Volume 3, Issue 4 ISSN 2582-743X

AI Assisted Criminal Investigation Under the Bharitya Sakshya Adhiniyam, 2023: Issues of Admissibility and Reliability

Sooraj Kumar Sonkar
Research Scholar
Faculty of Law, University of Allahabad, India

Abstract

The Bharatiya Sakshya Adhiniyam, 2023 ('BSA' or 'the Adhiniyam'), which replaced the Indian Evidence Act, 1872 with effect from 1 July 2024, modernised the law of documentary and electronic evidence for an age of digitised policing, but it did so without contemplating the distinct evidentiary problems posed by artificial intelligence ('AI') tools now deployed at the investigative stage — facial recognition, predictive-policing analytics, automated forensic matching and algorithmic risk scoring. This paper argues that the BSA's electronic-evidence framework, built around Sections 61 to 63 and the expert-opinion provisions of Sections 39 and 40, was designed to authenticate the *mechanical integrity* of a computer output — that a record was accurately generated and has not been tampered with — and is structurally unsuited to testing the *epistemic reliability* of an algorithmic inference produced by a system whose reasoning is probabilistic, proprietary and often opaque even to its operators. Drawing on the Supreme Court's privacy and due-process jurisprudence in *Justice K.S. Puttaswamy v Union of India* and *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal*, on the documented misidentification risks of facial recognition deployment during the 2020 Delhi riots investigations, and on comparative responses in the United Kingdom, the United States and the European Union, the paper contends that admissibility and reliability are analytically distinct inquiries that Indian evidence law currently collapses into a single certification gateway. It proposes a calibrated reform model — a reliability-specific gatekeeping standard, mandatory algorithmic disclosure and audit-trail requirements, a statutorily recognised class of AI-systems examiners distinct from the ordinary Examiner of Electronic Evidence, and a non-derogable human-corroboration rule for investigative leads — designed to permit AI-assisted investigation to continue while preventing algorithmic output from silently migrating, uninterrogated, from investigative tool to courtroom proof.

Keywords: Bharatiya Sakshya Adhiniyam; artificial intelligence; electronic evidence; facial recognition technology; algorithmic reliability; Section 63; expert evidence; admissibility; criminal investigation; Article 21; due process.

Introduction

On 1 July 2024, the Bharatiya Sakshya Adhiniyam, 2023 replaced the Indian Evidence Act, 1872, alongside two companion statutes recasting India's substantive and procedural criminal law.[1] The Adhiniyam's most consequential innovation for present purposes lies in Sections 61 to 63, which recognise electronic and digital records as documents on an equal evidentiary footing with paper, and which correct a doctrinal difficulty that had, under the old Section 65B

[1] The Bharatiya Nyaya Sanhita, 2023 replaced the Indian Penal Code, 1860; the Bharatiya Nagarik Suraksha Sanhita, 2023 replaced the Code of Criminal Procedure, 1973; and the Bharatiya Sakshya Adhiniyam, 2023 (Act No. 47 of 2023) replaced the Indian Evidence Act, 1872. All three came into force on 1 July 2024.

Volume 3, Issue 4 ISSN 2582-743X

regime, made a strict certification requirement the sole gateway through which a computer output could enter evidence.[2] This legislative modernisation, however, was drafted with a particular evidentiary object in view: authenticating records *generated* by a computer, camera or communication device in the ordinary course of its operation — a CCTV recording, a call detail record, an email. It was not drafted with artificial intelligence in mind.

Yet AI is no longer a peripheral feature of Indian criminal investigation. In February 2025, the Ministry of Law and Justice publicly committed the government to building a justice system that is 'fully future-ready' through the integration of artificial intelligence into policing and investigation.[3] Facial recognition technology ('FRT') is already deployed by police forces across the country — the Delhi Police has used FRT to screen crowds at protests and public events,[4] and the Hyderabad Command and Control Centre integrates facial-recognition-enabled analytics across nearly 700,000 CCTV cameras.[5] A National Automated Facial Recognition System has been proposed to integrate identification data across law enforcement databases nationally,[6] and Section 176(3) of the Bharatiya Nagarik Suraksha Sanhita, 2023 now imposes a statutory, technology-forward mandate requiring a forensic expert to attend the crime scene, and the process to be videographed, in every offence punishable with seven years' imprisonment or more — a mandate to be operationalised in stages over five years.[7]

This expansion of algorithmic policing has occurred in the near-total absence of statutory rules or judicial precedent tailored to AI-enabled investigative tools.[8] The 2020 Delhi riots investigations, in which facial recognition matching was used to identify persons for arrest, are frequently cited as the clearest domestic illustration of the risk: a technology deployed at speed and at scale, without a settled evidentiary protocol governing how — or whether — its output could be tested, challenged or corroborated before it translated into coercive state action.[9] This paper asks a narrower question than the broader policy debate over the desirability of AI-assisted policing. It does not ask whether AI tools should be used in criminal investigation at all

[2] Bharatiya Sakshya Adhiniyam, 2023, s 2(1)(e)(i) (classifying electronic or digital records as documents); s 61 (electronic or digital records not to be denied admissibility on the ground that they are electronic or digital); s 62 (contents of electronic records to be proved in accordance with s 63); s 63 (conditions for admissibility of electronic records, successor to s 65B of the Indian Evidence Act, 1872, and introducing a dual-certification requirement under s 63(4)).

[3] Press release, Ministry of Law and Justice, Government of India, 25 February 2025, quoted in the context of AI integration into Indian law enforcement and criminal investigation; see also discussion in S. et al, 'Unquestioned Use of AI-Based Facial Recognition Technology in Criminal Investigations: Delhi Riots Lessons on Rights and Reliability' (2026) MDPI

[4] See Aakriti Sharma, 'Facial Recognition Evidence: Legal and Ethical Limits' (FreeLaw, 12 September 2025), noting Delhi Police's use of facial recognition tools during protests and public events.

[5] Rahul Bedi, 'Facial recognition becomes key law enforcement tool in India' (Gulf News); the Hyderabad Command and Control Centre pairs live CCTV feeds with a mugshot database and facial recognition software to scan footage for known offenders.

[6] See discussion in Aakriti Sharma (n 3); see also the Facial Recognition Technology (Regulation of Police Powers) Bill, 2023, introduced in the Rajya Sabha in December 2023 and pending as of the date of this paper.

[7] Bharatiya Nagarik Suraksha Sanhita, 2023, s 176(3). The provision takes effect from a date to be notified by the State Government concerned within five years of the Sanhita's commencement, and requires videography of the forensic process on a mobile phone or other electronic device.

[8] The absence of Indian statutory rules or case law specifically addressing AI-enabled investigative tools is noted in the comparative literature; see 'Unquestioned Use of AI-Based Facial Recognition Technology in Criminal Investigations' (n 2).

[9] Ibid, discussing the 2020 Delhi riots cases alongside comparative instances of wrongful identification through facial recognition, including the Christopher Gatlin and Nijeer Parks cases in the United States, and documented racial disparities in the UK's retrospective facial recognition deployments.

Volume 3, Issue 4 ISSN 2582-743X

— a question on which legitimate policy disagreement exists — but whether the BSA's existing evidentiary architecture, designed for authenticating computer-generated records, can adequately test the admissibility *and* the reliability of output generated not by mechanical recording but by probabilistic inference The argument proceeds in nine further parts. Part II maps the principal AI tools currently deployed in Indian criminal investigation. Part III sets out the BSA's statutory architecture as it bears on electronic and AI-generated evidence. Part IV isolates the admissibility problem — the mismatch between a document-based certification gateway and algorithmic output. Part V isolates the distinct reliability problem — the black-box, bias and error-rate concerns that certification does not test. Part VI surveys the relevant constitutional and judicial trajectory. Part VII draws comparative lessons from the United Kingdom, the United States and the European Union. Part VIII proposes a reliability-centred evidentiary standard. Part IX sets out a calibrated reform model, and Part X concludes.

Mapping Artificial Intelligence in Indian Criminal Investigation

Four categories of AI tool are now embedded, in varying degrees of maturity, within Indian investigative practice. *First*, facial recognition technology is used both retrospectively — matching a suspect's image against a database of photographs or CCTV footage after an offence — and, more controversially, in real time at public gatherings, protests and events.[10] The Facial Recognition Technology (Regulation of Police Powers) Bill, 2023, introduced as a private member's bill and pending before the Rajya Sabha, would, if enacted, be India's first dedicated statutory framework governing the conditions of FRT deployment by police, its retention periods and its evidentiary use — a legislative vacuum that the BSA, drafted contemporaneously but silent on AI-specific tools, does not fill.[11]

Second, algorithmic crime-mapping and predictive-policing tools, integrated with the Crime and Criminal Tracking Network and Systems (‘CCTNS’) and the National Automated Fingerprint Identification System, are used to identify crime ‘hotspots’, flag repeat-offender patterns and *AI*- generate investigative leads from historical crime data — a use of AI that, unlike FRT, rarely produces output tendered directly as evidence, but that shapes the direction and intensity of investigation in ways that can determine whose conduct comes under judicial scrutiny in the first place. *Third*, forensic AI is increasingly used to accelerate DNA profile matching, ballistic comparison and digital-forensic triage — a development the legislature has itself encouraged through Section 176(3) of the Bharatiya Nagarik Suraksha Sanhita's mandatory forensic-attendance requirement for serious offences, though that provision addresses the *collection* of forensic evidence rather than the reliability of any algorithmic tool used to analyse it.[12] *Fourth*, generative and deepfake-detection AI is emerging as a tool both for investigators (verifying the authenticity of digital media tendered as evidence) and for adversarial parties (challenging the authenticity of that same media) — a use case the BSA addresses only obliquely, through the general expert-opinion provisions discussed in Part III.

[10] See Aakriti Sharma (n 3), distinguishing retrospective FRT matching from live, real-time deployment at public gatherings.

[11] See the discussion of the Facial Recognition Technology (Regulation of Police Powers) Bill, 2023 in the comparative literature on FRT admissibility under the BSA, including its interplay with the Digital Personal Data Protection Act, 2023.

[12] Bharatiya Nagarik Suraksha Sanhita, 2023, s 176(3) (n 6); see also 'Revolutionizing Criminal Investigations: The Forensic Mandate Under Section 176 of BNSS' (2025) IJLLR, on the provision's aim of enhancing evidentiary integrity through scientific policing.

Volume 3, Issue 4 ISSN 2582-743X

What unites these otherwise disparate applications is the absence of a settled answer to two distinct questions that this paper treats separately throughout: can the output of the tool be admitted into evidence at all, and, if admitted, how much weight should the trier of fact place upon it. The Delhi riots FRT deployments illustrate why the distinction matters in practice. Comparative research on facial recognition deployment documents materially higher false-positive rates for darker-skinned faces under real-world lighting and crowd conditions than under laboratory testing conditions[13] — a reliability concern entirely independent of whether the underlying photographic record was authentically captured and unaltered, which is the only question the BSA's certification regime is designed to test.

The Statutory Architecture of the BSA Relevant to AI Evidence

A. The Electronic Records Provisions: Sections 61 to 63

Section 2(1)(e)(i) of the BSA classifies 'electronic or digital records' as documents, placing them on the same footing as paper records for the purposes of the Adhiniyam.[14] Section 61 provides that nothing in the Adhiniyam shall be used to deny the admissibility of an electronic or digital record on the ground that it is electronic or digital, and that such a record shall, subject to Section 63, have the same legal effect, validity and enforceability as any other document.[15] Section 62 provides that the contents of an electronic record may be proved in accordance with Section 63, and Section 63 — the direct successor to Section 65B of the Indian Evidence Act, 1872 — sets out the conditions under which a 'computer output' is deemed to be a document, including, under Section 63(4), a dual-certification requirement calling for authentication by both the person in charge of the relevant device and, in specified circumstances, an independent expert.[16]

Section 61 carries a specific doctrinal history. The Supreme Court's decision in *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal* had held, reaffirming *Anvar P.V. v P.K. Basheer* and overruling the more lenient approach in *Shafhi Mohammad v State of Himachal Pradesh*, that a Section 65B(4) certificate was a mandatory precondition for the admission of secondary electronic evidence, with no substantial-compliance exception available where the certifying party had failed to produce one.[17] Section 61's opening formula — 'nothing in this Adhiniyam shall apply to deny the admissibility' — is understood to correct the rigidity of that certificate-only regime by affirming that a copy of an electronic record may also be proved by any other method otherwise permissible for proving a document, restoring a measure of the flexibility *Arjun Panditrao* had foreclosed.[18]

---

[13] See 'Unquestioned Use of AI-Based Facial Recognition Technology in Criminal Investigations' (n 2), citing UK Home Office data showing retrospective facial recognition systems producing false-positive rates of 0.04% for white faces as against approximately 4% for Asian faces and higher rates still for Black subjects, and noting the absence of any comparable Indian validation data.

[14] Bharatiya Sakshya Adhiniyam, 2023, s 2(1)(e)(i).

[15] Ibid

[16] Bharatiya Sakshya Adhiniyam, 2023, s 63, in particular s 63(4). Section 63 extends the earlier Section 65B framework to information stored in semiconductor memory and to output from 'any communication device', and refines the statutory definition of a computer or communication device under s 63(3).

[17] Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal (2020) 7 SCC 1 (Nariman, Bhat and Ramasubramanian JJ), reaffirming Anvar P.V. v P.K. Basheer (2014) 10 SCC 473 and overruling the substantial-compliance approach taken in Shafhi Mohammad v State of Himachal Pradesh (2018) 2 SCC 801.

[18] See Saji Koduvath, "'Nothing In This Adhiniyam Shall Apply To Deny The Admissibility" — New Provision (S. 61, BSA)' (Indian Law Live, 2026), arguing that Section 61 is enacted with a view to overriding the strict-

Volume 3, Issue 4 ISSN 2582-743X

This history matters for AI evidence because it reveals the conceptual register in which Sections 61 to 63 operate: the entire scheme is concerned with proving that a *copy* of a record accurately reproduces an *original* — that the hash value matches, that the device was operating correctly, that no tampering occurred in transmission. None of these conditions, however rigorously applied, says anything about whether the underlying inference generated by an algorithm operating on that record — a facial-recognition match score, a risk classification, a predictive flag — is itself accurate. A perfectly authenticated video recording can still feed a facial-recognition model that misidentifies its subject; Section 63's certificate would be satisfied in full even where the algorithmic output built upon that footage is wrong.

B. The Expert Opinion Provisions: Sections 39 to 41

The BSA's only sustained engagement with the reliability, as opposed to the authenticity, of technical evidence lies in its expert-opinion provisions. Section 39(1), the successor to Section 45 of the Indian Evidence Act, 1872, makes relevant the opinion of persons specially skilled in 'foreign law, science or art, or any other field', including the identity of handwriting or finger impressions.[19] Section 39(2) — a genuinely new provision without a direct predecessor — makes the opinion of the 'Examiner of Electronic Evidence' recognised under Section 79A of the Information Technology Act, 2000 a relevant fact whenever the court must form an opinion on any matter relating to information transmitted or stored in a computer resource or in any electronic or digital form, and deems such an examiner to be an expert for this purpose.[20] Section 40 permits facts that support or are inconsistent with an expert's opinion to be treated as relevant, allowing the grounds and methodology underlying an opinion to be tested and corroborated or contradicted.[21]

Section 39(2) is the closest doctrinal hook the BSA offers for AI-generated investigative output, and it is instructive precisely because of how far short it falls. An Examiner of Electronic Evidence under Section 79A of the Information Technology Act, 2000 is certified competent in digital forensics generally — recovering, preserving and interpreting data from computer systems — not in the specific epistemic risks that machine-learning systems present: non-deterministic output, training-data bias, proprietary opacity, and a probability of error that is a property of the model's design rather than of any defect in the record it examined. Treating a facial-recognition match or a predictive-policing flag as simply another species of 'information stored in a computer resource', testable through the general expert-opinion machinery of Section 39, elides a distinction Part V of this paper argues the law cannot safely elide: the difference between an expert *interpreting* a record and a system *generating* an inference about it.

The Admissibility Problem: Fitting Algorithmic Output into a Document-Based Scheme

The first and narrower difficulty is doctrinal fit. Electronic evidence law, both before and after the BSA, has been built around the paradigm of the *document* — a discrete, static record that a machine mechanically produces and that a human party then seeks to prove. Commentary on

certificate effect of Arjun Panditrao and would otherwise be redundant.

[19] Bharatiya Sakshya Adhiniyam, 2023, s 39(1), corresponding to s 45 of the Indian Evidence Act, 1872.

[20] Bharatiya Sakshya Adhiniyam, 2023, s 39(2), read with s 79A, Information Technology Act, 2000 (empowering the Central Government to notify Examiners of Electronic Evidence).

[21] Bharatiya Sakshya Adhiniyam, 2023, s 40, corresponding to s 46 of the Indian Evidence Act, 1872.

Volume 3, Issue 4 ISSN 2582-743X

the BSA's electronic-evidence framework observes that the entire Section 61–63 scheme responds to the reality that a digital file 'can be copied a thousand times, edited invisibly, and stripped of the very data that would prove where it came from', and answers that risk with a scheme of authentication: recognition (Section 61), a route to proof (Section 62) and conditions for admissibility including certification (Section 63).[22] Facial recognition output, by contrast, is not a copy of anything that existed before the algorithm ran. It is a newly generated inference — a probability score, a ranked list of candidate matches — produced by applying a trained statistical model to an underlying image. As commentary on FRT's evidentiary status in India observes, the pre-BSA electronic-evidence provisions of the Indian Evidence Act were 'limited to "electronic records" being deemed admissible in law — the same being proxies in lieu of physical documents', whereas FRT output is 'an algorithmic technology that is more sophisticated and distinct from electronic records', such that it remains 'unclear how inputs provided by it in a live investigation or surveillance exercise can be used as acceptable evidence in a court of law'.[23]

This gap has not been closed by the transition from the Indian Evidence Act to the BSA, because Sections 61 to 63 retain precisely the same conceptual structure as the former Sections 65A and 65B — they merely refine it, most notably through Section 61's correction of *Arjun Panditrao*'s rigid certificate requirement and Section 63's extension to semiconductor memory and communication devices. Neither amendment addresses the categorical question of what counts as the relevant 'computer output' when a system does not simply store or reproduce data but analyses it and returns a conclusion the human investigator did not independently reach. In practice, prosecutors and investigating agencies resolve this gap informally by treating the algorithmic output as though it were itself a document — a printout of a match score, certified under Section 63 in the same manner as a call detail record. That approach satisfies the letter of Section 63 while leaving entirely untested the question Part V addresses: whether the process that generated the printout is one a court has any principled basis to trust.

The Reliability Problem: Opacity, Bias and the Limits of Certification

The second and deeper difficulty is that even a wholly compliant Section 63 certificate resolves nothing about reliability. Three features of AI-assisted investigative tools place them outside the assumptions on which the certification regime, and indeed the ordinary expert-opinion regime under Section 39, were built.

First, opacity. Commentary on AI-generated evidence in Indian courts observes that the right to a fair trial may be violated by the use of opaque, algorithmically generated evidence, since 'a "decision" made by an algorithm whose logic is inaccessible cannot be rationally defended against by an individual'.[24] This is not a peculiarly Indian problem: in the leading American illustration, *State v Loomis*, the Wisconsin Supreme Court permitted a court to consider a proprietary COMPAS risk-assessment score at sentencing notwithstanding that the algorithm's internal weighting of factors was a trade secret unavailable to the defendant, while cautioning

[22] See the account of the BSA's three-section electronic-evidence scheme in the discussion of Sections 61–63, describing the statutory response to the malleability of digital records.

[23] Vipra Jauhar, 'Addressing Constitutional Challenges in Use of Facial Recognition Technology by Indian Law Enforcement Agencies' (JURIST, 10 February 2022), a critique made under the Indian Evidence Act, 1872 that the BSA's electronic-records provisions have not resolved, since Sections 61 to 63 retain the same document/computer-output paradigm as the former Sections 65A and 65B.

[24] 'AI-Generated Evidence in Indian Courts: Admissibility and Legal Challenges' (Law Jurist, 2 July 2025).

Volume 3, Issue 4 ISSN 2582-743X

that such tools may be used only to inform, not determine, judicial outcomes, and mandating that sentencing courts be furnished with a written advisement of the tool's documented limitations.[25] Section 39(2) of the BSA contains no analogous safeguard: an Examiner of Electronic Evidence testifying to a facial-recognition match is not required to disclose — because the examiner may not possess — the model's training data, its documented error rates, or the confidence threshold applied to the match.

Second, demographic bias. Empirical study of facial recognition deployment documents systematic disparities in false-positive rates across demographic groups under real-world conditions. UK Home Office data on retrospective facial-recognition systems recorded false-positive rates of approximately 0.04% for white faces as against roughly 4% for Asian faces and higher rates again for Black subjects — a disparity the relevant literature describes as evidence that FRT 'is not neutral in retrospective circumstances'.[26] No published validation study of comparable rigour exists for FRT systems deployed by Indian police forces, notwithstanding their use in live operational settings including the 2020 Delhi riots investigations and routine crowd screening at public events. A Section 63 certificate authenticating the chain of custody of a matched photograph says nothing about whether the underlying matching algorithm performs with materially different accuracy across the skin tones, lighting conditions and camera angles that Indian policing conditions typically present.

Third, the absence of a settled judicial reliability test. Common-law and constitutional systems that have confronted algorithmic evidence directly have developed gatekeeping doctrines specifically calibrated to scientific and technical reliability — the *Daubert* standard in American federal practice, and the general acceptance inquiry it displaced. Indian evidence law has no comparable, judicially articulated reliability threshold distinct from the ordinary rules of relevance and expert competence under Sections 39 and 40. The result is that an algorithmic tool's output is tested, if at all, by the same standard applied to a fingerprint examiner's opinion — a standard built for a discipline with decades of peer-reviewed validation, applied to a class of tools that are frequently proprietary, rapidly iterated and, in the Indian context, largely unvalidated on domestic populations.

Constitutional Foundations and the Judicial Trajectory

The constitutional backdrop against which these evidentiary gaps must be assessed is supplied principally by Article 21. In *Justice K.S. Puttaswamy v Union of India*, the Supreme Court located a right to privacy, encompassing informational and decisional dimensions, within the guarantee of life and personal liberty, and required that any State intrusion upon it satisfy a structured proportionality standard — legality, legitimate aim, necessity and proportionality stricto sensu.[27] Commentary on facial recognition's constitutional standing in India applies this framework directly, observing that FRT deployment must conform to Article 21 and that the

[25] State v Loomis, 2016 WI 68, 881 N.W.2d 749 (Wis 2016). The Wisconsin Supreme Court upheld the use of a COMPAS risk-assessment score at sentencing subject to safeguards, including judicial discretion not to be bound by the score and a mandatory written advisement of COMPAS's documented limitations, among them its proprietary and undisclosed weighting methodology and its use of group-level, rather than individualised, risk data.

[26] 'Unquestioned Use of AI-Based Facial Recognition Technology in Criminal Investigations' (n 2), citing UK Home Office and BBC-reported data on live and retrospective facial recognition technology deployment between January 2024 and mid-2025.

[27] Justice K.S. Puttaswamy (Retd) v Union of India (2017) 10 SCC 1.

Volume 3, Issue 4 ISSN 2582-743X

absence of a comprehensive data-protection regime historically left FRT's use 'potentially unconstitutional' for want of a legality safeguard.[28] The enactment of the Digital Personal Data Protection Act, 2023 has partially addressed that legality gap for personal data generally, but neither that Act nor the BSA speaks to the distinct evidentiary question this paper isolates: even where FRT deployment is itself lawful under Article 21 and the DPDP Act, the *output* of that lawful deployment may still be unreliable, and unreliable evidence used to secure an arrest or conviction implicates the fair-trial and due-process guarantees of Article 21 independently of any privacy violation in its collection.

India's courts have not yet had occasion to confront this admissibility-versus-reliability distinction directly in the context of an AI investigative tool. The nearest domestic analogue remains *Arjun Panditrao*, which, though concerned with an ordinary computer output rather than an algorithmic inference, is instructive for the rigour of its insistence that a party seeking to rely on electronic evidence bear the burden of establishing, through a properly sourced certificate, that the record is what it purports to be.[29] Applied by extension — and this paper argues it must be, if the proportionality logic of *Puttaswamy* is to be given effect — the burden-allocation logic of *Arjun Panditrao* suggests that a party relying on AI-generated investigative output should equally bear the burden of establishing, through evidence a defendant can meaningfully test, that the underlying system is reliable for the purpose for which it was used, and not merely that the record it produced was accurately transmitted and stored.

Comparative Perspectives

India is not alone in confronting the mismatch between inherited evidentiary categories and algorithmic investigative tools, and comparative practice offers three distinct responses.

The United Kingdom has confronted FRT's constitutional limits directly. In *R (Bridges) v Chief Constable of South Wales Police*, the Court of Appeal held that South Wales Police's use of live automated facial recognition breached Article 8 of the European Convention on Human Rights, the Data Protection Act 2018 and the public sector equality duty, principally because the force had failed to satisfy itself that the software did not produce racially or sexually discriminatory outcomes.[30] The decision has since shaped operational guidance requiring bias auditing as a precondition of deployment, addressing the reliability question at the point of use rather than leaving it to be litigated after the fact at trial.

The United States has confronted the reliability question primarily in the sentencing rather than the investigative context, through *State v Loomis*'s conditional approval of algorithmic risk assessment subject to mandatory disclosure of a tool's documented limitations and a rule against sole or determinative reliance on its output.[31] More broadly, American federal courts test the admissibility of novel scientific and technical evidence, including forensic-AI methodologies, against the reliability-focused *Daubert* standard — an inquiry expressly

[28] Aakriti Sharma (n 3), applying the Puttaswamy proportionality framework to facial recognition technology and noting the historical absence of comprehensive data-protection legislation in India.

[29] Arjun Panditrao Khotkar (n 12).

[30] R (Bridges) v Chief Constable of South Wales Police [2020] EWCA Civ 1058, holding the deployment of live automated facial recognition technology unlawful for want of an adequate legal framework, adequate assessment of the software's demographic bias, and compliance with the public sector equality duty.

[31] State v Loomis (n 20).

Volume 3, Issue 4 ISSN 2582-743X

directed at testability, known error rates, peer review and general acceptance, and thus structurally distinct from, and additional to, any authentication requirement analogous to the BSA's Section 63.

The European Union's Artificial Intelligence Act classifies AI systems used by law enforcement for individual risk assessment, evidence reliability evaluation, or biometric identification as 'high-risk', triggering mandatory obligations of accuracy, robustness, human oversight, transparency and documentation before such systems may be deployed at all — a regulatory, ex ante approach to reliability that operates independently of, and prior to, any evidentiary admissibility determination made later in a criminal proceeding.[32]

What unites these three approaches, despite their differing legal traditions, is a structural feature the BSA presently lacks: each treats reliability as a question requiring its own dedicated inquiry — whether through ex ante regulatory classification (the EU), a judicially developed scientific-reliability threshold (the United States), or a bias-specific public-law duty enforceable independently of any criminal trial (the United Kingdom) — rather than allowing it to be subsumed within an authentication or expert-competence test built for a different evidentiary problem.

Toward a Reliability-Centred Evidentiary Standard

The preceding analysis suggests that Indian evidence law currently asks only one of the two questions AI-generated investigative output requires. Section 63 asks: is this an accurate copy of what the system produced? It does not ask, and Section 39(2)'s Examiner of Electronic Evidence is not equipped to answer: is what the system produced itself trustworthy? A reliability-centred standard, adapted from the comparative material surveyed in Part VII to the specific structure of the BSA, would require a court, before admitting AI-generated output as evidence of guilt or as the basis for an arrest, to satisfy itself on four matters distinct from Section 63 certification

First, that the system's documented error rate, and any demographic variance in that error rate, has been disclosed and is available for cross-examination — addressing the opacity concern that *Loomis* partially addressed through mandatory advisement rather than exclusion. Second, that the system's output was corroborated by independent, non-algorithmic investigative evidence before being acted upon, a safeguard directed at the risk, most vividly illustrated by the Delhi riots deployments, of treating a probabilistic match as though it were an eyewitness identification. Third, that the specific deployment context — lighting, image quality, crowd density — falls within conditions for which the system has been validated, rather than merely within the conditions under which it was originally trained. Fourth, that where the tool's proprietary status genuinely precludes full algorithmic disclosure, the burden of establishing reliability by other means — validation studies, audit outcomes, comparative accuracy data — rests on the party seeking to rely on the evidence, mirroring the burden-allocation logic *Arjun Panditrao* applied to conventional electronic records.

[32] See discussion of the EU Artificial Intelligence Act's classification of judicial and law-enforcement AI systems as 'high-risk', with attendant obligations of accountability, transparency and human oversight, in 'AI-Generated Evidence in Indian Courts' (n 19).

Volume 3, Issue 4 ISSN 2582-743X

A Calibrated Reform Model

None of the foregoing requires dismantling the BSA's electronic-evidence architecture or treating AI-assisted investigation as inherently illegitimate. It requires supplementing Sections 39 and 63 with provisions addressed specifically to algorithmic reliability. Five elements, drawn from the comparative and doctrinal analysis above, would constitute the core of such a model.

A. Statutorily Recognised Class of AI-Systems Examiners.

Section 39(2) should be amended to create a category of certified AI-systems examiner, distinct from the Examiner of Electronic Evidence under Section 79A of the Information Technology Act, 2000, whose certification standard specifically tests competence in algorithmic validation, bias auditing and error-rate interpretation — competencies the digital-forensics-oriented Section 79A certification does not test.

B. Mandatory Algorithmic Disclosure and Audit-Trail Requirements.

Modelled on the disclosure obligation *Loomis* imposed at sentencing, any AI-generated output tendered as investigative evidence should be accompanied by a standardised disclosure of the system's documented accuracy, any known demographic performance variance, and the confidence threshold applied — available to the defence in the same manner as a Section 63 certificate is presently available to test authenticity.

C. A Non-Derogable Human-Corroboration Rule.

Following the operational safeguard developed in response to *Bridges*, algorithmic output such as a facial-recognition match should be treated as an investigative lead requiring independent corroboration before it may found an arrest, and should never, standing alone, be sufficient to establish identity for the purposes of conviction — a rule that would need to operate through amendment to the Bharatiya Nagarik Suraksha Sanhita's arrest and investigation provisions as much as through the BSA itself.

D. Pre-Deployment Validation Aligned with Section 176(3).

Just as Section 176(3) of the Bharatiya Nagarik Suraksha Sanhita now mandates forensic-expert attendance for serious offences, an analogous ex ante validation requirement — independent bias and accuracy auditing before operational deployment, of the kind the EU's high-risk classification imposes — should apply to any AI tool a police force proposes to use for identification or evidentiary purposes, addressing reliability before the point of trial rather than only at it.

E. Enactment of the Facial Recognition Technology (Regulation of Police Powers) Bill.

The pending Bill should be enacted and its evidentiary provisions expressly cross-referenced to the BSA, so that FRT-specific safeguards — retention limits, deployment authorisation, audit obligations — are not left to operate in a separate silo from the general law of evidence that ultimately determines whether their output reaches a court.

Volume 3, Issue 4 ISSN 2582-743X

Conclusion

The Bharatiya Sakshya Adhiniyam, 2023 answers, more clearly than its predecessor, the question of whether an electronic record may be admitted into evidence. It does not answer, because it was not drafted to answer, the distinct question this paper has sought to isolate: whether an algorithm's inference about that record may be trusted. Sections 61 to 63 authenticate copies; Section 39 tests expert competence in interpreting records; neither provision was built to test the probabilistic, opaque and often demographically uneven reasoning of a machine-learning system. The 2020 Delhi riots investigations, the absence of any published Indian validation study for operationally deployed facial recognition systems, and the continuing legislative limbo of the Facial Recognition Technology (Regulation of Police Powers) Bill together suggest that this gap is not hypothetical. Comparative practice in the United Kingdom, the United States and the European Union demonstrates that reliability can be treated as a question in its own right — tested through bias auditing, mandatory disclosure, or ex ante regulatory classification — without requiring wholesale rejection of AI-assisted investigation. The constitutional future of criminal evidence in India, on the narrow question this paper has addressed, lies not in choosing between technological modernisation and evidentiary rigour, but in recognising, as the BSA's own correction of the *Arjun Panditrao* certificate rigidity through Section 61 already illustrates, that a statute drafted for one generation of evidentiary problems can, and should, be adapted before the next generation's problems arrive fully formed in a courtroom.

Bibliography

Statutes and Bills

- Constitution of India 1950.
- Bharatiya Sakshya Adhiniyam, 2023 (Act No. 47 of 2023). Bharatiya Nagarik Suraksha Sanhita, 2023.
- Bharatiya Nyaya Sanhita, 2023. Indian Evidence Act, 1872 (repealed).
- Code of Criminal Procedure, 1973 (repealed). Information Technology Act, 2000.
- Digital Personal Data Protection Act, 2023.
- Facial Recognition Technology (Regulation of Police Powers) Bill, 2023 (pending, Rajya Sabha).
- Data Protection Act 2018 (UK).
- Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).

Cases

- Anvar P.V. v P.K. Basheer (2014) 10 SCC 473.
- Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal (2020) 7 SCC 1. Justice K.S. Puttaswamy (Retd) v Union of India (2017) 10 SCC 1.
- R (Bridges) v Chief Constable of South Wales Police [2020] EWCA Civ 1058. Shafhi Mohammad v State of Himachal Pradesh (2018) 2 SCC 801.
- State v Loomis, 2016 WI 68, 881 N.W.2d 749 (Wis 2016).

Volume 3, Issue 4 ISSN 2582-743X

A. Reports and Official Documents

- Ministry of Law and Justice, Government of India, Press Release (25 February 2025)
- Ministry of Home Affairs, Government of India, The Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023 (Gazette of India, 25 December 2023).

B. Articles and Secondary Sources

- Aakriti Sharma, 'Facial Recognition Evidence: Legal and Ethical Limits' (FreeLaw, 12 September 2025).
- 'AI-Generated Evidence in Indian Courts: Admissibility and Legal Challenges' (Law Jurist, 2 July 2025).
- 'Regulation of FRT through India's Facial Recognition Technology Bill, 2023 and its Admissibility under BSA' (2026) Journal, National Forensic Sciences University.
- Rahul Bedi, 'Facial recognition becomes key law enforcement tool in India' (Gulf News).
- Saji Koduvath, '"Nothing In This Adhiniyam Shall Apply To Deny The Admissibility" — New Provision (S. 61, BSA)' (Indian Law Live, 2026).
- 'Revolutionizing Criminal Investigations: The Forensic Mandate Under Section 176 of BNSS' (2025) IJLLR.
- 'Unquestioned Use of AI-Based Facial Recognition Technology in Criminal Investigations: Delhi Riots Lessons on Rights and Reliability' (2026) MDPI.
- Vipra Jauhar, 'Addressing Constitutional Challenges in Use of Facial Recognition Technology by Indian Law Enforcement Agencies' (JURIST, 10 February 2022).