau (NCRB), the National Automated Fingerprint Identification System (NAFIS) utilizes AI-driven minutiae extraction and ridge-pattern matching algorithms to search crime-scene latent prints against a centralized repository exceeding ten million criminal fingerprint records[19]. NAFIS assigns unique 10-digit national identifiers and has enabled state police forces to link unidentified deceased persons and latent scene prints to repeat offenders across state boundaries within minutes.
- Forensic Speaker Recognition: Voice biometrics has become critical in investigating kidnapping-for-ransom, bribery, corruption traps, and terror financing. Traditional spectrographic voice comparison suffered from subjective examiner variability. Modern AI speaker verification systems extract acoustic features-such as Mel-Frequency Cepstral Coefficients (MFCCs) and deep speaker embeddings (x-vectors)-to calculate likelihood ratios comparing questioned recordings against known voice samples, even in the presence of background noise or channel distortion[20].

Forensic Biology and DNA Profiling: DNA evidence is widely regarded as the gold standard of forensic identification, yet complex biological samples frequently challenge conventional interpretation. Crime scenes often yield degraded DNA, low-template samples, or complex mixtures containing genetic material from multiple contributors. Manual deconvolution of mixed Short Tandem Repeat (STR) electropherograms is extraordinarily complex and prone to inter-examiner subjectivity[21].

AI and probabilistic genotyping software address these limitations by applying machine learning and Markov Chain Monte Carlo (MCMC) simulations to separate overlapping alleles, account for stochastic artifacts such as stutter peaks and allelic drop-out, and compute objective likelihood ratios[22]. In India, where DNA profiling is increasingly relied upon in sexual assault, homicide, and mass disaster victim identification, AI-assisted bioinformatics tools accelerate sequence alignment and kinship matching. Additionally, emerging research in forensic phenotyping and epigenetic age estimation uses machine learning to predict externally visible characteristics (such as biogeographical ancestry, eye colour, and chronological age) from biological traces when no database match exists.

Forensic Ballistics, Toolmarks, and Questioned Documents: In physical trace disciplines, AI introduces quantitative objectivity to domains historically critiqued for subjective pattern matching[23]:

- Ballistics and Toolmark Analysis: Automated Ballistic Identification Systems (ABIS) employ 3D topographic surface scanning combined with computer vision algorithms to analyse breech-face impressions, firing-pin marks, and land-and-groove striations on spent cartridge cases and projectiles. Machine learning classifiers score similarity metrics across regional and national ballistics databases, linking firearms used in multiple incidents across jurisdictions.
- Forensic Document Examination: In a jurisdiction plagued by land-title forgery, counterfeit currency, and financial instrument fraud, AI-based document forensics analyses handwriting kinematics, stroke pressure, ink spectral profiles, and printer micro-dots. Convolutional neural networks distinguish genuine signatures from skilled simulations and detect subtle pixel-level alterations in scanned contracts and identity documents[24].

Forensic Pathology, Toxicology, and Crime Scene Reconstruction: AI is reshaping forensic medicine and

[19] (Ministry of Home Affairs, 2024)
[20] (Saikanth, 2025)
[21] (al., 2024)
[22] (Saikanth, 2025)
[23] (al., 2024)
[24] (Mogali, 2025)

crime scene analysis through computational imaging and predictive modelling[25]:

- Virtual Autopsy (Virtopsy) and Pathology: Institutions such as the All-India Institute of Medical Sciences (AIIMS), New Delhi, have pioneered virtual autopsy protocols utilizing post-mortem computed tomography (PMCT) and magnetic resonance imaging. AI image-segmentation algorithms assist forensic pathologists in detecting hairline skeletal fractures, internal haemorrhages, projectile trajectories, and embolism patterns non-invasively, while machine learning models estimate the Post-Mortem Interval (PMI) by integrating biochemical markers, microbiome succession data, and environmental variables.
- Forensic Toxicology: In poisoning and narcotics investigations, machine learning algorithms automate the interpretation of Gas Chromatography–Mass Spectrometry (GC-MS) and Liquid Chromatography–Mass Spectrometry (LC-MS) spectra, rapidly identifying novel psychoactive substances (NPS), synthetic opioids, and pesticide metabolites that might evade standard library searches.
- 3D Crime Scene Reconstruction: Combining terrestrial laser scanning, photogrammetry, and AI-driven spatial analytics, forensic teams reconstruct three-dimensional crime scenes to simulate bloodstain spatter trajectories, bullet flight paths, and line-of-sight visibility, providing courts with objective spatial visualizations[26].

Deepfake Detection and Synthetic Media Forensics: The proliferation of generative AI has introduced a dual-use challenge: while AI aids investigators, generative adversarial networks (GANs) and diffusion models empower criminals to fabricate convincing synthetic audio, video, and images[27]. India has witnessed a surge in AI voice-cloning scams, non-consensual synthetic intimate imagery, fabricated political speeches, and manipulated digital evidence submitted in civil and criminal disputes.

To counter synthetic media, Indian forensic laboratories and academic consortia are deploying defensive AI detection tools[28]. These forensic classifiers examine biological micro-signals-such as irregular blinking, unnatural facial blood-flow pulsatility (photoplethysmography), and lip-sync desynchronization-alongside frequency-domain artifacts, sensor pattern noise (PRNU) inconsistencies, and compression anomalies left behind by generative models.

Table I: Comparative matrix of traditional and ai-enabled forensic methodologies in India

Forensic Discipline	Traditional Methodology	AI-Enabled Methodology	Primary Operational Impact in India
Digital & Cyber Forensics	Manual file browsing, keyword indexing, basic hash verification	ML-based artifact triage, NLP multilingual chat analysis, automated malware clustering	Compresses multi-terabyte device review from weeks to hours in cyber fraud and terror cases.
Biometrics & Surveillance	Manual CCTV scrubbing, human visual comparison, manual minutiae plotting	Deep learning AFRS, NAFIS ridge matching, acoustic speaker embeddings	Enables real-time suspect identification across 10M+ fingerprint records and urban camera networks.
DNA & Forensic Biology	Manual STR peak interpretation, basic statistical probability calculations	Probabilistic genotyping via MCMC/ML, automated mixture deconvolution	Resolves complex multi-contributor and degraded samples in sexual assault and homicide cases.
Ballistics & Documents	Comparison microscopy, visual inspection under magnifying optics	3D surface topography matching, CNN-based signature and ink spectral analysis	Links serial firearm offenses across states and detects sophisticated financial forgery.
Pathology & Crime Scene	Invasive physical dissection, manual crime scene sketching	AI-assisted PMCT Virtopsy segmentation, 3D laser photogrammetry reconstruction	Enhances non-invasive injury documentation and objective trajectory modelling.

[25] (Saikanth, 2025)
[26] (al., 2024)
[27] (Saikanth, 2025)
[28] (Press Information Bureau (PIB), 2026)

V. INDIA'S INSTITUTIONAL, TECHNOLOGICAL, AND POLICY ECOSYSTEM

National Digital Policing Infrastructure: CCTNS 2.0, ICJS 2.0, and NAFIS: The deployment of AI in Indian forensics operates within an ambitious, nationwide digital governance architecture spearheaded by the Ministry of Home Affairs (MHA) and the National Crime Records Bureau (NCRB)[29].

At the core of this architecture is the Crime and Criminal Tracking Network and Systems (CCTNS), which connects over 17,700 police stations across all States and Union Territories into a unified national database. Under the upgraded CCTNS 2.0 roadmap, the NCRB is integrating advanced AI capabilities-including entity resolution algorithms that link disparate First Information Reports (FIRs) across state lines to a single offender profile, custom Large Language Models (LLMs) that automatically recommend applicable statutory sections from FIR narratives, and predictive crime-hotspot analytics[30].

Complementing CCTNS is the Inter-Operable Criminal Justice System (ICJS 2.0), which establishes seamless data exchange across five institutional pillars: Police (CCTNS), Courts (e-Courts), Prisons (e-Prisons), Prosecution (e-Prosecution), and Forensics (e-Forensics)[31]. Within ICJS 2.0, the e-Forensics module digitizes sample tracking, laboratory workflows, and report transmission, reducing chain-of-custody gaps and administrative delays between investigating officers, forensic scientists, and trial judges. Simultaneously, the rollout of the e-Sakshya mobile application mandates audio-visual recording of crime scene searches and seizures, generating tamper-evident digital records directly linked to cloud repositories.

Role of the National Forensic Sciences University (NFSU) and R&D Initiatives: Recognizing that technological infrastructure requires specialized human capital and indigenous research, Parliament elevated the Gujarat Forensic Sciences University to an Institution of National Importance under the National Forensic Sciences University Act, 2020, establishing the National Forensic Sciences University (NFSU) with campuses across India[32]. NFSU functions as the primary academic and research hub driving AI integration into Indian forensic science.

Through specialized postgraduate programs in Artificial Intelligence, Data Science, and Cyber Security, as well as dedicated Centres of Excellence in Cyber Defence and Digital Forensics, NFSU develops indigenous forensic tools tailored to Indian operational realities. Notable institutional initiatives include:

- Strategic Collaborations: In May 2026, the Unique Identification Authority of India (UIDAI) signed a five-year Memorandum of Understanding with NFSU to conduct joint research in AI, deepfake detection, cryptographic security, and forensic laboratory excellence[33]. Similarly, NFSU's July 2026 partnership with Digital India BHASHINI integrates sovereign AI language models into forensic workflows to overcome multilingual investigative barriers[34].
- Capacity Building: NFSU regularly conducts specialized training programs in AI-enabled digital forensics for Indian police officers, judicial officers, public prosecutors, and international law enforcement delegates under the Ministry of External Affairs' ITEC framework.
- Policy Deliberation: In collaboration with the MHA and National Law Universities, NFSU convenes national conferences addressing the operational, legal, and governance challenges posed by AI in internal security and criminal justice[35].

Broader National AI Governance Context: Forensic AI development also intersects with broader national policy frameworks, including NITI Aayog's National Strategy for Artificial Intelligence (AIforAll) and the Principles for Responsible AI (2021), which emphasize safety, reliability, inclusivity, privacy, and accountability[36]. Furthermore, the India AI Mission, approved by the Union Cabinet in 2024 with a

[29] ((NCRB), 2025)
[30] (Parliament of India, 2025)
[31] (Ministry of Home Affairs, 2024)
[32] (Acts of Parliament 2. (., 2020)
[33] (Press Information Bureau (PIB), 2026)
[34] (Division, Memorandum of Understanding on AI-Driven Language Translation for Criminal Investigations and Forensic Science, 2026)
[35] (University, 2024)
[36] (Aayog, 2018)

substantial budgetary outlay for sovereign compute capacity and indigenous dataset creation, supports foundational AI research capable of benefiting public-sector law enforcement and forensic analytics[37].

VI. EVIDENTIARY JURISPRUDENCE AND STATUTORY FRAMEWORK IN INDIA

Transition from the Indian Evidence Act, 1872 to the Bharatiya Sakshya Adhiniyam, 2023: The enactment of the Bharatiya Sakshya Adhiniyam, 2023 (BSA), which came into force on July 1, 2024, replaced the colonial-era Indian Evidence Act, 1872, with the explicit objective of modernizing evidentiary rules for the digital age[38]. Under the erstwhile regime, judicial interpretation of Section 65B-culminating in landmark Supreme Court rulings in Anvar P.V. v. P.K. Basheer (2014)[39] and Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020)[40]-established strict mandatory certification requirements for secondary electronic evidence.

The BSA retains and refines this architecture across Sections 57, 61, 62, and 63[41]:

- Section 2(1)(d) and Section 61: The BSA broadens the definition of "document" to encompass electronic and digital records and explicitly declares under Section 61 that electronic records shall have the same legal effect, validity, and enforceability as paper documents.
- Section 63 (Replacing Section 65B): Section 63 governs the admissibility of electronic records produced as secondary evidence. Crucially, Section 63(4) introduces a dual-certification mechanism accompanied by a prescribed statutory form in the Schedule. Part A of the certificate must be signed by the person in lawful control or management of the device or communication system, while Part B must be signed by an expert certifying the technical integrity and hash value of the electronic record.

The Admissibility vs. Reliability Gap for AI-Generated Evidence: While the BSA strengthens procedural safeguards against post-collection tampering through mandatory hash-value disclosure and expert certification, legal scholars highlight a critical doctrinal gap when these provisions are applied to AI-generated forensic evidence[42]:

- Authentication vs. Epistemic Reliability: A Section 63(4) certificate verifies integrity-that a digital file or AI output has not been altered between extraction and courtroom production. However, it does not establish epistemic reliability-whether the underlying machine learning algorithm was trained on representative data, validated against ground-truth benchmarks, free from systemic error, or accurately calibrated for the specific forensic task.
- Expert Opinion Under Section 39 BSA (Formerly Section 45 IEA): When an AI system generates an analytical conclusion-such as a facial recognition match score, a probabilistic DNA likelihood ratio, or a deepfake classification-that output functions substantively as an opinion on a point of science. Under Section 39 of the BSA, opinions of experts upon points of science or art are relevant facts, subject to judicial scrutiny of the expert's qualifications and the scientific validity of their methodology[43]. Yet, if a forensic examiner merely reports the output of a proprietary AI software package without understanding its internal weights, error rates, or training limitations, the human witness becomes a mere conduit for an uncross-examinable algorithm.
- Absence of a Daubert-Style Gatekeeping Standard: Unlike the United States federal judiciary, which applies the Daubert standard[44] (assessing testability, peer review, known error rates, and general scientific acceptance) to screen novel scientific methodologies, Indian criminal jurisprudence lacks a codified statutory threshold for validating algorithmic forensic tools prior to trial admission.

[37] (Aayog, Responsible AI: Approach Document for India — Part 1: Principles for Responsible AI, 2021)
[38] (Acts of Parliament 2. (., The Bharatiya Sakshya Adhiniyam, 2023, 2023)
[39] (Anvar P.V. v. P.K. Basheer, 2014)
[40] (Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, 2020)
[41] (Acts of Parliament 2. (., The Bharatiya Sakshya Adhiniyam, 2023, 2023)
[42] (Sharma, 2026)
[43] (Acts of Parliament 2. (., The Bharatiya Sakshya Adhiniyam, 2023, 2023)
[44] (Daubert v. Merrell Dow Pharmaceuticals, Inc., 1993)

The "Black-Box" Problem and the Right to Fair Cross-Examination: Deep neural networks utilized in modern facial recognition, speaker verification, and image enhancement operate as computational "black boxes". Because millions of non-linear parameters govern how inputs map to outputs, even the software developers cannot trace a deterministic, human-comprehensible causal chain explaining why an algorithm flagged a particular suspect.

In an adversarial criminal trial governed by the BNSS and BSA, the accused possesses a fundamental right to test prosecution evidence through cross-examination. When forensic findings rely on proprietary, closed-source commercial AI tools often protected by vendors under trade-secret claims defence counsel is denied access to source code, training datasets, false-positive rates, and confidence thresholds. This informational asymmetry undermines the presumption of innocence and risks transforming judicial adjudication into uncritical deference to automated outputs.

VII. CONSTITUTIONAL, ETHICAL, AND OPERATIONAL CHALLENGES

Right to Privacy and Informational Self-Determination (Article 21): In Justice K.S. Puttaswamy (Retd.) v. Union of India (2017), a nine-judge bench of the Supreme Court of India unanimously affirmed that the right to privacy is a fundamental right intrinsic to life and personal liberty under Article 21 of the Constitution[45]. The Court established a rigorous four-pronged proportionality test for any state intrusion into privacy:

- Legality: The action must be sanctioned by a valid law.
- Legitimate State Aim: There must be a pressing social need.
- Proportionality: There must be a rational nexus between the measure and the objective, and the measure must be the least intrusive means available.
- Procedural Safeguards: Robust institutional checks must prevent abuse.

Indiscriminate deployment of AI-powered mass surveillance, live facial recognition in public protests, and speculative data mining across linked government databases struggle to satisfy the Puttaswamy proportionality standard. Moreover, the Digital Personal Data Protection Act, 2023 (DPDPA) grants broad exemptions under Section 17(1)(c) for the processing of personal data in the interest of prevention, detection, investigation, or prosecution of offenses[46]. While operationally facilitating police investigations, this statutory exemption leaves citizens with minimal data-protection guardrails against disproportionate retention, function creep, or unauthorized sharing of sensitive biometric and forensic profiles.

Algorithmic Bias, Discrimination, and Article 14: Article 14 of the Constitution guarantees equality before the law and equal protection of the laws. Machine learning algorithms, however, are not neutral arbiters; they inherit and amplify historical patterns embedded in their training datasets[47].

In the Indian socio-demographic context, algorithmic bias poses acute risks across two dimensions:

- Demographic and Phenotypic Skew: Commercial facial and voice recognition models trained predominantly on Western or non-diverse datasets exhibit demonstrably higher false-positive and false-negative rates across darker skin tones, diverse Indian facial structures, regional accents, and socio-economic groups. A false match in a criminal investigation can trigger wrongful arrest, custodial interrogation, and severe reputational harm.
- Historical Policing Bias in Predictive Analytics: Predictive policing and criminal profiling tools trained on historical FIR and arrest records risk codifying structural socio-economic and caste-based disparities in policing. If historical enforcement disproportionately targeted marginalized neighbourhoods or renotified communities, AI hotspot algorithms will direct heightened surveillance back toward those same populations, creating a self-reinforcing feedback loop of systemic discrimination.

[45] (Justice K.S. Puttaswamy (Retd.) v. Union of India, 2017)

[46] (Acts of Parliament 2. (., The Digital Personal Data Protection Act, 2023, 2023)

[47] (Board, 2025)

Privilege Against Self-Incrimination (Article 20(3)): Article 20(3) protects an accused person from being compelled to be a witness against themselves. In Selvi v. State of Karnataka (2010), the Supreme Court held that involuntary administration of neuro-scientific and physiological deception-detection techniques-such as narco-analysis, polygraph examination, and Brain Electrical Activation Profile (BEAP)-violates Article 20(3) and substantive due process under Article 21[48]. The emergence of AI-driven behavioral biometrics, automated micro-expression analysis, vocal stress-detection algorithms, and AI-assisted functional MRI (fMRI) or EEG cognitive decoding directly implicates Selvi. If investigating agencies utilize AI tools to infer mental states, emotional deception, or testimonial knowledge from an accused person's physiological or vocal responses without informed consent, such practices risk infringing constitutional protections against testimonial compulsion.

Automation Bias and Institutional Skill Deficits: Beyond constitutional questions, operational challenges threaten the reliability of AI-assisted forensics on the ground:

- Automation Bias: Psychological research demonstrates that human decision-makers tend to over-rely on automated recommendations, discounting contradictory physical or circumstantial evidence. In overburdened police stations and forensic laboratories, investigators may treat a low-confidence AI facial match or an automated FIR categorization as conclusive proof rather than an investigative lead requiring independent corroboration.
- Infrastructure and Training Disparities: While premier central institutions and metropolitan police forces possess advanced forensic suites, district-level police stations and state forensic laboratories often face uneven hardware availability, bandwidth constraints, and a shortage of personnel trained in statistical literacy and AI validation. Without standardized Standard Operating Procedures (SOPs), identical digital evidence may yield divergent analytical outcomes across jurisdictions.

VIII. COMPARATIVE INTERNATIONAL PERSPECTIVES

To contextualize India's regulatory trajectory, it is instructive to examine how comparable jurisdictions govern AI in law enforcement and forensic science:

- European Union (EU AI Act, 2024): Regulation (EU) 2024/1689 adopts a risk-based regulatory framework that classifies AI systems used by law enforcement-including biometric identification, polygraphs, emotion recognition, predictive profiling, and evidence reliability evaluation-as High-Risk AI Systems[49]. Providers and deployers of high-risk forensic AI must comply with mandatory requirements covering high-quality training data governance, technical documentation, automated event logging, human oversight, accuracy robustness, and pre-market conformity assessments. Real-time remote biometric identification in publicly accessible spaces is strictly prohibited save for narrowly defined, judicially authorized exceptions.
- United States (NIST Standards and Judicial Scrutiny): While the U.S. lacks a single federal AI statute, forensic AI tools are governed by evidentiary gatekeeping under Federal Rule of Evidence 702 (Daubert)[50] and technical validation frameworks developed by the National Institute of Standards and Technology (NIST) and the Organization of Scientific Area Committees (OSAC) for Forensic Science. NIST conducts independent, rigorous benchmarking (such as the Face Recognition Vendor Test) that publicly quantifies demographic error rates, enabling defence attorneys and judges to evaluate the empirical precision of specific algorithms.
- United Kingdom (Forensic Science Regulator Act, 2021): The UK placed its Forensic Science Regulator on a statutory footing, empowering the office to issue binding Codes of Practice and require ISO/IEC 17025 accreditation for forensic laboratories. Any AI or probabilistic software used in forensic analysis must undergo documented validation studies demonstrating fitness for

[48] (Selvi v. State of Karnataka, 2010)
[49] (Union, 2024)
[50] (Daubert v. Merrell Dow Pharmaceuticals, Inc., 1993)

purpose before its outputs can be adduced in criminal courts.

These international models underscore a shared consensus: AI tools in criminal justice cannot rely solely on general electronic evidence rules; they require domain-specific validation, transparent error-rate reporting, and enforceable human oversight.

IX. RECOMMENDATIONS AND POLICY FRAMEWORK FOR INDIA

To harness the transformative efficiency of AI while safeguarding constitutional rights and evidentiary integrity, India should adopt a multi-tiered governance framework:

Legislative and Evidentiary Reforms:

- Codify Scientific Reliability Standards in the BSA: Amend the Bharatiya Sakshya Adhiniyam, 2023- or issue authoritative judicial practice directions-to supplement Section 63(4) certification with a substantive reliability inquiry for AI-derived evidence[51]. Courts should require the prosecution to disclose the software version, validation status, known false-positive/false-negative error rates, and confidence thresholds underlying any AI-assisted forensic conclusion.
- Enact a Statutory Forensic Accreditation Framework: Establish a statutory National Forensic Science Regulatory Authority-building upon the Directorate of Forensic Science Services (DFSS) and NFSU-mandating ISO/IEC 17025 accreditation and formal pre-deployment validation for all forensic laboratories and AI software tools used in criminal investigations.
- Establish Disclosure Protocols Balancing Trade Secrets and Fair Trial Rights: Where vendors assert intellectual property claims over forensic algorithms, trial courts should utilize protective orders and independent court-appointed technical experts to audit source code and validation data in camera, ensuring the defence can meaningfully challenge algorithmic reliability.

Technical and Operational Safeguards:

- Mandatory Human-in-the-Loop (HITL) Governance: Prohibit criminal arrests, chargesheets, or convictions based solely on uncorroborated AI outputs. Operational SOPs must mandate that AI outputs-particularly facial recognition matches and predictive alerts-serve strictly as investigative leads verified by independent human forensic examiners and corroborating physical or documentary evidence.
- Indigenous Benchmarking and Bias Audits: Task NFSU, the Bureau of Police Research and Development (BPR&D), and the Bureau of Indian Standards (BIS) with establishing national forensic AI testing benchmarks using diverse, representative Indian demographic datasets. Mandatory periodic algorithmic audits should measure and mitigate demographic performance disparities prior to operational deployment.
- Explainable AI (XAI) Procurement Mandates: Government procurement guidelines for law enforcement and CFSLs/SFSLs should prioritize Explainable AI (XAI) architectures such as saliency heatmaps in image comparison and transparent likelihood-ratio models in DNA and voice forensics-over opaque black-box systems[52].

Constitutional Oversight and Capacity Building:

- Judicial Authorization and Oversight Boards: Require prior judicial authorization for intrusive AI surveillance applications, such as real-time public facial recognition or bulk predictive profiling, accompanied by independent civilian and technical oversight committees to audit database access and prevent function creep.
- Interdisciplinary Training Across the Criminal Justice System: Institutionalize recurring training modules at the National Judicial Academy, State Judicial Academies, and NFSU to equip judges, public prosecutors, defence lawyers, and investigating officers with foundational literacy in machine learning, probabilistic statistics, and algorithmic limitations.

[51] (Verma, 2026)

[52] (Sharma, 2026)

X. CONCLUSION

Artificial Intelligence has undeniably initiated a new era in Indian forensic science, offering powerful solutions to long-standing systemic challenges of case pendency, subjective human error, and the overwhelming scale of modern digital evidence. Through national initiatives such as CCTNS 2.0, ICJS 2.0, NAFIS, e-Sakshya, and cutting-edge research led by the National Forensic Sciences University, India is rapidly constructing a digitally integrated forensic ecosystem. Across cyber forensics, biometrics, DNA mixture deconvolution, ballistics, and virtual pathology, AI demonstrably accelerates investigative workflows and enhances analytical precision.

Nevertheless, technological capability must never be conflated with legal infallibility. As the criminal justice system transitions into the era of the Bharatiya Nagarik Suraksha Sanhita and the Bharatiya Sakshya Adhiniyam, the legitimacy of AI-assisted forensics depends on bridging the gap between electronic record authentication and algorithmic reliability. Unchecked reliance on opaque, unvalidated, or biased algorithms risks eroding foundational constitutional guarantees of privacy, equality, protection against self-incrimination, and a fair trial. By embedding explainable AI standards, mandatory empirical validation, strict human-in-the-loop oversight, and statutory regulatory accountability into its forensic architecture, India can ensure that artificial intelligence serves as a reliable instrument of truth and constitutional justice rather than a mechanized source of error.

REFERENCES

[1]. S. S. Mogali, "Impact of artificial intelligence on forensic investigations," *International Journal of Research and Analytical Reviews*, vol. 12, no. 3, pp. 672–679, Jul. 2025.

[2]. N. Kumar, "The role of artificial intelligence in criminal investigations in India," *Journal of Artificial Intelligence and Law*, pp. 1–12, Apr. 2025.

[3]. V. Kumari and V. Kumar, "The role of artificial intelligence in digital forensic investigations: Legal and ethical challenges," *International Journal of Novel Research and Development*, vol. 11, no. 2, pp. 149–158, Feb. 2026.

[4]. M. Arjamand *et al*., "The role of artificial intelligence in forensic science: Transforming investigations through technology," *International Journal of Multidisciplinary Research and Publications*, vol. 7, no. 5, pp. 67–70, Oct. 2024.

[5]. E. Saikanth, "Harnessing artificial intelligence in forensic science: Advancements, applications, and investigative implications," *International Journal of Innovative Research in Technology*, vol. 12, no. 6, pp. 2500–2508, Nov. 2025.

[6]. A. Sharma, "Artificial intelligence-driven forensic evidence: Scientific, legal and institutional challenges in India," *International Journal of Research and Scientific Innovation*, vol. 13, no. 1, pp. 287–293, Jan. 2026.

[7]. R. Verma, "AI-generated evidence in the Indian legal system: Navigating the evidentiary vacuum and charting a reform agenda," *Indian Journal of Integrated Research in Law*, vol. 6, no. 1, pp. 112–128, 2026.

[8]. The Bharatiya Nagarik Suraksha Sanhita, 2023, Act No. 46 of 2023, § 176(3), Acts of Parliament, India, 2023.

[9]. A. Kumar, V. Sharma, and S. Kumar, "Advancing artificial intelligence in criminal investigation: A comprehensive review and future directions," *Indian Journal of Forensic Medicine and Pathology*, vol. 18, no. 2, pp. 243–250, 2025.

[10]. National Forensic Sciences University (NFSU) and Digital India BHASHINI Division, "Memorandum of understanding on AI-driven language translation for criminal investigations and forensic science," Gandhinagar, India, Jul. 8, 2026.

[11]. A. Prasannan and M. B. Mathapathi, "The evolving role of artificial intelligence in forensic analysis," Karnataka State Law University Research Paper Series, 2025.

[12]. Ministry of Home Affairs, Government of India, "Union Home Minister chairs NCRB review meeting on implementation of three new criminal laws and integration of CCTNS 2.0, NAFIS, and ICJS 2.0," Press Information Bureau, New Delhi, India, Dec. 24, 2024.

[13]. Press Information Bureau, Government of India, "UIDAI joins hands with NFSU to enhance cybersecurity and digital forensics," Ministry of

Electronics and Information Technology, New Delhi, India, May 5, 2026.

[14]. National Crime Records Bureau, *National Automated Fingerprint Identification System (NAFIS) and CCTNS Operational Overview*. New Delhi, India: Ministry of Home Affairs, Government of India, 2025.

[15]. Parliament of India, Standing Committee on Communications and Information Technology, *Report on the Impact of Emergence of Artificial Intelligence and Related Issues (Submission of the Ministry of Home Affairs on CCTNS 2.0)*. New Delhi, India: Lok Sabha Secretariat, 2025.

[16]. The National Forensic Sciences University Act, 2020, Act No. 32 of 2020, Acts of Parliament, India, 2020.

[17]. Ministry of Home Affairs and National Forensic Sciences University, *Proceedings of the National Conference on Challenges Posed by Artificial Intelligence*, Gandhinagar/New Delhi, India, Oct. 17–18, 2024.

[18]. NITI Aayog, *National Strategy for Artificial Intelligence (#AIforAll)*. New Delhi, India: Government of India, Jun. 2018.

[19]. NITI Aayog, *Responsible AI: Approach Document for India, Part I: Principles for Responsible AI*. New Delhi, India: Government of India, Feb. 2021.

[20]. The Bharatiya Sakshya Adhiniyam, 2023, Act No. 47 of 2023, §§ 2(1)(d), 39, 57, 61–63, Acts of Parliament, India, 2023.

[21]. *Anvar P. V. v. P. K. Basheer*, (2014) 10 SCC 473 (Supreme Court of India).

[22]. *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1 (Supreme Court of India).

[23]. *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (Supreme Court of the United States, 1993).

[24]. *Justice K. S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (Supreme Court of India).

[25]. The Digital Personal Data Protection Act, 2023, Act No. 22 of 2023, § 17(1)(c), Acts of Parliament, India, 2023.

[26]. Editorial Board, "Ethical integration of artificial intelligence in forensic science: Prospects and challenges," *CMR University Journal for Contemporary Legal Affairs*, vol. 7, no. 1, pp. 45–62, 2025.

[27]. *Selvi v. State of Karnataka*, (2010) 7 SCC 263 (Supreme Court of India).

[28]. European Parliament and Council of the European Union, "Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)," *Official Journal of the European Union*, Jul. 12, 2024.