ARTIFICIAL INTELLIGENCE (AI)-GENERATED SYNTHETIC EVIDENCE AND THE CRIMINAL TRIAL IN INDIA: RETHINKING AUTHENTICATION, PROOF, AND STATUTORY SILENCE UNDER THE BHARATIYA SAKSHYA ADHINIYAM, 2023

Dr. Priyadarshi Nagda, Assistant Professor, University College of Law, Mohanlal Sukhadia University, Udaipur[1]

Zibran Khan Pathan, Research Scholar, University College of Law, Mohanlal Sukhadia University, Udaipur.[2]

ABSTRACT

Generative Artificial Intelligence (GenAI) has quietly upended the assumptions on which criminal evidence law was built. Systems capable of producing convincing synthetic audio, video, still images and written documents grouped here under the umbrella term "AI-generated evidence" have opened a jurisprudential fault line that legal systems worldwide, India included, have yet to close. India's newest evidence statute, the Bharatiya Sakshya Adhiniyam, 2023 ("BSA"), which supplanted the one-hundred-and-fifty-year-old Indian Evidence Act, 1872 with effect from 1 July 2024, is in many respects a genuine modernisation of the country's proof regime. Yet, as this paper contends, that modernisation stops short precisely where it is needed most: the BSA offers no meaningful answer to deepfakes, machine-fabricated documents, algorithmic behavioural predictions, or the wider category of machine-learning output now entering criminal courtrooms.

Working through doctrinal analysis, comparative law and constitutional reasoning, the paper isolates five structural gaps in the BSA: (i) no definitional scaffolding exists for AI-generated evidence as a distinct category; (ii) the certificate-driven authentication regime in Section 63 was never designed to test synthetic content and cannot do so reliably; (iii) the so-called "liar's dividend" erodes confidence even in genuine digital evidence; (iv) chain-of-custody norms remain silent on evidence that has passed through, or been produced by, an AI system; and (v) no competency benchmark exists for judges or forensic examiners tasked with evaluating AI-based outputs. The paper places these gaps against the backdrop of three

[1] Assistant Professor, University College of Law, Mohanlal Sukhadia University Udaipur.
[2] Research Scholar, University college of Law, Mohanlal Sukhadia University, Udaipur.

foreign models the still-developing US Federal Rule of Evidence 707, the European Union's Artificial Intelligence Act of 2024, and the United Kingdom's Forensic Science Regulator Act, 2021 to sketch out a reform agenda for India. It closes by proposing a new Schedule V-A to the BSA as a workable statutory template for regulating AI-generated evidence in Indian criminal trials.

I. INTRODUCTION: WHEN THE COURTROOM MEETS SYNTHETIC MEDIA

In mid-2023 an image began circulating across Indian social media showing a well-known political figure engaged in conduct entirely out of step with his public persona. The picture was quickly traced to AI generation, though only after it had already reached millions of screens. No court was ever asked to rule on it, yet the episode made something plain: generative AI can now manufacture falsehoods that the unaided eye cannot distinguish from reality. The obvious next question is what a court is supposed to do when such material is offered as evidence rather than gossip.

That question has already moved beyond the hypothetical. Around the world, litigants have begun tendering synthetic voice clips, doctored CCTV footage and algorithmically produced documents in both civil and criminal matters.[3] India's criminal justice apparatus already stretched thin by chronic case backlogs and limited institutional capacity is in no position to absorb this new category of risk.

The recent overhaul of India's criminal statutes the Bharatiya Nyaya Sanhita, 2023 ("BNS"), the Bharatiya Nagarik Suraksha Sanhita, 2023 ("BNSS") and the BSA is arguably the most sweeping rewrite of the country's criminal law since 1947.[4] All three came into force on 1 July 2024, replacing respectively the Indian Penal Code, 1860, the Code of Criminal Procedure, 1973, and the Indian Evidence Act, 1872. Of the three, the BSA presents itself as an evidence code built for the digital era, with electronic records and digital material given far more room than before. Even so, this paper argues that when it comes to evidence *generated* rather than merely *stored* by machines, the statute falls dangerously short.

The remainder of the paper is organised as follows. Part II maps the technology behind AI-

[3] Maura R. Grossman & Paul W. Grimm, 'Judicial Approaches to Acknowledged and Unacknowledged AI-Generated Evidence,' (2025) 26(2) Science and Technology Law Review, Columbia University.

[4] The Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023); the Bharatiya Nagarik Suraksha Sanhita, 2023 (Act 46 of 2023); the Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023); all brought into force from 1 July 2024 vide Gazette of India, Extraordinary, Part II, Section 3(ii).

generated evidence and proposes a working taxonomy. Part III sets out how the BSA currently treats electronic evidence. Part IV works through five specific statutory gaps. Part V compares the Indian position with approaches taken in the United States, the European Union and the United Kingdom. Part VI considers the constitutional stakes. Part VII sets out a reform proposal, and Part VIII concludes.

II. MAPPING THE TECHNOLOGY: WHAT COUNTS AS AI-GENERATED EVIDENCE

2.1 What Generative AI Actually Does

Generative Artificial Intelligence is best understood as a family of machine-learning models trained on enormous datasets so that they can produce fresh content statistically consistent with whatever patterns they absorbed during training. This marks a sharp departure from ordinary software, which merely executes fixed instructions; a generative model instead learns an underlying probability distribution and then samples new, previously non-existent outputs from it. The technologies most relevant to evidentiary disputes are Generative Adversarial Networks ("GANs"), diffusion models, Large Language Models ("LLMs"), and neural voice-synthesis engines.[5]

A GAN, an architecture Ian Goodfellow introduced in 2014, pits two neural networks against one another: a generator that manufactures synthetic content and a discriminator that tries to unmask it as fake.[6] Repeated rounds of this contest push the generator toward output a face, a voice, a video clip that the discriminator (and, eventually, a human observer) can no longer flag as artificial.

Large Language Models such as GPT-4 and Claude can now draft synthetic letters, confessions, contracts or medical notes so fluently that conventional forensic document examination may simply fail to catch them. Diffusion models, for their part, generate still images and audio that forensic practitioners have started calling "superhuman" in their realism.

2.2 Four Categories of AI-Generated Evidence Relevant to Criminal Trials

For the purposes of legal analysis, this paper sorts AI-generated evidence in criminal

[5] Ian Goodfellow et al., 'Generative Adversarial Networks,' (2014) arXiv:1406.2661.
[6] Ibid.

proceedings into four broad classes.

First, audiovisual deepfakes video, still imagery, or audio that has been either wholly synthesised or manipulated by AI tools. Typical instances include a fabricated video appearing to show a defendant committing an offence, a cloned voice recording that sounds like a confession, or surveillance footage in which a face has been digitally swapped.

Second, fabricated documentary material financial records, medical files, correspondence or contracts produced by LLMs or comparable systems. This category is especially dangerous in forgery, fraud and white-collar prosecutions, where the paper trail often carries the case.

Third, algorithmic profiling output the results of predictive-policing tools, risk-scoring systems (COMPAS being the best-known US example) and facial recognition platforms. When such outputs are treated in court as proof of likely guilt or dangerousness, they raise serious concerns about hidden bias and the accused's ability to interrogate an opaque process.[7]

Fourth, AI-enhanced evidentiary material evidence that began as genuine but was subsequently run through an AI pipeline, such as upscaled surveillance video, audio reconstructed from a degraded recording, or AI-assisted DNA interpretation. Here the underlying evidence is real, but its final form has been shaped by an algorithm.

2.3 The "Liar's Dividend" and Its Threat to Evidentiary Trust

Legal scholars Bobby Chesney and Danielle Keats Citron gave a name to a curious side-effect of widespread deepfake technology: as convincing fakes become more common, it becomes correspondingly easier for a litigant to dismiss *genuine* evidence as fabricated. Chesney and Citron called this the "liar's dividend."[8] The result is a double bind courts risk being fooled by fake evidence on one hand, while authentic evidence risks being wrongly discredited on the other.

For India, where both wrongful convictions and wrongful acquittals carry heavy social costs, the liar's dividend is a particularly serious hazard. An accused caught on genuine CCTV footage might successfully claim the recording is synthetic; conversely, an investigating agency willing

[7] Julia Angwin et al., 'Machine Bias,' ProPublica (23 May 2016); see also State v. Loomis, 881 N.W.2d 749 (Wis. 2016), on judicial treatment of AI risk-assessment tools at sentencing.
[8] Bobby Chesney & Danielle Keats Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107 California Law Review 1753.

to fabricate evidence could use AI tools to build a case against an innocent person. Neither scenario is acceptable, and both point to the same underlying vulnerability.

III. THE BSA'S ELECTRONIC EVIDENCE FRAMEWORK, EXAMINED

3.1 Origins and Stated Purpose

The BSA emerged as one strand of the Union Government's broader rewrite of India's criminal law under the Modi administration. All three reform bills were tabled in the Lok Sabha on 11 August 2023 by the Union Home Minister, framed as an exercise in removing colonial-era language and aligning criminal law with present-day needs.[9] The BSA received Presidential assent on 25 December 2023 and took effect on 1 July 2024.

The Parliamentary Standing Committee on Home Affairs, which examined the three bills and reported in November 2023, acknowledged the need to bring the evidence framework up to date with digital realities but its report is silent on AI-generated evidence or deepfakes specifically, an omission this paper treats as significant rather than incidental.

3.2 A Wider Definition of "Electronic Record"

Compared with its predecessor, the BSA casts a noticeably wider net around "electronic records." The 1872 Act had simply borrowed its definition from Section 2(t) of the Information Technology Act, 2000. The BSA instead builds its own definition: Section 2(1)(e) defines "document" broadly as any matter recorded on any substance through letters, figures, marks or any combination of these, and folds electronic and digital records squarely into that definition.[10]

Section 57 goes further, extending oral evidence to cover statements recorded through video-conferencing or other audio-visual electronic means, while Sections 265, 266 and 308 of the BNSS allow witnesses to be examined remotely through similar technology.[11]

3.3 Sections 62 and 63: The Backbone of Electronic Admissibility

Sections 62 and 63 do the heavy lifting in the BSA's treatment of electronic evidence. Section

[9] Statement of Objects and Reasons, Bharatiya Sakshya Bill, 2023, as introduced in the Lok Sabha on 11 August 2023.
[10] Section 2(1)(e), Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023).
[11] Sections 265, 266 and 308, Bharatiya Nagarik Suraksha Sanhita, 2023 (Act 46 of 2023).

62 states that the contents of an electronic record may be proved as Section 63 prescribes. Section 63 itself closely tracks the old Section 65B of the 1872 Act as construed by the Supreme Court in *Anvar P.V. v. P.K. Basheer*[12] and later *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*[13] and lays down the conditions an electronic record must satisfy to be admitted.

Under Section 63(4), a certificate must accompany the record, furnished either by a person holding a "responsible official position" with respect to the relevant device, or by an expert. The BSA's innovation is to split this certificate into two parts Part A, completed by the person responsible for the device, and Part B, completed by an expert a structural refinement absent from the earlier statute.

3.4 Section 45: Expert Opinion, and Its Silence on AI

Section 45 allows expert opinion on matters of foreign law, science, art, handwriting and fingerprint identification. Notably absent, however, is any distinct evidentiary category for "digital forensics expert" or "AI forensics expert." One could argue that the general "science or art" language of Section 45 stretches far enough to cover AI forensic analysis, but the provision sets out no qualification criteria, no certification pathway, and no admissibility threshold tailored to that kind of expertise a gap this paper treats as consequential.

3.5 What the Statute Leaves Unsaid

A close reading of the BSA shows it contains nothing that: (i) defines AI-generated or synthetically produced evidence as such; (ii) sets out authentication requirements specific to deepfakes or synthetic media; (iii) allocates the burden of proof when a party alleges that evidence is AI-generated; (iv) obliges a party relying on AI-processed evidence to disclose that fact; (v) sets qualification standards for anyone offering AI forensic opinions; (vi) speaks to chain-of-custody where an AI system has touched the evidence; or (vii) establishes any body a National AI Forensics Authority, for instance to oversee AI evidence in criminal cases.[14]

[12] *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473 (Supreme Court of India).
[13] *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1 (Supreme Court of India).
[14] See generally, *Electronic Evidence under Bhartiya Sakshya Adhiniyam, 2023*, Drishti Judiciary, July 2024; ELP Law, 'Bhartiya Sakshya Adhiniyam, 2023 A Dynamic Shift to the Digital Era' (July 2024).

IV. FIVE STATUTORY GAPS: A CLOSER LOOK

4.1 Gap One No Definition at All

The most basic problem with the BSA is that it never defines, or even names, "AI-generated evidence," "synthetic media," "deepfake," "generative AI output," or anything resembling these concepts. Its definition of "electronic record" is deliberately technology-neutral, sweeping in any data stored or transmitted electronically. Neutrality of this kind is usually a virtue it keeps a statute from going stale as technology moves on but AI-generated evidence poses a qualitatively different problem that neutral drafting cannot solve on its own.

An ordinary electronic record has a traceable origin: a human being made it with a device, and the live question is usually whether it was altered afterward. AI-generated material often has no human author whatsoever its "origin" is an algorithm, and the real question shifts from "has this been tampered with?" to "was this ever a record of anything real?" A framework built around the first question cannot simply be repurposed for the second.[15]

The practical fallout is immediate. When a party claims that a piece of evidence is AI-generated, judges have no statutory compass to guide classification, procedure, or evidentiary weight. Left to improvise, different courts will inevitably reach different, sometimes contradictory, results precisely the kind of unpredictability the rule of law is meant to prevent.

4.2 Gap Two A Certification Regime Built for the Wrong Problem

Section 63's certificate mechanism assumes a world where a human operator uses a device to create a record, and the only live question is whether that record faithfully reflects what the device produced. Part A confirms the device was working properly and that the record arose in the ordinary course of business; Part B supplies expert technical corroboration.

That model breaks down for AI-generated evidence in at least three ways. First, a deepfake video can sail through certification as a technically "proper" electronic record properly stored, properly time-stamped, produced by a functioning device even though everything it depicts is invented. The certificate vouches for the container, not the contents.[16] Second, AI-generated

[15] cf. Rebecca Delfino, 'Deepfakes on Trial 2.0: A Revised Proposal for a New Federal Rule of Evidence to Mitigate Deepfake Deceptions in Court,' Loyola Law School Research Paper No. 2025-10, SSRN No. 5188767 (February 2025).

[16] National Center for State Courts, 'AI-Generated Evidence is a Threat to Public Trust in the Courts' (February

material typically has no "responsible official" in any conventional sense, since its author is an algorithm rather than a person leaving open the question of who, exactly, signs Part A for a machine-generated video. Third, the Part B expert is asked to certify that a device functioned correctly, which is a completely different skill from detecting synthetic-media artefacts, timing anomalies, GAN-specific fingerprints, or other tell-tale signs of algorithmic generation.

The Supreme Court's strict reading of the old Section 65B in *Anvar P.V.* and *Khotkar*, if applied without modification to AI-generated content, would produce one of two bad outcomes: either a well-certified deepfake gets treated as authentic, or genuinely AI-processed (but legitimate) evidence is thrown out on a technicality. Justice is not served either way.

4.3 Gap Three Who Carries the Burden When "Deepfake" Is the Defence?

Once a party in a criminal case asserts that digital evidence is AI-generated, the question of who bears the burden of proof becomes pressing. Under the BSA as it stands, a party seeking to challenge an electronic record must overcome a presumption of authenticity a demanding standard, and one that an accused person of limited means may struggle to meet without expensive expert analysis.

The US Federal Advisory Committee on Evidence Rules has been grappling with the identical issue while developing proposed Federal Rule of Evidence 901(c).[17] Under the November 2024 draft, a party disputing evidence would first need to show that "a jury could reasonably find" the material was AI-altered; only then would the burden shift to the proponent to show that probative value outweighs the risk of prejudice.

Nothing comparable exists in the BSA. That absence produces two mirror-image injustices. Accused persons especially those without financial resources are left exposed when genuine evidence is used against them, because they cannot afford independent AI forensic verification. At the same time, a well-resourced litigant can weaponise the "deepfake defence" purely as a tactic, exploiting judicial uncertainty about what AI can and cannot do.

2026), available at ncsc.org.

[17] US Advisory Committee on Evidence Rules, Agenda Book, 2 May 2025 Meeting, US Courts (May 2025); see also US Judicial Panel, Proposed FRE Rule 901(c) (November 2024).

4.4 Gap Four Custody Rules That Do Not Contemplate an AI "Black Box"

Chain-of-custody doctrine grew out of concerns about physical evidence the risk that an object might be tampered with, contaminated or swapped between seizure and trial. Digital evidence extended the same logic through access logs and hash-based integrity checks.

AI-processed evidence poses an entirely different custody problem. When an AI system sharpens a blurry surveillance clip, interprets DNA data, or transcribes garbled audio, the transformation happens inside a system whose internal logic is opaque often even to the people who built it. What comes out the other end is not simply a copy of the input; it has been reshaped by a process that cannot always be traced step by step or fully explained.[18]

The BSA imposes no obligation on a party tendering AI-processed evidence to disclose which system was used, which version, what data trained it, its error rate for the relevant task, any known biases, or whether its output has been independently validated. Without such disclosure duties, AI-processed evidence quietly enjoys a presumption of reliability it has not actually earned.

4.5 Gap Five No Baseline Competency for the People Who Must Judge This Evidence

The final, and arguably most far-reaching, gap is institutional: nothing in the BSA (or in any adjacent statute) ensures that judges, prosecutors or defence lawyers possess even a minimal technical grounding in AI-generated or AI-processed evidence. A judge unable to distinguish a GAN from a routine video edit cannot meaningfully rule on admissibility. A prosecutor unfamiliar with the training-data limits of a facial-recognition tool cannot present that evidence responsibly. A defence lawyer who cannot spot deepfake artefacts cannot challenge fabricated material effectively.

Neither the Bangalore Principles of Judicial Conduct nor the training curriculum run by the National Judicial Academy currently mandates instruction in AI forensics or AI evidence evaluation. The BSA imposes no training requirement, sets no competency benchmark for experts offering AI forensic testimony, and creates no accreditation scheme for AI forensics

[18] Illinois State Bar Association, 'Deepfakes in the Courtroom: Problems and Solutions' (March 2025) (citing Linna et al., observing that detection technologies for AI-generated content remain unreliable and prone to bias).

laboratories.[19]

V. LOOKING ABROAD: THE US, EU AND UK APPROACHES

5.1 United States Proposed Federal Rule of Evidence 707

The United States has moved furthest in confronting AI-generated evidence directly. On 10 June 2025, the Committee on Rules of Practice and Procedure which advises the Judicial Conference of the United States approved a proposed Federal Rule of Evidence 707 aimed squarely at AI-generated and AI-manipulated digital evidence.[20]

Proposed Rule 707 borrows the reliability-gatekeeping logic of *Daubert v. Merrell Dow Pharmaceuticals, Inc.*[21], ordinarily reserved for expert testimony, and applies it to machine-generated evidence. It asks courts to weigh the reliability of the underlying methodology, whether the technique has been peer-reviewed and published, its known or likely error rate, and how widely it is accepted within the relevant scientific community. In effect, this treats AI-generated evidence not as just another electronic record awaiting authentication but as a distinct category of scientific evidence requiring its own admissibility gate.

A parallel proposal, FRE Rule 901(c), tackles the deepfake-defence problem directly: once an opposing party shows that a reasonable jury could find the evidence was AI-altered, admissibility turns on whether the proponent can show that probative value outweighs prejudicial risk.[22] This burden-shifting device avoids the two extremes of excluding every challenged item or admitting every claimed deepfake.

California's Judicial Council AI Task Force has added further guidance at state level, with legislation passed in 2025 directing the Judicial Council to assess AI's impact on the introduction of evidence and to produce supporting rules by 1 January 2026.[23]

---

[19] National Judicial Academy, Annual Report 2023–24; see also Judiciary Committee, Report on Digital Evidence Training, Government of India (2023).
[20] Committee on Rules of Practice and Procedure, Judicial Conference of the United States, Proposed Federal Rule of Evidence 707 (approved 10 June 2025); see also JDSupra, 'Safeguarding the Courtroom from AI-Generated Evidence: Federal Rule of Evidence 707 Approved by Judicial Conference' (June 2025).
[21] *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 US 579 (1993).
[22] University of Baltimore Law Review, 'Deepfakes in the Courtroom: Challenges in Authenticating Evidence and Jury Evaluation' (December 2025).
[23] California Legislative Assembly, Bill [Year], directing Judicial Council review of AI evidence by 1 January 2026; cited in Illinois State Bar Association, supra n. 16.

5.2 European Union The AI Act and GDPR

The EU's Artificial Intelligence Act, in force since 2 August 2024 and due for full application by August 2026, is the first comprehensive AI-regulation statute anywhere in the world.[24] It is not an evidence code, but its reach into criminal proceedings is substantial.

The Act sorts AI systems by risk tier. Biometric identification tools, including facial recognition, sit in the "high-risk" category and must satisfy conformity assessments, maintain technical documentation, meet transparency obligations, and register in an EU-wide database. Tools that generate deepfakes carry their own transparency duty users must be told when they are looking at AI-generated content. Together these obligations build an evidentiary infrastructure India currently has no equivalent of.

The GDPR supplies additional procedural safeguards relevant here: Article 22 gives individuals a right not to be subject to decisions based solely on automated processing, a right that has been read to cover AI-driven risk assessments in criminal matters, while Article 15 gives affected parties a right of access to understand systems whose output is used against them.[25]

The European Court of Human Rights has also begun to develop Convention-based standards on AI evidence, notably in *Yüksel Yalçınkaya v. Turkey* (2023), where the Court scrutinised the fairness of proceedings that relied heavily on AI-based analysis of encrypted messaging data.[26]

5.3 United Kingdom The Forensic Science Regulator Act, 2021

The UK took a different, more institutional route through the Forensic Science Regulator Act, 2021, which gave the Forensic Science Regulator statutory power to set binding codes of practice for forensic work used in criminal proceedings.[27] Under this authority, the Regulator has issued guidance requiring that AI tools used forensically be validated for their specific purpose, that their known error rates be disclosed, that their methodology be open to peer

[24] 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), OJ L, 2024/1689.
[25] Regulation (EU) 2016/679 (General Data Protection Regulation), Articles 15 and 22.
[26] *Yüksel Yalçınkaya v. Turkey*, Application No. 15669/20 (European Court of Human Rights, Grand Chamber, 2023).
[27] Forensic Science Regulator Act 2021 (UK), c. 14.

review, and that experts presenting AI forensic output meet defined qualification standards.

The UK Law Commission's earlier consultation on hearsay and related topics in criminal proceedings, though written before the modern GenAI era, still offers a useful conceptual distinction between "computer-generated evidence" (which needs no human author) and "computer-stored evidence" (which simply records something a human said) a distinction Indian courts could usefully borrow.[28]

5.4 What the Comparison Suggests

Across all three jurisdictions, effective regulation of AI-generated evidence tends to rest on three pillars: a definitional pillar that classifies AI-generated evidence and calibrates treatment to risk; an authentication pillar that raises the admissibility bar in proportion to how synthetic the evidence is; and an institutional pillar that builds dedicated forensic bodies, expert-certification schemes and judicial training. The BSA, on the evidence examined above, has none of the three.

VI. CONSTITUTIONAL STAKES: FUNDAMENTAL RIGHTS AND AI EVIDENCE

6.1 Article 21 and the Fair-Trial Guarantee

The right to a fair trial sits at the core of the right to life and personal liberty under Article 21 of the Constitution.[29] The Supreme Court has repeatedly held that this right includes the ability to challenge evidence, to know the substance of the case against oneself, and to insist that evidence be properly authenticated before it is used to convict.[30]

AI-generated evidence tests this guarantee from both directions. Fabricated deepfakes tendered by the prosecution threaten wrongful conviction; genuine electronic evidence wrongly dismissed as a deepfake threatens wrongful acquittal or a failure to hold the guilty accountable. A conviction resting on fabricated AI evidence is a straightforward deprivation of liberty under Article 21. Equally, a court that fails to properly scrutinise AI-generated exculpatory material

[28] UK Law Commission, *Evidence in Criminal Proceedings: Hearsay and Related Topics*, Consultation Paper No. 138 (1995); see also *R v. Skinner* [1994] 99 Cr App R 212, on computer-generated evidence.
[29] *Hussainara Khatoon v. State of Bihar*, (1980) 1 SCC 81; *Zahira Habibullah Sheikh v. State of Gujarat*, (2004) 4 SCC 158.
[30] *Manoharlal Sharma v. Union of India*, (2014) 6 SCC 1; *Vineet Narain v. Union of India*, (1998) 1 SCC 226.

falls short of its constitutional obligations.

The Supreme Court's holding in *Maneka Gandhi v. Union of India*[31] that any procedure depriving a person of liberty must be "just, fair and reasonable" supports the argument that a statutory framework offering no real mechanism for authenticating AI-generated evidence may itself be constitutionally suspect.

6.2 Article 20(3) and the Privilege Against Self-Incrimination

Article 20(3) shields an accused from being compelled to testify against himself. In *Selvi v. State of Karnataka*[32], the Supreme Court extended that protection to narco-analysis, brain mapping and polygraph tests, holding that compelled extraction of testimonial material breaches Article 20(3) even where the accused is not, in a formal sense, "testifying."

AI-generated evidence adds new wrinkles to this doctrine. Facial recognition can identify a person from images gathered publicly or without consent; voice-recognition tools can identify a speaker from communications metadata; predictive-policing systems generate "risk profiles" that function, in substance, as accusations built entirely from an individual's data trail. Where such outputs are used evidentially, it becomes fair to ask whether the accused has, in effect, been forced to "testify" through the involuntary surrender of biometric and behavioural data to an algorithm.[33]

6.3 Article 14 and Algorithmic Bias

Article 14 guarantees equality before the law. Facial-recognition and predictive-policing tools have been well documented to produce uneven error rates across racial, ethnic and gender lines.[34] A system that misidentifies people from a particular community more often than others will, if relied on as evidence, systematically generate more false accusations against that community a differential impact that squarely implicates Article 14.

The proportionality framework the Supreme Court set out in *K.S. Puttaswamy v. Union of*

[31] *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248.
[32] *Selvi v. State of Karnataka*, (2010) 7 SCC 263.
[33] Arindrajit Basu & Elonnai Hickok, 'The Personalised Data Diet,' Internet Freedom Foundation (2020); see also *K.S. Puttaswamy (Privacy-9J) v. Union of India*, (2017) 10 SCC 1, on informational privacy.
[34] Joy Buolamwini & Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' (2018) 81 Proceedings of ML Research 1.

India[35] in the privacy context would similarly demand that biased AI evidence systems be tested against the legitimate aim they serve, with less discriminatory alternatives considered before their use is permitted.

6.4 Article 19(1)(a) and the Deepfake Problem

Deepfake technology threatens freedom of speech and expression under Article 19(1)(a) from two directions at once. It can be used to put fabricated statements in the mouths of real people politicians, journalists, activists corroding the shared factual ground that meaningful public debate depends on. At the same time, its mere existence gives people who *did* make genuine statements a plausible way to deny them, further eroding public trust in what is real.

Any legislation targeting deepfakes must therefore balance the legitimate aim of curbing deceptive synthetic media against the expressive rights of those creating such content for art, satire or research. India's law currently offers no such balance a gap in the fundamental-rights architecture, not merely in evidence law.

VII. A PATH TO REFORM: LEGISLATIVE AND INSTITUTIONAL PROPOSALS

7.1 Guiding Philosophy: A Calibrated Admissibility Model

This paper proposes a "Calibrated Admissibility Model" (CAM) as the organising principle for regulating AI-generated evidence in Indian criminal courts. Three ideas anchor the CAM: first, technological differentiation AI-generated evidence should be treated as its own category rather than folded into ordinary electronic evidence; second, proportionate scrutiny admissibility thresholds should scale with the risk posed by the AI system and the degree to which the evidence is synthetic; and third, structural equity the framework must not leave accused persons worse off simply because they cannot afford AI forensic expertise.

7.2 A Proposed Schedule V-A to the BSA

This paper proposes inserting a new Schedule V-A into the BSA, titled "Provisions Relating to AI-Generated and AI-Processed Evidence in Criminal Proceedings," containing the following clauses.

[35] *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1; (2019) 1 SCC 1 (Aadhaar).

Clause 1 Definitions. "AI-generated evidence" means any audio, visual, audio-visual, textual or documentary material created, wholly or substantially, by an artificial intelligence system including generative adversarial networks, diffusion models, large language models and neural voice-synthesis systems without direct human authorship. "AI-processed evidence" means genuine evidence that has undergone algorithmic transformation, enhancement or analysis. "Deepfake" means AI-generated or AI-manipulated audio-visual content that falsely depicts a real person doing or saying something, or being somewhere they were not. "Synthetic document" means any document generated, wholly or substantially, by an LLM or comparable generative system.

Clause 2 Admissibility Standard. AI-generated evidence should be inadmissible in criminal proceedings unless the party relying on it can show, by clear and convincing evidence, that: (a) the AI system used has been validated for the specific task at hand; (b) its known error rate does not render the output unreliable; (c) its methodology is capable of, and has undergone, independent peer review; and (d) it does not display differential error rates on the basis of race, religion, caste, ethnicity or gender that would make its output discriminatory. Courts should treat this as a preliminary admissibility question, analogous to the framework under Section 136 of the BSA.

Clause 3 Challenge Mechanism. When a party challenges electronic evidence as possibly AI-generated or AI-manipulated, the court should: (a) on a prima facie showing of possible synthetic origin, order forensic examination by an accredited AI forensics laboratory; (b) assign reduced probative weight to the disputed evidence while that examination is pending; and (c) exclude the evidence, and consider adverse inference against the party who introduced it, if the examination confirms synthetic or manipulated origin.

Clause 4 Chain of Custody for AI Systems. A party tendering AI-processed evidence should be required to disclose: (a) the identity and version of the AI system used; (b) the training data underlying it, to the extent feasible; (c) its error rate and the confidence level attached to the specific output; (d) any known biases; and (e) any independent validation reports available. Failure to disclose should render the evidence inadmissible.

Clause 5 Accreditation of AI Forensics Laboratories. Within one year of this Schedule coming into force, the Central Government should establish, by notification, a National AI Forensics Authority ("NAIFA") under the Ministry of Home Affairs, tasked with: (a)

accrediting laboratories that carry out AI evidence forensic analysis; (b) setting and maintaining methodological standards; (c) maintaining a registry of AI systems used in criminal investigations; and (d) running training programmes for judges, prosecutors and defence counsel.

7.3 A Complementary Amendment to the BNS, 2023

This paper also proposes a new provision in the BNS, 2023 that specifically criminalises knowingly introducing fabricated AI-generated evidence in judicial proceedings. The existing false-evidence provision (Section 229, BNS) covers false statements made in the course of proceedings but does not squarely address the tendering of synthetically fabricated media a gap a dedicated provision would close.

The proposed text: "Whoever knowingly introduces AI-generated or AI-manipulated material as evidence in judicial proceedings, purporting it to be authentic, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine." Limiting liability to knowing conduct ensures that a party who unwittingly tenders material later found to be AI-generated is not swept up in criminal liability.[36]

7.4 Mandatory Training Through the National Judicial Academy

The paper further proposes that the National Judicial Academy and its state-level counterparts be directed whether through a Supreme Court direction under Article 142 or a legislative amendment to the BNSS to build mandatory AI-evidence modules into every induction and refresher programme for judicial officers. Such training should cover the fundamentals of generative AI, forensic indicators of synthetic content, the limits and error rates of AI forensic tools, the constitutional dimensions discussed in Part VI, and the proposed Schedule V-A framework itself.

7.5 An Interim Role for the Supreme Court

Pending legislative reform, this paper argues that the Supreme Court has both the power and the responsibility to issue Practice Directions on AI-generated evidence under its plenary authority in Article 142. The Court has stepped into comparable legislative vacuums before most famously on workplace sexual harassment in *Vishaka v. State of Rajasthan*[37] and in

[36] cf. Section 229, Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023) (False Evidence).
[37] *Vishaka v. State of Rajasthan*, (1997) 6 SCC 241 (Supreme Court practice directions in the absence of

juvenile justice matters. A Practice Direction on AI evidence could put interim protocols in place for authentication, challenge procedures and forensic examination while Parliament works toward the fuller reform proposed here.

VIII. CONCLUSION

India's criminal justice system stands at an inflection point. The Bharatiya Sakshya Adhiniyam, 2023 is, in real terms, a historic modernisation of the country's evidence law but it is a modernisation that stops just short of the single most transformative technology of the current moment. The five gaps traced in this paper the absence of any definition, a certification regime unfit for synthetic content, the liar's-dividend problem, the missing chain-of-custody framework, and the lack of institutional competency together add up to a structural vulnerability that will only deepen as generative AI tools become cheaper, better and more widely available.

The costs of doing nothing cut both ways. Fabricated AI evidence, whether introduced by careless investigators or determined bad actors, can put innocent people behind bars. Genuine evidence, meanwhile, can be knocked out through a well-timed deepfake defence, letting guilty parties walk free. Neither outcome is compatible with the basic promise the justice system is supposed to keep.

The comparative record from the United States, the European Union and the United Kingdom points to a common lesson: durable regulation of AI-generated evidence needs definitional clarity, admissibility standards calibrated to risk, and real institutional capacity. India's proposed Schedule V-A, paired with the BNS amendment and mandatory judicial training set out above, offers exactly that combination. What remains is whether the legislature, the judiciary and the executive choose to move with the urgency the moment calls for.

In an age where reality itself can be synthesised on demand, the fairness of a criminal trial depends not only on whether witnesses tell the truth but on whether the evidence itself can be trusted at all. Once that trust becomes uncertain, the adversarial system's basic promise a just outcome reached through tested evidence starts to look shaky. The reforms proposed here are not a minor technical fix to evidence law; they are close to a constitutional necessity.

legislation).