
AI-DRIVEN INVESTIGATIVE TECHNOLOGIES AND THEIR EVIDENTIARY VALIDITY

Mohit Kumar Gupta, Advocate, Delhi High Court (Enrolment No – D/10507/2023)
LLM, Jamia Millia Islamia, New Delhi (2023-2025)

ABSTRACT

The integration of Artificial Intelligence into India's criminal justice administration has accelerated substantially, with law enforcement agencies deploying Automated Facial Recognition Systems (AFRS), probabilistic genotyping, predictive policing algorithms, and Natural Language Processing tools across investigative and prosecutorial processes. While these technologies promise enhanced investigative efficiency, evidentiary accuracy, and resource optimisation, their deployment has outpaced the development of a coherent legal and regulatory framework capable of governing their use within a rights-respecting constitutional order. This paper critically examines the evidentiary validity, constitutional implications, and regulatory lacunae surrounding AI-driven investigative technologies in the Indian context. It evaluates the adequacy of the current legal situation in addressing the admissibility, authenticity, and reliability of AI-generated evidence. It identifies the doctrinal challenges posed by the "black-box" opacity inherent in machine-learning systems. Through comparative engagement with the EU AI Act (2024), the US Daubert standard, and Singapore's statutory presumption model, the paper identifies international best practices and evaluates their transposability to the Indian legal context. The paper concludes by proposing a dedicated statutory framework for AI in criminal justice, encompassing mandatory algorithmic impact assessments, judicially recognised testing standards for AI-generated evidence modelled on the Daubert framework, an independent AI oversight authority, and constitutional compliance protocols ensuring that AI serves as an instrument of justice rather than an engine of institutional arbitrariness.

1. INTRODUCTION

Artificial Intelligence has become a transformative tool in criminal investigations, enabling faster data analysis, increasing accuracy, and supporting evidence-based policing. AI tools can assist with crime detection, suspect identification, digital evidence extraction, and the prediction of criminal behaviour. Although India currently lacks a specific statutory or regulatory framework governing their use, AI-based techniques are beginning to find practical applications in criminal investigations in various parts of India. This paper explores AI techniques used in criminal investigations, examines their evidentiary value under current law, reviews government policy on their adoption, and concludes with key policy recommendations.

These techniques include Automated Facial Recognition Systems (AFRS), which generate biometric “faceprints” matched against national databases; AI-powered image enhancement tools used to reconstruct blurred CCTV footage; probabilistic genotyping platforms that interpret complex or mixed DNA samples through statistical simulation; and predictive policing algorithms trained on historical crime data to forecast future offences. These technologies are being operationally deployed by agencies, including the Delhi Police, the National Crime Records Bureau, and police forces in Maharashtra and Uttar Pradesh.

The Government of India is increasingly moving toward integrating artificial intelligence into the criminal justice system. For instance, *Vimarsh 2023*,¹ launched by the Bureau of Police Research and Development, is a 5g hackathon that explored how AI could assist with tasks such as preparing charge sheets, classifying FIRs, managing evidence seizure, and supporting forensic analysis. Prime Minister Narendra Modi has also emphasised that technology will help connect police, forensic services, prisons, and courts into a more coordinated system. At the same time, national platforms like the Crime and Criminal Tracking Network System (CCTNS) are being enhanced with AI-driven analytics, and new initiatives such as e-Forensics and e-Prisons are being developed to allow real-time information sharing among investigative agencies.

Although there is a lack of coherent development in the evidentiary, regulatory, and constitutional framework of such techniques. The Bharatiya Sakshya Adhiniyam, 2023 (BSA)

¹ Press Info. Bureau, *Vimarsh 2023: 5G Hackathon for Law Enforcement Agencies*, PRESS INFO. BUREAU (Feb. 24, 2024), <https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=2008631®=3&lang=2> (last visited April 3, 2026)

classifies digital records as primary evidence under Section 61 and imposes a dual-certification requirement under Section 63(4). Nevertheless, the questions of how AI-generated outputs, as distinct from conventional electronic records, are to be tested for admissibility, reliability, and authenticity remain unanswered. The reasoning behind machine-learning models is opaque, commonly referred to as the “black-box problem”², and this lack of transparency does not sit comfortably with legal systems that rely on evidence being clear and verifiable. The challenge becomes even more serious with the rise of deepfake technology, which enables the creation of highly convincing yet entirely fabricated audio and video evidence.

India’s constitutional framework strongly safeguards individual liberty, which may be at risk of being curtailed with the use of such AI-driven technologies. In the landmark *Justice K.S. Puttaswamy v. Union of India* (2017)³ judgment, the Supreme Court recognised privacy as a fundamental right under Article 21. It also made clear that any state action that intrudes on this right must pass a three-part test, viz., it must have a legal basis, pursue a legitimate objective, and be proportionate. The use of AI also raises serious equality concerns. If the data used to train these systems is biased, it can lead to discriminatory outcomes, especially in predictive policing. This creates risks under Articles 14 and 15, as marginalised communities may be unfairly targeted, effectively reinforcing existing structural inequalities through technology.

This research paper studies how effective AI-based investigative tools currently used in India really are, evaluates whether there are adequate legal framework for handling such evidence, and analyses the constitutional limits on AI-driven surveillance and decision-making. It also builds a comparative perspective by drawing on global approaches, including the EU AI Act, the US Daubert standard, and Singapore’s statutory presumption model. It concludes by offering practical regulatory recommendations aimed at ensuring that AI functions as a tool for delivering justice, rather than becoming a source of arbitrary or unchecked institutional power.

2. AI-DRIVEN INVESTIGATIVE TECHNOLOGIES

There are four main AI-driven investigative techniques currently prevalent in criminal investigation, namely, automated facial recognition systems, probabilistic genotyping,

² Jenna Burrell, *How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms*, 3 BIG DATA & SOC’Y 1, 3 (2016).

³ Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

predictive policing, and natural language processing.

2.1. Automated Facial Recognition System (AFRS)

An Automated Facial Recognition System (AFRS) uses Artificial Intelligence and algorithm-driven technology to generate a digital biometric template, i.e., a “faceprint” of an individual’s face by identifying and mapping distinct facial features. This template is subsequently matched against an existing database to which the system has access. For instance, when an image of an unidentified person is obtained, such as from CCTV footage, it is processed and analysed using AFRS to detect similarities and verify identity against the stored database. Concurrently, in support of that process, AI-powered image-enhancement tools are used to reconstruct low-quality visuals and clarify blurred frames, thereby improving the accuracy and evidentiary reliability of the identification process.

In the Indian context, the Union Ministry of Law and Justice has acknowledged⁴ that Artificial Intelligence is being integrated into criminal-tracking mechanisms and digital forensic processes. National databases such as the Crime and Criminal Tracking Network System (CCTNS) and the “e-Forensics” digital evidence repository are currently being augmented with AI-based analytical capabilities. The National Crime Records Bureau (NCRB) is implementing⁵ a nationwide AFRS, designed to interlink police photographic records, including driving licence databases and electoral rolls, for the identification of missing persons as well as suspected offenders. The Delhi Police have publicly documented the operational deployment of Facial Recognition Technology in criminal investigations, crowd-control scenarios, and efforts to trace missing persons⁶.

2.2. Probabilistic Genotyping

Probabilistic genotyping represents a significant technological advancement in criminal investigations. It employs artificial intelligence algorithms to interpret complex or low-quality DNA samples recovered during police investigations or criminal prosecutions.

⁴ Oxford Inst. for Tech. & Just. *India – Increasing Use of AI Across the Justice System*, BLAVATNIK SCH. OF GOV'T (Oct. 17, 2025), <https://www.techandjustice.bsg.ox.ac.uk/research/india> (last visited Mar. 29, 2026).

⁵ Pooja Jyoti, *Automated Facial Recognition: What NCRB Proposes, What Are the Concerns*, INDIAN EXPRESS (July 10, 2019), <https://indianexpress.com/article/explained/automated-facial-recognition-what-ncrb-proposes-what-are-the-concerns-5823110/> (last visited Mar. 25, 2026).

⁶ Upasika Singhal, *AI in the Sky: Police to Soon Deploy Facial Recognition Tech Across Delhi*, INDIAN EXPRESS (Apr. 6, 2025), <https://indianexpress.com/article/cities/delhi/ai-in-the-sky-police-to-soon-deploy-facial-recognition-tech-across-delhi-9927353/>. (last visited Mar. 26, 2026).

Unlike traditional DNA analysis, which often struggles with mixed, degraded, or minimal biological material, probabilistic genotyping evaluates the statistical likelihood that a particular individual contributed to a given DNA sample. These AI-enabled models run extensive simulations to generate a scientifically grounded likelihood ratio, which may assist the court in determining guilt or innocence. AI-based probabilistic genotyping has emerged as a critical component of evidence generation. Its extensive use in jurisdictions such as the United States and Canada demonstrates its practical value and judicial acceptance. As India explores similar technological integration in criminal justice processes, probabilistic genotyping offers a structured, objective, and scientifically robust method for strengthening evidentiary reliability and enhancing investigative accuracy⁷.

2.3. Predictive Policing

Predictive policing refers to the use of advanced data-driven analytical tools to forecast potential criminal activity and enable preventive law-enforcement responses. It involves aggregating and analysing large datasets from diverse sources, such as past crime records, geospatial information, demographic indicators, CCTV and sensor data, and social-network linkages. They are used to identify patterns and probabilities of future offences. AI tools are used for crime mapping, hot-spot analysis, geospatial modelling, machine-learning algorithms, data mining, and social-network analysis have significantly expanded the capabilities of law-enforcement agencies to anticipate localized crime spikes, allocate resources efficiently, plan urban safety strategies, and improve operational decision-making.

In India, several states have initiated pilot models for predictive policing. In Mumbai, a prototype AI-driven system utilizing five years of historical crime data predicted mobile and vehicle-theft hotspots with approximately 75% accuracy⁸, enabling targeted patrolling and pre-emptive deployment of personnel. Similarly, the Uttar Pradesh Police have announced initiatives involving AI-based predictive analytics for crime pattern recognition, biometric-database integration, and rapid digital evidence processing to identify high-risk

⁷ John Buckleton, *Labs Live*, JOHN BUCKLETON (June 2020), <https://johnbuckleton.files.wordpress.com/2020/06/labs-live-ii.pdf> (last visited Mar. 31, 2026).

⁸ Niraj Pandit, *How AI Tools Are Helping Mumbai Cops Prevent Crimes*, HINDUSTAN TIMES (Apr. 16, 2025), <https://www.hindustantimes.com/cities/mumbai-news/how-ai-tools-are-helping-mumbai-cops-prevent-crimes-101744744869314.html> (last visited Mar. 27, 2026).

zones and habitual offenders⁹. Other metropolitan jurisdictions, including Delhi¹⁰ have begun experimenting with crime-mapping tools integrated with real-time surveillance networks, reflecting a gradual transition toward technologically supported policing in India.

2.4.Natural Language Processing (NLP)

Natural Language Processing in criminal investigations refers to the use of AI to examine large volumes of text and speech data in order to identify patterns, extract relevant information, and connect pieces of evidence more efficiently than traditional manual methods. Its major uses include studying police reports to detect trends, reviewing digital materials such as emails and social media content to find links between individuals and their communications, and applying linguistic analysis to writing styles or speech patterns to help identify possible suspects. In India, NLP capabilities are being integrated into the CCTNS and proposed for automated charge-sheet scrutiny under the Vimarsh 2023 framework.

Technology	Deployment Status in India	Primary Legal Challenge
Automated Facial Recognition (AFRS)	Operational — NCRB, Delhi Police, Safe City Project	Algorithmic bias; BSA s.63 certification; Article 21 proportionality
Image Enhancement (AMPED FIVE)	Operational — Delhi Police	Artefact generation; authenticity of enhanced record
Probabilistic Genotyping	Under consideration; not yet formally adopted	Proprietary opacity; expert competency; Kattavellai (2025)
Predictive Policing (CMAPS, Trinetra)	Pilot deployments — Maharashtra, Delhi, UP	Algorithmic bias; pre-crime targeting; Articles 14, 21
NLP / Communications Analysis	Proposed — CCTNS integration, Vimarsh 2023	Interception law; linguistic profiling; privacy

⁹ Vijay Chopra, *Focus Is on People-Centric, AI-Based Policing: UP DGP Prashant Kumar*, TIMES OF INDIA (Feb. 1, 2024), <https://timesofindia.indiatimes.com/city/lucknow/our-focus-is-on-people-centric-ai-based-policing-dgp-prashant-kumar/articleshow/107334913.cms> (last visited Mar. 29, 2026).

¹⁰ *Delhi Police Implements Crime Mapping, Analytics & Predictive System (CMAPS)*, BW POLICE WORLD (Dec. 11, 2017), <https://www.bwpoliceworld.com/article/delhi-police-implements-crime-mapping-analytics-predictive-system-cmaps-134283> (last visited Mar. 30, 2026).

3. EVIDENTIARY FRAMEWORK

The evidentiary admissibility of these technologies remains unaddressed by the Indian Evidence Act, 1872 or the recently enacted Bhartiya Sakshya Adhiniyam. Since AI-generated outputs are fundamentally electronic in nature, they are inherently vulnerable to alteration, corruption, or unintentional distortion. This makes it essential to establish the admissibility, reliability and authenticity of the AI-led evidences. Further, the integrity and trustworthiness of the systems that store, process, or analyse such data are also to be ensured.

Common law traditionally presumes that computer systems operate reliably unless proven otherwise, this assumption becomes problematic when applied to opaque and complex AI and ML models whose internal processes are not immediately apparent¹¹. Some jurisdictions such as Singapore have elevated¹² this assumption into a legal presumption, thereby shifting the burden of disproving system reliability to the opponent. Even then, the proponent must still demonstrate, through credible scientific and technical material, that the AI tool or method in question is one that ordinarily produces accurate outputs when properly used, thus satisfying the evidential presumption.

In the Indian context, the Supreme Court, through *Anvar P.V. v. P.K. Basheer*¹³ and *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*¹⁴ had laid down strict law that electronic records would be admissible only when they are accompanied by a certificate under section 65B(4). The admissibility of electronic evidence under the Bhartiya Sakshya Adhiniyam, 2023, is governed by Section 63, which preserves a mandatory certification requirement. However, Section 63(4) introduces a significant departure from the prior law: the certificate must now be signed not only by the individual responsible for the device (the “device controller”) but also by an expert. This dual-attestation requirement reflects a legislative acknowledgement that electronic evidence requires technical validation beyond mere custody records. But AI-generated evidence makes this complicated by arising questions like how an expert can certify the algorithmic process that created the output. The thinking process of AI offers no

¹¹ LAW COMM'N (UK), *EVIDENCE IN CRIMINAL PROCEEDINGS: HEARSAY AND RELATED TOPICS* ¶ 13.13 (Consultation Paper No. 138, 1997).

¹² Evidence Act, § 116A, Cap. 97 (2008 Rev. Ed.) (Sing.) (as amended by Evidence (Amendment) Act 2012, No. 4 of 2012).

¹³ *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.

¹⁴ *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.

opportunity to review the reasoning process involved, referred to as the “black box problem”¹⁵.

Therefore, courts continue to treat AI-generated evidence cautiously. Facial recognition results are accepted only as electronic records subject to Section 65B compliance, and judicial practice shows reluctance to treat algorithmic matches as conclusive proof due to risks of bias and accuracy errors¹⁶. Probabilistic genotyping, although grounded in established DNA science, introduces statistical interpretations that are difficult to verify, raising concerns about transparency and explainability under Section 45 (expert opinion). In *Kattavellai (Devakar) v. State of Tamil Nadu* (2025)¹⁷, the Supreme Court clarified that under the *Bharatiya Sakshya Adhiniyam*, 2023, DNA profiles constitute a species of “opinion evidence”, the probative weight of which must be assessed contextually in each case. These judicial observations assume heightened significance in contemporary investigative settings where AI-led forensic tools—such as automated DNA matching algorithms, probabilistic genotyping systems, and machine-learning-based pattern-recognition platforms—play an increasingly central role. By emphasising strict chain-of-custody compliance and case-specific judicial scrutiny of expert opinions, the judgment implicitly extends its rationale to AI-processed forensic outputs, underscoring that algorithmic results, too, must satisfy standards of reliability, transparency, and evidentiary admissibility within the criminal justice process.

A distinctive challenge across all AI systems is that traditional software-verification methods, such as unit testing, are insufficient for evaluating machine-learning models, particularly their “corner cases” where hidden errors may surface only under atypical conditions. Consequently, ensuring integrity, authenticity, and reliability of AI evidence demands new evidentiary norms and judicially recognised testing standards tailored to the complexities of algorithmic systems. While Indian courts have embraced technological evidence in principle, the overarching trend reveals a restrained and rights-conscious approach, emphasizing that any AI-generated material must withstand rigorous scrutiny to safeguard fair trial rights, privacy protections, and constitutional guarantees under Article 21.

¹⁵ Burrell, *supra* note 2, at 3.

¹⁶ Apoorva Mandhani, *Courts Flag Reliability of Facial Recognition in Delhi Riots Cases*, INDIAN EXPRESS (Mar. 12, 2021).

¹⁷ *Kattavellai @ Devakar v. State of Tamil Nadu*, Criminal Appeal No. 1672 of 2019, 2025 INSC 845.

Legal Issue	BSA 2023 Position / Gap
Admissibility of electronic records	Section 61: Primary evidence; admissible on same basis as paper
Certification requirement	Section 63(4): Dual certificate — device controller AND expert
Definition of ‘expert’ for AI systems	SILENT — critical gap requiring legislative/judicial intervention
Reliability standard for AI outputs	ABSENT — no AI-specific evidentiary standard
Deepfake authentication	ABSENT — no detection or authentication regime
Presumption of computer reliability	NOT ADOPTED — unlike Singapore’s statutory model
DNA / PG evidence classification	Opinion evidence under Section 39; Kattavellai (2025)

4. CONSTITUTIONAL FRAMEWORK: RIGHTS, SURVEILLANCE, AND ALGORITHMIC ACCOUNTABILITY

The deployment of AI-driven investigative technologies also raises fundamental concerns regarding overdependence, reliability, and the protection of constitutional rights. In the criminal justice context, the central objective of integrating such tools must be to augment human legal intelligence rather than supplant it. As scholars argue¹⁸, artificial intelligence must operate in a manner “aligned with law and the Rule of Law in a testable and contestable way,” emphasising the need for transparency, verifiability, and human oversight. The Indian judiciary has echoed these apprehensions. Justice Surya Kant of the Supreme Court has cautioned¹⁹ that AI tools are inherently fallible, capable of generating inaccuracies, hallucinations, or inheriting biases embedded in their training data, thereby reinforcing the imperative that human decision-

¹⁸ Marion Oswald et al., *Algorithmic Risk Assessment Policing Models: Lessons from the Durham HART Model and "Experimental" Proportionality*, 27 INFO. & COMM’NS TECH. L. 223 (2018).

¹⁹ Surya Kant, *AI Can Guide but Lawyers, Judges Must Be Final Arbiter: Supreme Court Justice Surya Kant*, BAR & BENCH (Oct. 25, 2025), <https://www.barandbench.com/news/ai-can-guide-but-lawyers-judges-must-be-final-arbiter-supreme-court-justice-surya-kant> (last visited Mar. 29, 2025).

makers remain the final arbiters of legal outcomes.

These technological concerns are situated within a constitutional framework that mandates rigorous protection of personal liberty and informational privacy under Article 21. Following the landmark judgment in *Justice K.S. Puttaswamy v. Union of India* (2017)²⁰, any state action involving AI-enabled surveillance, data extraction, or automated decision-support must satisfy the threefold test of legality, legitimate aim, and proportionality. This standard demands not only statutory backing but also demonstrable necessity and narrowly tailored use of intrusive technologies. In investigative settings—particularly those involving facial recognition, probability genotyping, or digital tracking—compliance with this constitutional threshold becomes indispensable to prevent arbitrary or disproportionate interference with individual rights. For Instance, predictive policing, though increasingly promoted for its perceived potential to enhance public safety, optimise resource allocation, and support evidence-based policing, simultaneously presents serious normative and operational challenges. Algorithmic models risk perpetuating structural biases present in historical crime data, thereby amplifying discriminatory outcomes against marginalised communities. Moreover, the integration of predictive systems into regular policing expands the surveillance apparatus of the State, raising intricate questions about data minimisation, retention, and transparency. The opacity of proprietary algorithms further undermines procedural fairness by limiting the ability of individuals to contest or scrutinise decisions that directly affect their rights.

The Digital Personal Data Protection Act, 2023, establishes a framework for the protection of personal data, including biometric data, health data, and data that reveals religious or political beliefs. Its application to law enforcement data processing in the AI investigative context raises fundamental unresolved questions:

- Section 17 of the DPDPA exempts the state from certain data protection obligations for purposes of national security and prevention or detection of crime. The scope of this exemption — and whether it covers the large-scale biometric data aggregation implicit in AFRS deployment — has not been judicially determined.
- The DPDPA establishes a Data Protection Board to adjudicate complaints, but it has no

²⁰ Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

criminal justice-specific mandate or technical capacity to audit AI surveillance systems.

- The principle of data minimisation under the DPDPA requires that only the personal data necessary for the specified purpose be collected and processed. Mass CCTV surveillance with facial recognition, by definition, captures data on all individuals in a public space irrespective of any suspicion of criminal activity — a practice whose compatibility with the DPDPA's minimisation principle is untested.

5. COMPARATIVE FRAMEWORK: INTERNATIONAL REGULATORY MODELS

A comparative analysis of international regulatory approaches to AI in criminal justice reveals a spectrum ranging from categorical prohibition to permissive deployment with minimal oversight. This section examines the three most instructive models for Indian regulatory design: the European Union AI Act (2024), the United States Daubert standard, and Singapore's statutory presumption framework.

5.1. The European Union AI Act, 2024

The EU AI Act, which entered into force in 2024, establishes a risk-based regulatory framework for AI systems. For criminal justice applications, the Act makes two distinctions of direct relevance to this paper:

- Unacceptable Risk is prohibited under EU law: AI systems used for social scoring of individuals²¹ based on behaviour and for biometric categorisation systems that infer sensitive attributes²², are categorically prohibited. Real-time remote biometric identification²³ in public spaces, the use of force by law enforcement is subject to extremely limited exceptions. Individual criminal risk scoring systems²⁴ are also classified as prohibited.
- High Risk is regulated under EU law: AI systems used as safety components of critical infrastructure²⁵, in the administration of criminal justice²⁶, and for the evaluation of

²¹ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) art. 5(1)(c), 2024 O.J. (L 2024/1689).

²² *Id.* art. 5(1)(g).

²³ *Id.* art. 5(1)(h), ¶¶ 2–5.

²⁴ *Id.* art. 5(1)(d).

²⁵ *Id.* art. 6(2), Annex III, ¶ 2.

²⁶ *Id.* art. 6(2), Annex III, ¶ 8.

evidence in criminal proceedings are classified as high-risk and subject to mandatory conformity assessment, transparency obligations, human oversight requirements, and post-market monitoring.

The contrast with India is stark: India operates predictive policing and facial recognition systems that would be either prohibited or heavily regulated under the EU framework, entirely without a corresponding domestic regulatory structure. This comparison does not suggest that India must adopt the EU model wholesale, but it establishes a principled basis for arguing that the current Indian regulatory vacuum is unsustainable from a rule-of-law perspective.

5.2.The United States: The Daubert Standard

In the United States, the admissibility of scientific expert testimony in federal proceedings is governed by the Daubert standard, as elaborated by the Supreme Court in *Daubert v. Merrell Dow Pharmaceuticals Inc* (1993)²⁷ and its progeny²⁸. Under Daubert, a trial court performs a gatekeeping function: before expert scientific evidence is admitted, the court must assess whether the underlying methodology is

- (i) testable and falsifiable;
- (ii) peer-reviewed and published;
- (iii) associated with a known or potential error rate; and
- (iv) generally accepted in the relevant scientific community.

Applied to AI evidence, the Daubert framework provides a structured methodology for judicial gatekeeping that is directly adaptable to the Indian context. The BSA's requirement of expert certification under Section 63(4) could be developed through judicial interpretation into a Daubert-equivalent inquiry, requiring the proponent of AI evidence to demonstrate testability, error rates, peer review, and scientific consensus before the evidence is admitted. This paper proposes the formal adoption of a Daubert-equivalent standard for AI evidence in India.

²⁷ *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993)

²⁸ *Gen. Elec. Co. v. Joiner*, 522 U.S. 136 (1997) (establishing abuse-of-discretion as the appellate standard of review for expert testimony admissibility rulings); *see also* *Kumho Tire Co. v. Carmichael*, 526 U.S. 137 (1999) (extending the *Daubert* gatekeeping function to all expert testimony under Federal Rule of Evidence 702).

5.3.Singapore's Statutory Presumption Model

Singapore's Evidence Act (Cap. 97) adopts a statutory presumption of computer reliability under Section 116A²⁹, shifting the burden of disproving system reliability to the opposing party. The said section creates a rebuttable presumption that where a device or process is of a kind that ordinarily produces or communicates an electronic record when properly used, the court shall presume that the device or process accurately produced the record in question. The burden of rebutting the presumption lies with the opposing party. This model streamlines the admissibility process for well-validated systems. However, it is poorly suited to AI systems because the presumption was designed for deterministic software and does not account for the probabilistic, context-sensitive, and potentially biased outputs of machine-learning models. Even under Singapore's model, the proponent must establish through credible scientific and technical material that the AI tool ordinarily produces accurate outputs when properly used — a requirement that cannot be satisfied without transparency about the system's design, training data, and error rates.

6. PROPOSALS TOWARDS A REGULATORY FRAMEWORK

The foregoing analysis demonstrates that India's current legal framework — the BSA 2023, the DPDPA 2023, and the BNSS 2023 — provides a necessary but insufficient foundation for the governance of AI in criminal justice. This section sets out eight concrete regulatory proposals, structured around three pillars: evidentiary standards, institutional architecture, and constitutional compliance.

6.1.Evidentiary Standards

Proposal 6.1.1: A Daubert-Equivalent Pre-Admission Inquiry for AI Evidence

The legislature shall, through an amendment to the BSA, establish a mandatory gatekeeping inquiry before AI-generated evidence is admitted in criminal proceedings. This inquiry should assess: (i) whether the AI system has been validated through peer-reviewed testing; (ii) its documented error rate, including disaggregated performance across demographic groups; (iii) whether the system's methodology is publicly documented and independently reproducible; and (iv) whether there is scientific

²⁹ Evidence Act, *supra* note 12, § 116A.

consensus on the system's reliability for the specific investigative application.

Proposal 6.1.2: Statutory Definition of 'AI Expert' Under BSA Section 63(4)

An amendment to Section 63(4) of the BSA should define the qualifications required of an "expert" certifying AI-generated evidence. This definition should require, at a minimum: formal training in machine learning or AI systems; familiarity with the specific system being certified; and independence from the agency that deployed the system. A national register of accredited AI evidence experts should be maintained by the Ministry of Law and Justice.

Proposal 6.1.3: A Mandatory Deepfake Authentication Protocol

Any audio-visual electronic record submitted as evidence in criminal proceedings should be subject to mandatory deepfake detection analysis as a pre-admission requirement. The Ministry of Electronics and Information Technology should, in consultation with the Ministry of Home Affairs, prescribe technical standards for deepfake detection, and accredited Forensic Science Laboratories should be equipped with the relevant detection tools.

6.2. Institutional Architecture

Proposal 6.2.1: A National AI in Criminal Justice Oversight Authority

An independent statutory authority should be established to oversee the deployment of AI in criminal justice. Its functions should include: (i) pre-deployment certification of AI investigative tools; (ii) mandatory algorithmic impact assessments; (iii) post-deployment auditing for accuracy, bias, and constitutional compliance; (iv) maintenance of a public register of all AI systems deployed by law enforcement agencies; and (v) adjudication of complaints from individuals affected by AI investigative decisions.

Proposal 6.2.2: Mandatory Algorithmic Impact Assessments

No AI investigative tool should be deployed by any law enforcement agency without a prior algorithmic impact assessment (AIA) conducted by an accredited independent

body. The AIA should evaluate accuracy metrics across demographic groups, potential for bias amplification, the constitutional proportionality of the proposed deployment, DPDPA compliance, and the operational safeguards in place to prevent misuse. AIA reports should be publicly available.

Proposal 6.2.3: Upgrading Forensic Science Laboratory Capacity

The Central and State Forensic Science Laboratories should be resourced with dedicated AI forensics units staffed by qualified data scientists and machine-learning specialists. These units should be available to conduct independent technical review of AI-generated evidence for both the prosecution and the defence — with defence access guaranteed free of charge to economically vulnerable accused persons — and to provide expert witness testimony in criminal proceedings.

6.3. Constitutional Compliance

Proposal 6.3.1: A Dedicated Statutory Framework for AI Surveillance

A dedicated statute governing law enforcement use of AI surveillance technologies should be enacted, providing: (i) a clear legal basis for each category of AI surveillance (AFRS, predictive policing, NLP-based monitoring), satisfying the Puttaswamy legality requirement; (ii) a sunset clause requiring parliamentary review of each deployment authorisation every three years; (iii) data minimisation and retention limits consistent with the DPDPA; (iv) prohibition on individual predictive profiling by reference to protected characteristics under Articles 14 and 15; and (v) a mandatory access-to-information right enabling individuals to know whether AI surveillance has been conducted on them.

Proposal 6.3.2: A Proportionality Protocol for AFRS and Predictive Policing Deployment

Any deployment of AFRS or predictive policing in a specific operational context — whether crowd management, missing persons identification, or crime prevention — should be subject to a written proportionality assessment, signed by a senior officer of at least Superintendent rank, before deployment. This assessment should document the specific legitimate aim pursued, the necessity of AI deployment relative to less intrusive alternatives, and the safeguards in place to prevent scope creep or misuse.

7. CONCLUSION

Artificial Intelligence is already reshaping the operational landscape of Indian criminal justice. Facial recognition systems scan crowds at public events. Predictive algorithms assign risk scores to communities and individuals. Probabilistic genotyping interprets DNA evidence through statistical simulation. NLP tools mine social media and communications data for investigative leads. These are not prospective developments; they are present realities operating in an institutional and legal environment that has not been designed to accommodate them.

The Bharatiya Sakshya Adhiniyam, 2023, provides the most current statutory framework for this challenge. Its reclassification of electronic records as primary evidence and its dual-certification requirement under Section 63(4) represent meaningful progress. But the BSA's silence on what constitutes a qualifying AI expert, its absence of any AI-specific reliability standard, and its complete inattention to emerging threats such as deepfake evidence reveal a statute that was drafted for the electronic world of today rather than the algorithmic world of tomorrow.

The constitutional framework, anchored by the Puttaswamy proportionality standard, provides indispensable protections. But constitutional scrutiny is retrospective and case-specific; it adjudicates harm after it has occurred. India requires a proactive regulatory architecture: one that mandates pre-deployment validation, ensures algorithmic transparency, guarantees adversarial access to AI evidence, and institutionalises independent oversight. The EU AI Act demonstrates that such architecture is achievable. The Daubert standard demonstrates that judicial gatekeeping of scientific evidence is both workable and rights-protective. India does not need to replicate these models wholesale, but it cannot responsibly ignore them.

The overarching principle that must guide Indian policy is clearly stated by the Supreme Court and by scholars across the field: AI may assist in law enforcement, but it must never displace the constitutional and ethical foundations of India's criminal justice system. Human decision-makers must remain the final arbiters of legal outcomes. AI must be testable, contestable, and accountable. Evidence produced by algorithms must meet the same standards of reliability, authenticity, and transparency as evidence produced by any other means.

This research paper provides the first comprehensive doctrinal analysis of AI-generated evidence under the BSA 2023, the first constitutional mapping of AI surveillance obligations

under the Puttaswamy-DPDPA framework, and the first comparative-regulatory proposal tailored to the Indian criminal justice ecosystem. The gap between AI's operational deployment and its legal accountability is not merely a technical inconvenience but a structural threat to the rule of law, one that demands urgent, systematic, and constitutionally grounded scholarly and legislative attention.