AI AND THE BHARATIYA SAKSHYA ADHINIYAM 2023: A CRITICAL APPRAISAL

Aryan Leander Wishard[*] & Ashita Khonde[**]

ABSTRACT

The emerging technology of artificial intelligence is getting accurate on each successive day, intersecting the legal backdrop it heightens the cyber-crimes around the world along with posing risks and harms to investigate and admit the specific piece of evidence in the court, indirectly proving the criminal justice system weak and underdeveloped in the context of high-paced self-learning automations and designs. To resolve these particular challenges posed by AI and synthetic deepfake outputs, necessary amendments are made under the Indian criminal justice system like the addition and acceptance of digital and electronic records as a primary piece of evidence under the Bharatiya Sakshya Adhiniyam, 2023[1]; along with this, the global trends include the laws governing data privacy and AI are also getting polished consistently across jurisdictions. The objective of this paper is to critically identify, examine and analyse such challenges posed by AI and provide a clear perspective on how other foreign jurisdictions are dealing with the same. This paper critically examines the growing interface between Artificial Intelligence (AI) and the Bharatiya Sakshya Adhiniyam, 2023, with a focus on the evidentiary treatment of digital and algorithmically generated material. Drawing from legal analysis, trends in landmark precedents along with international jurisprudential development on misuse of AI, we can spot key weaknesses in BSA statutory framework. The paper discusses about the adequacy of the Indian evidence laws in the context of persistently trailblazing automations and algorithms, extracting out the associated risks and harms, and offers a cross jurisdictional comparative picture on governance of Artificial Intelligence and data risks in the European Union and the United States for a broader perspective.

Keywords: Artificial Intelligence, Reliability, Evidence, Deepfakes and Synthetic Media, Digital Evidence.

[*] PhD candidate, Renaissance University, Indore, Madhya Pradesh,
[**] Student, School of Law, Devi Ahilya Vishwavidyalaya, Indore, Madhya Pradesh,
[1] Bharatiya Sakshya Adhiniyam, 2023, § 62, No. 47, Acts of Parliament, 2023 (India).

1. INTRODUCTION

Artificial Intelligence, commonly known as AI, has touched every aspect of human life in the 21st century. It is being developed as the next big thing for betterment and advancement of mankind, its impact has far reaching implications even during the present nascent stage of AI. The use of artificial intelligence in various fields is persistently increasing due to its ever evolving, dynamic and active learning nature which in most aspects provide better data synthesis and outputs than human intelligence. In the legal field where consistent scholarship is necessary for expertise and application, AI provides better outputs using features like Predictive coding, Generative AI, XAI (explainable AI), Continuous Active learning models and its integration with blockchain technology. The Indian judicial system, operating under heavy infrastructure constraints, where technology and technical know-how is scarce, presents significant challenges as well with respect to the usage of AI, such as the black-box nature of AI, inconsistency in chain of custody, biasness in responses and most importantly judicial literacy.[2]

The concept of trial in courtrooms depends upon the sanctity of appreciation of evidence, its admissibility and evidentiary value. The Bharatiya Sakshya Adhiniyam 2023 repealed the Indian Evidence Act of 1872 and incorporated electronic records as primary evidence[3], which also led to the inception of the challenges in determining the credibility of evidence in the emerging AI era. Even though the rigorous framework of Indian laws dealing with technology and evidence such as the Information Technology Act 2000[4], The Digital Personal Data Protection Act 2023[5], and the major criminal statutes provides foundational provisions for digital and electronic evidence, yet it does not comprehensively address challenges unique to AI mentioned above, to which the courts may increasingly face evidence that is firstly – AI generated rather than drafted by humans, secondly – AI processed documents rather than raw records, and thirdly – AI interpreted rather than directly perceptible. The lack of explicit standards and provisions to regulate AI conceived risks potentially leads to the problems like increased wrongful attributions and erosion of evidentiary reliability, which proposes the

[2] Trishita Chatterjee*, Admissibility of Ai-Reviewed Digital Evidence in Legal Investigations,* V, IJIRL, 2056, 2060-2062, (2025).
[3] Tanmay Pradeep, *Comparison Analysis between the Indian Evidence Act, 1872 and the Bharatiya Sakshya Adhiniyam, 2023,* Volume 16, Issue 1, IJSAT, 1, 1-3 (2025).
[4] Information Technology Act, 2000,§ 1, No. 21, Acts of Parliament, 2000 (India).
[5] Digital Personal Data Protection Act, 2023, § 1, No. 23, Acts of Parliament, 2023 (India).

following research questions for this study:

1.1. RESEARCH QUESTIONS

1. Whether the existing provisions with respect to electronic and digital records are adequate enough to deal with the problems and challenges incepted by the use of AI in the Indian criminal justice system?

2. How artificial system outputs such as deepfakes and synthetic media introduces principal evidentiary risks in assessing the court records?

3. What comparative benchmarks can be indoctrinated from developed jurisdictions to the Indian framework?

1.2. RESEARCH OBJECTIVES

1. To critically examine the adequacy of the existing provisions of the Bharatiya Sakshya Adhiniyam 2023, concerned with electronic and digital records in addressing AI-driven challenges with the Indian criminal justice system?

2. To identify and analyze the principal evidentiary risks posed by AI-generated outputs, including deepfakes and other forms of synthetic media, in assessment and admissibility along with probative value of court records under the Bharatiya Sakshya Adhiniyam.

3. To undertake a comparative study of evidentiary approaches to AI-related electronic evidence in selected developed jurisdictions and to derive practical benchmarks that can be adapted or incorporated in the Indian Evidence Law framework under the Bharatiya Sakshya Adhiniyam 2023.

2. LITERATURE REVIEW

Authenticated primary sources used for this study include the statutes, legislations, and landmark judicial decisions of Indian courts along with the government databases and reports; the legislations and statutory references of the United States and European Union are also relied upon for offering a cross jurisdictional comparative perspective. Legal academic scholarship and research papers from law review journal are used including:

- *"From Surveillance to Sentencing: Evaluating AI's Role in Indian Criminal Justice":* This work evaluates AI's expanding use across the criminal justice pipeline in India, weighing gains in investigative efficiency and decision-making against serious concerns over privacy, ethics, and civil liberties.[6]

- *"The Evidentiary Value of AI-Generated Data: A Framework for Reliability and Admissibility":* This study critiques the suitability of traditional rules of evidence for AI-generated data and proposes a normative framework centered on verifiability, transparency, and procedural safeguards to protect accused persons' rights.[7]

- *"AI-Generated Evidence Indian Courts: Admissibility, Reliability, and the Chain of Custody Challenge":* This article argues that India's evidentiary regime must be reformed to properly handle AI-generated proof, emphasizing the need to address reliability, explainability, algorithmic bias, and robust chain-of-custody standards.[8]

- *"Navigating Deepfakes in Indian Criminal Law":* This paper examines how deepfake technologies threaten the integrity of digital evidence and advocates for updated legal and regulatory mechanisms to prevent miscarriages of justice stemming from manipulated media.[9]

- *"Comparative Perspectives on AI and Evidence Law":* This paper uses cross-jurisdictional comparison to show how different countries are updating evidentiary rules for AI-generated evidence and suggests that India should draw on these models to design context-sensitive regulations that promote innovation while preserving core legal safeguards.[10]

2.1. RESEARCH GAP

Since both Artificial Intelligence and The Bharatiya Sakshya Adhiniyam 2023 are recent

[6] Navin Kumar*, From Surveillance to Sentencing: Evaluating AI's Role in Indian Criminal Justice*, 30 SCI. BULL. 68, 68–78 (2025).
[7] Hua Zhang, *The Evidentiary Value of AI-Generated Data: A Framework for Reliability and Admissibility*, 2(2) ESW 34, 34-41 (2025).
[8] Deepanker Singhal & Pragya Narang, *Ai-Generated Evidence in Indian Courts: Admissibility, Reliability and The Chain of Custody Challenge*, Vol. V. Issue. V IJIRL 186, 186-204 (2025) [hereinafter *Deepanker*].
[9] Dr. Deepti Singhla, *Navigating Deepfakes in, Indian Criminal Law*, Vol. V Issue III IJIRL 1943, 1943-1960 (2025) [hereinafter *Deepti S*].
[10] Sukhandeep Kaur et. al., *Hindi audio-video-Deepfake (HAV-DF): A Hindi language-based Audio-video Deepfake Dataset*, arXiv:2411.15457v1 [cs.SD] 1, 1-22 (2024).

developments, the academic work on it is in its infancy. The present paper, being timely and conceptually robust, reveals a significant gap that merits further inquiry. The present paper identifies the fact that deepfakes and synthetic media as core risks to appreciation of evidence in court of law, therefore, the elephant in the room is as follows-

"Existing scholarship focuses on the transition from The Indian Evidence Act, 1872, to The Bharatiya Sakshya Adhiniyam, 2023 as a modernisation of format. However, a critical gap remains that the essence of Bharatiya Sakshya Adhiniyam preserves a 'mechanical view of technology' that is obsolete in the age of generative AI".

This paper bridges the gap by demonstrating how the BSA's certification and authentication frameworks are insufficient for synthetic media, necessitating a new judicial standard for 'Algorithmic Probity'.

3. RESEARCH DESIGN AND METHODOLOGY

This section is constructed and classified in a fourfold manner; initially distinguishing the research methodology adopted for the study, followed by a delineation of the scope, inspection of limitations faced during the study and moreover providing with an articulation of its significance.

3.1. METHODOLOGICAL APPROACH

This research study is conducted by pure doctrinal method, using primary sources of legislation and government databases, along with secondary sources inclusive of academic scholarship, treatises and textbooks. The research design is formulated to include analytical approach to derive the gaps from existing literature, bridge the gap through research questions and, provide conclusion by addressing respective research objectives – to rigorously investigate the convoluted interplay between the emerging tech of AI and the present evidentiary framework established in India, followed by the limited and comparative policy analysis of foreign jurisdictions to identify functional benchmarks, alternative doctrinal formulations and pragmatic judicial responses to similar problems. The methodology looks forward to appraise the technological challenges, ensuring the research to be both grounded in the existing laws and engaged with emerging realities.

3.2. SCOPE

The scope of this research includes a thematic integration of admissibility and evidentiary values of digital and electronic records under the Bharatiya Sakshya Adhiniyam 2023, and artificial system outputs, deepfakes and synthetic media challenges. The scope is limited to the challenges advanced by the use of AI in digital and electronic records; limited comparative and policy analysis of other jurisdictions is also incorporated. However, this paper does not deal with various technicalities of both – the emerging tech, and frameworks of other jurisdictions, and purely focuses on the critical appraisal of emerging challenges in the Indian evidentiary framework.

3.3. LIMITATIONS OF THE STUDY

The present study acknowledges certain limitations which majorly includes the pace of technological advancement in artificial intelligence as it may outpace the timeframe of this legal analysis. Furthermore, the adopted comparative analysis in this study is constrained by the socio-legal jurisdictional structure and respective norms. The study relied on legal analysis supplemented by recognised technical literature instead of testing the intricacies of AI responses in real time.

3.4. SIGNIFICANCE OF THE STUDY

The study is relevant to the academicians, policymakers, legal scholars and researchers as its significance lies in providing a clear structural perception on the substantial reliability and admissibility of AI driven evidence and associated potential risks and harms.

4. THE ADEQUACY OF BHARATIYA SAKSHYA ADHINIYAM (BSA) 2023 IN THE AGE OF GENERATIVE AI

4.1. A 19TH-CENTURY PARADIGM IN A 21ST-CENTURY AI ECOSYSTEM

The Bharatiya Sakshya Adhiniyam, 2023 ("BSA 2023") enacts a comprehensive overhaul of India's evidentiary framework, supplanting the Indian Evidence Act, 1872 with provisions ostensibly calibrated for digital realities.[11] Enacted amid India's trinitarian criminal law

[11] BSA, 2023 § 52.

reforms—alongside the Bharatiya Nyaya Sanhita and Bharatiya Nagarik Suraksha Sanhita—BSA 2023 explicitly recognizes "electronic records" within its definition of documents, elevates them to primary evidence status under specified conditions, and codifies certificate requirements for admissibility.[12] Legislative materials emphasize "technology-neutrality" and "future-proofing," responding to decades of judicial evolution from *Anvar P.V. v. P.K. Basheer (2014) to Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020)*.[13]

Yet, this modernization coincides with the explosive proliferation of generative artificial intelligence (GenAI)—multimodal systems like OpenAI's GPT-4o, Google's Veo, and Stability AI's Stable Video Diffusion that synthesize text, images, audio, and video from probabilistic latent spaces, often indistinguishable from human-authored content.[14] GenAI's evidentiary disruption is existential: it manufactures "synthetic originals" devoid of real-world referents, eroding the perceptual reliability presupposed by evidentiary law.[15] Danielle Citron and Robert Chesney's seminal framework identifies the "liar's dividend"—fabricated evidence poisons wells of truth, while genuine evidence is dismissed as deepfake.[16] This Part conducts a granular doctrinal audit of BSA 2023's adequacy across conceptual, procedural, and institutional dimensions, testing its provisions against GenAI fact patterns and proposing targeted reforms.

4.2. BSA 2023'S ELECTRONIC EVIDENCE ARCHITECTURE: DOCTRINAL FOUNDATIONS

*A. Definitional Expansion: "Document" and "Electronic Record"***:** BSA Section 2(1)(d) defines "document" expansively to subsume "electronic and digital records," aligning with Information Technology Act, 2000 definitions while obviating amendment dependency.[17] Section 2(1)(e) clarifies "electronic record" as data generated, received, or stored by computer, network, or device—capturing GenAI outputs as admissible artifacts.[18] This resolves pre-BSA

[12] *Id.* § 2(1)(d), 61-63; Statement of Objects and Reasons, The Bharatiya Sakshya (Second) Bill, 2023, Bill No. 130 of 2023, Lok Sabha (India).
[13] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473; Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.
[14]Google DeepMind, Veo: A New Frontier in Video Generation (2024), https://deepmind.google/technologies/veo.
[15] Hany Farid, *Seeing Is No Longer Believing: Detecting Deepfakes*, 372 Science 1396 (2021).
[16] Danille Keats Citron & Robert Chesney, *Deep Fakes: A Looming Challenge for Privacy, Democracy and National Security*, 107 CALIF. L. REV. 1753, 1757-60 (2019).
[17] BSA, 2023 § 2(1)(d); IT Act, 2000, § 2(1)(t).
[18] *Id.*

ambiguities where courts strained Evidence Act language for digital nativity.[19]

*B. Primary Evidence Status***:** Sections 61–63: Section 61 revolutionizes admissibility by deeming electronic records "produced from proper custody" as primary evidence, abrogating *Anvar*'s secondary-evidence presumption for printouts.[20] Section 62 reinforces this for standalone devices; Section 63 mandates certificates attesting device functionality, production process, and integrity (hash values, chain-of-custody).[21] Section 63A integrates digital signatures under IT Act Section 3A, enabling PKI-verified provenance for transmissions.[22] Parliamentary debates hailed this as streamlining e-evidence without compromising reliability.[23]

C. Admissibility Gatekeepers: Judicial Notice and Expert Evidence: Section 57 (facts of which judicial notice must be taken) retains admissibility for public documents and scientific facts but omits GenAI benchmarks (e.g., NIST detection error rates).[24] Section 45 (opinions of experts) remains available for forensic authentication, yet lacks GenAI-specific protocols.[25]

4.3. CONCEPTUAL MISMATCH: GENAI'S DISRUPTION OF BSA PARADIGMS

*A. From "Records of Events" to "Synthetic Artifacts"***:** BSA presumes electronic records document *real-world referents*—emails chronicle communications; CCTV captures events.[26] GenAI inverts this: diffusion models sample from training distributions to generate *de novo* content sans originals.[27] A Stable Diffusion video of a politician's "confession" bears perfect metadata yet zero ontological grounding. BSA's "best evidence" rule (Section 60 analogue) falters: no "original" exists to compare against.[28]

B. Perceptual Reliability Collapse: Human vision/audition (95%+ confidence in high-fidelity deepfakes) underpins Sections 59–60 (oral/documentary evidence). The Deepfake Detection

[19] State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600, (India).
[20] BSA, 2023 § 61; Report of the Standing Committee on Home Affairs (Bharatiya Sakshya Bill, 2023), Lok Sabha Secretariat, (Nov. 10, 2023).
[21] BSA, 2023 § 62-63.
[22] *Id.* § 63A; IT Act, 2000 § 3A.
[23] Lok Sabha Debates on Bharatiya Sakshya Bill, 2023, (Dec. 2023) (India).
[24] BSA, 2023 § 57; Nat'l Inst. Of Standards & Tech., NISTIR 8456: Face Recognition Vendor Test (FRVT) Part 9: Face Recognition Accuracy with Synthetic Images (2024).
[25] BSA, 2023 § 45.
[26] *Id.* § 59-60, 61.
[27] Patrick Esser et al., *Improving Image Generation with Better Captions*, Proc. IEEE/CVF Conf. Computer Vision & Pattern Recognition 11937 (2024).
[28] BSA, 2023 § 60.

Challenge (DFDC) datasets shows that top models achieve only 65–80% accuracy on adversarial samples.[29] Courts untrained in error-rate calculus risk "illusory truth" effects.[30]

C. Device-Centric Certificates vs. Model-Centric Risks: Section 63 certificates verify *post-generation integrity* (SHA-256 hashes unchanged) but ignore *generation provenance* (prompts, model weights, seeds).[31] A deepfake exported from RunwayML passes hash tests impeccably, masquerading as authentic surveillance.[32]

4.4. DOCTRINAL STRESS-TESTING: GEN AI FACT PATTERNS UNDER BSA

A. Criminal Trial: Deepfake Confession (Sections 61, 63 and 27 Illustration)

Scenario: Prosecution tenders video of the accused confessing in custody; defence alleges DeepFaceLab synthesis.

BSA Application: Admissible as primary evidence (Section 61) with IO/forensic certificate (Section 63) confirming device extraction, unaltered hash. Court assesses weight via observation (Section 60), potentially noticing voice biometrics (Section 57).

Failures: No mandate for model disclosure, prompt logs, or detection scores.

B. Civil Fraud: LLM-Generated Emails (Sections 61–63A Illustration)

Scenario: Plaintiff produces GPT-4o "emails" with forged signatures, certified from "business server."

BSA Application: Primary evidence if PKI-signed (Section 63A); hash verifies integrity.

Failures: No AI-use disclosure; "ordinary course" presumption (Section 61) launders hallucinations. Absent Section 45 expert on LLM stochasticity, court presumes human

[29] *Id.* § 59-60; Deepfake Detection Challenge Results: An open initiative to advance AI, https://ai.meta.com/blog/deepfake-detection-challenge-results-an-open-initiative-to-advance-ai/ (last visited Jan. 10, 2026).
[30] Lisa Fazio*, Repetition Increases Perceived Truth Even for Known Falsehoods*, 28 Collabra Psychol. 1, 4 (2022).
[31] BSA, 2023 § 63.
[32] Introducing gen-3 alpha: A new frontier for video generation (2024) Runway Research. Available at: https://runwayml.com/research/introducing-gen-3-alpha (last visited Jan. 1, 2026).

authorship.

C. Harassment: Voice Clone Calls (Sections 59 and 63 Illustration)

Scenario: ElevenLabs clone of accused's voice threatens complainant.

BSA Application: Oral evidence analogue (Section 59) with extraction certificate.

Failures: No waveform forensics mandate; Section 45 experts opinions are scarce.

4.5. REFORM ROADMAP: AI-RESILIENT BSA FRAMEWORK

A. Statutory Amendments

1. **Section 63B (AI Disclosure)**: Mandate affidavits detailing model, prompts, seeds, detection scores.
2. **Section 63C (Provenance Standards)**: Require C2PA/ISO 42001 compliance; rebuttable presumption for biometric media.
3. **Section 57(2A) (Judicial Notice)**: Incorporate NIST/DFDC error rates.[33]

B. Procedural Innovations

1. **Court-Appointed Experts**: BSA Section 45A for AI forensics panels.
2. **Probabilistic Gatekeeping**: Admissibility if authenticity score >80% (Daubert-plus).[34]

C. Institutional Ecosystem

1. **National AI Evidence Lab**: Under NFSU/CFSL, equipped with MediFor/Sentinel.
2. **Judicial Training**: NJA modules on ELMo classifiers, watermark verification.
3. **Regulatory Harmonization**: IT Rules mandate platform provenance APIs.

[33] Int'l Org. for Standardization, ISO/IEC 42001:2023, AI Management Systems (2023).
[34] Daubert v. Merrell Dow Pharm., 509 U.S. 579 (1993); BSA, 2023 § 1(4).

D. Phased Implementation

Rule-making under BSA Section 1(4): Phase 1 (2026)—disclosure mandates; Phase 2 (2027)—tool integration.

BSA 2023 vaults India into digital-evidence modernity but stumbles at GenAI's threshold. Its architecture—laudable for CCTV/emails—crumbles under synthetic loads, exposing courts to liar's dividends and miscarriages. Targeted reforms—disclosure, provenance, expertise—can forge an AI-resilient framework, preserving truth-seeking amid technological tumult. Absent these, BSA risks obsolescence by 2030, as GenAI fluency eclipses judicial safeguards.

5. PRINCIPAL EVIDENTIARY RISKS: DEEPFAKES, SYNTHETIC MEDIA AND THE CORROSION OF JUDICIAL FACT FINDING

The heightened pace of Artificial Intelligence has given rise to the synthetic media popularly known as deepfakes, which are hyper realistic images, audio, and visual medias generated using high end AI techniques such as Generative Adversarial Networks, and Diffusion model which are indistinguishable from authentic media due to its dynamic nature causing increase in malpractices and crimes in digital world, which also leads to the inception of certain challenges which can corrode the judicial fact finding despite countermeasures like watermarking, metadata, and AI-based detection tools.[35]

The transition from Indian Evidence Act 1872, to the Bharatiya Sakshya Adhiniyam 2023 has been significant as it mandated digital certification of electronic records, hash value verification, and recognition of electronic records as primary evidence, however these modernised evidentiary norms struggle in identifying evidentiary risks and remain underdeveloped in regulating deepfakes and blockchain evidence.[36] The courts due to the high-end developing features of AI may constantly face the evidence which is generated, altered, interpreted and processed by AI rather than raw records drafted and presented by humans. This shift leads to the principal evidentiary risks posed by AI which are classified in a threefold manner, firstly authentication collapse and the insufficiency of the traditional evidentiary standards, secondly cognitive vulnerability, and thirdly the systematic collapse of evidence

[35] Irene Amerini et al., *Deepfake Media Forensics: Status and Future Challenges,* J.Imaging 11, 73 (2025) [hereinafter *Status & Future Challenges*].
[36] Deepti S, *supra* note 8 at 1947.

integrity.

5.1. AUTHENTICATION FAILURE & THE INSUFFICIENCY OF TRADITIONAL EVIDENTIARY STANDARDS

Authentication failure is a condition when the process of authentication gets compromised, which allows other users to impersonate registered legitimate users and gain unauthorised access to sensitive data and resources.[37] Often overlooked as a minor problem, authentication failure, in the judicial fact finding, disrupts the procedural structure of evidence laws by advancing numerous challenges before the court and investigating authorities, most of the time leaving courts in a binary crisis of either admitting such synthetic evidence which appears real, or exclude legitimate evidence by invoking baseless allegations.

The traditional evidentiary norms which have witnessed the transformation from the old evidence laws to the new statutory authorities, has its own implications, for which the digital evidence needs to get aligned with the probative value of the evidence laid down in the provisions of the Bharatiya Sakshya Adhiniyam, 2023 which includes authenticity, integrity, reliability and admissibility.[38] However, due to the deceptive nature of deepfakes the courts are confronted to decipher that whether the available records depict real incidents, does any manipulation occurred intentionally or accidentally, and whether the content is violating rights of a person – it is difficult to distinguish what is real and what is altered, which raises a significant question about the evidentiary value. Furthermore, the act assumes records to be reliable unless otherwise determined, and states about the involvement of an expert for specialised authentication as synthetic media potentially bypass ordinary forensic verification, the incoherence in adjudicating the AI based evidence persists in current framework which mark the evidentiary standards as insufficient.[39]

5.2. COGNITIVE VULNERABILITY

In psychology, cognitive vulnerability refers to a pattern of dysfunctional thinking that

[37] Vinay Kulkarni et. al., *Centrify DC Authentication Failures: Patterns, Prevention, and Protocols,* Vol. 10 Issue 6 IJSRET 1, 1 (2024) .
[38] Tanmay Pradeep, *Comparison Analysis between the Indian Evidence Act, 1872 and the Bharatiya Sakshya Adhiniyam, 2023,* Volume 16 Issue 1 IJSAT 1, 1-3 (2025).
[39] Harmanjeet Singh & Dr. Ritu Panta, *Deepfake Evidence and the Indian Criminal Justice System: Challenges of Authenticity, Consent and Admissibility in Law, 2025,* Volume 7 Issue 6 IJFMR 1, 3-4 (2025) [hereinafter *Harmanjeet*].

increases an individual's susceptibility to negative psychological outcomes, such as depression and anxiety which is often characterized by a high intolerance of uncertainty, leading to catastrophic interpretations of ambiguous information and trigger worry and anxiety.[40] The rise of deepfakes and synthetic media has become a significant domain of study as it potentially affects the cognitive vulnerability and intellectual capacity of individuals, it's upsurge leads to the development of "impostor bias", where individuals constantly mistrust the veracity of multimedia elements due to the awareness of synthetic media capability which induces systematic doubt of all digital evidence, authentic or otherwise.[41] This imposter bias can potentially trigger the cognitive vulnerability of investigating officers and other involved individuals in the chain of custody, which can lead to the unjust outcomes like wrongful convictions and acquittal. Recent case of Ankur Warikoo, listed in the High Court of Delhi ordered the removal of deepfake synthetic content posted on various social media platforms, however it did not mention any evidentiary framework for the courts to determine the authenticity in case where synthetic media is alleged in criminal contexts, which also implies the lack of systematic training of judicial officers across Indian states with respect to the subject.[42]

5.3. SYSTEMIC COLLAPSE OF EVIDENCE INTEGRITY

One of the principal evidentiary risks posed by deepfakes and synthetic media is systemic collapse of evidence preservation and integrity under the current evidentiary framework. The organisational weakness like inadequacy of AI detection centers to detect deepfake media in cyber-forensic laboratories, unreachable digital forensic experts during investigations, absence of consistent methods for determination of authenticity of deepfakes, and absence of machine learning driven indicators of validation in Digital Evidence Management Systems of investigation agencies make it difficult in distinguishing between deepfake media and real records, which ultimately causes the systemic collapse and disintegration of evidence at every other step.[43] This unfolds into multiple dimensions as follows:

1. *Chain of custody:* Every evidence documentation follows a process which incorporates chain of custody, that is the most significant link necessary to prove the integrity of a

[40] Taylor and Francis, Cognitive vulnerability – Knowledge and References, (last visited Dec. 22, 2025).
[41] Irene Amerini et al.; *Deepfake Media Forensics: State of the Art and Challenges Ahead, [cs. CV] arXiv:2408.00388*, 1, 1-2, (2024) [hereinafter *DMF: Challenges Ahead*].
[42] Ankur Warikoo & Anr. v. John Doe & Anr. CS(COMM) 514/2025.
[43] Harmanjeet, *supra* note 38, at 19.

piece of evidence, and assure before the court the authenticity of evidence. It needs to document every transmission and transfer from the point the evidence was retrieved, ensuring and allowing only authorised possession over it.[44] The chain of custody ensures whether such a piece of evidence is altered or not. In the case of AI based evidence, the situation gets more intricate and challenging as both the data and the algorithm needs to be authenticated, that too within a time limit. However, the courts might need to rely on third-parties and private companies for validating such data due to the operation of AI on a distributed cloud system.[45] Intermediaries with access to deepfake evidence must be competent enough to identify such reconstructions in chain of custody and use case-based verification processes, as solid procedures are required to assure evidence authenticity through strict provenance tracing.[46]

2. *Perpetual Detection Lag:* Perpetual Detection Lag refers to the condition when, deepfake detection methods in realistic scenarios poses certain challenges including time constraint and continuous training of AI detection models without experiencing catastrophic forgetting, and their capability to evolve, interpret, and detect the data accurately, however the evolved methods strain to cope up with new generative techniques due to data drift, here deepfake creation technologies consistently advances faster than detection methods creating endless reactive lag that undermines the reliability of such element.[47]

3. *Explainability and Black-Box Evidence:* Another critical challenge in context of deepfake detection for criminal justice system follows the lack of explainability of the outcomes of deep learning-based deepfake detectors, as while thriving for maximum accuracy, these datasets operate as Black boxes, where the internal reasoning and learning processes are opaque and not explicable to judges or expert witnesses, often hindering the ability to track down the specifications responsible for such results and complicating the decision making process of the courts.[48] Explainable and interpretable AI used in forensic investigations plays a significant role in legal and high-stakes

[44] Badiye A, Kapoor N, Menezes RG. Chain of Custody. [Updated 2023 Feb 13]. In: StatPearls [Internet]. Treasure Island (FL): StatPearls Publishing; 2025 Jan-. Available from: https://www.ncbi.nlm.nih.gov/books/NBK551677/.
[45] Deepanker, *supra* note 7, at 196.
[46] Harmanjeet, *supra* note 38, at 10-11.
[47] DMF: Challenges Ahead, *supra* note 40, at 4-6.
[48] E. Hydara et al.: *Empirical Assessment of Deepfake Detection: Advancing Judicial Evidence Verification,* Volume 12 IEEE Access 151188, 151191 (2024).

scenario, where these synthetic data systems are expected to provide clear, and interpretable decision process as it is essential for identification of biases and error sources, for enhanced trust and credibility, and facilitation of expert collaboration and continuous improvement in the integration of AI into the criminal justice system.[49]

6. COMPARATIVE BENCHMARKS: EVOLVING EVIDENTIARY FRAMEWORKS IN DEVELOPED JURISDICTIONS

6.1 EUROPEAN UNION

The principle evidentiary risks posed by AI are not only present in India but also lies in the framework of the European Union, as per UNESCO, the challenge of admissibility of AI generated evidence in courts is a striking issue within the framework, and the role of judicial operators is to develop an understanding of the algorithm, it's potential risks, biases, principles and potential misuses – to navigate the complexities of AI to provide well informed decisions regarding the admissibility of the evidence.[50]

However, the challenges got duly acknowledged and to address such AI posed risks, the European Union introduced the European Union Artificial Intelligence Act[51] which entered into force on August 1, 2024 and thereafter be effective from August 2, 2026.[52]

The EU Artificial Intelligence Act has set numerous benchmarks including the four-level risk classification under which the AI posed risks are chronologically arranged based on the gravity, which are: unacceptable risk (prohibited), high risk (strictly regulated), limited risk (transparency obligations), and minimal risk (unregulated). Other comparative benchmarks which are set by the EU include transparency obligations to clearly inform the end-users about the interaction; prohibition of deceptive AI which ensures AI manipulated evidence can't be used for deceptive means; ban on exploiting vulnerabilities which prevents AI tempered sensitive attributes from being admissible; limits on criminal profiling and predictive evidence that it cannot replace human decisions or objective facts; and high risk classification for

[49] Status & Future Challenges, *supra* note 34, at 15-16.
[50] *How to determine the admissibility of AI-generated evidence in courts?,* UNESCO NEWS (July 21, 2023), https://www.unesco.org/en/articles/how-determine-admissibility-ai-generated-evidence-courts?.com.
[51] THE ACT TEXTS | EU ARTIFICIAL INTELLIGENCE ACT, The AI Act Explorer | EU Artificial Intelligence Act [hereinafter *EU AI Act*] (last visited Dec. 22, 2025).
[52] Timo Gaudszun, et al., *AI Watch: Global regulatory tracker - European Union,* WHITE & CASE (July 21, 2025),https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-european-union?.com.

ensuring strict oversight and documentation in case of presence of AI in evidence generation or adjudication.[53]

The European Union in regulating the AI and deepfake synthetics, has critically evolved it's evidentiary framework by enforcing and interlinking the acts like the EU Artificial Intelligence Act[54], the EU General Data Protection Regulation[55], and the Digital Services Act[56] etc. altogether, to strictly maintain the standard of evidential adjudication, ensuring that synthetic media is subject to the transparency obligations, prohibitions against manipulative, deceptive & discriminatory practices, and strict oversight in justice and democratic contexts.

6.2. UNITED STATES OF AMERICA

The incorporation of artificial intelligence with the United States judicial framework has not led to bespoke statutory measures. When we look at how artificial intelligence fits into the American court system, no new laws have specifically emerged to handle it. Courts end up tweaking the Federal Rules of Evidence instead, those old standbys known as the FRE[57]. Mostly there exists a clash between how much courts trust outputs from algorithms and the sheer murkiness of those black-box systems that hide their inner workings.

Getting AI evidence into a trial relies heavily on judges acting as gatekeepers. Think back to Daubert v. Merrell Dow Pharmaceuticals[58] that case really hammered down the above-mentioned idea, and it has been stirred and baked into FRE 702[59] now. Now we have to check if a method holds up scientifically, look at its error margins, see what peers say about it. But applying all that to machine learning setups? Serious hurdles pop up. Proprietary algorithms just don't offer the openness needed for proper checks. At this point let's take State v. Loomis[60] in consideration, where Wisconsin's top court examined the COMPAS tool for predicting repeat offenses in sentencing. The usage of the tool was allowed, however, it was pointed out that there exists due process issues because the defendant cannot by any means peek at the

[53] EU ARTIFICIAL INTELLIGENCE ACT, High-level summary of the AI Act | EU Artificial Intelligence Act (last visited Dec. 22, 2025).
[54] EU AI Act, *supra* note 50.
[55] GENERAL DATA PROTECTION REGULATION, General Data Protection Regulation (GDPR) – Legal Text (last visited Dec. 22, 2025).
[56] DIGITAL SERVICES ACT (DSA) | FINAL TEXT, Digital Services Act (DSA) | Final Text (last visited Dec. 22, 2025).
[57] Fed. R. Evid. 28 U.S.C. app (2012).
[58] 509 U.S. 579 (1993).
[59] Fed. R. Evid. 702, (2012).
[60] 881 N.W.2d. 749 (Wis 2016).

secret code, setting a kind of standard in its operation. Evidence from these opaque systems can get misleading unless a system of checks and balances is being introduced.

Then there's authentication under FRE 901(b)(9)[61], which deals with verifying processes or setups, and it brings its own tough barriers. Traditional digital checks follow a clear chain of logic, step by step. Modern neural networks? They run on complex, twisting paths that aren't easy to explain. Add in generative AI or deepfakes, and suddenly courts demand strict verification steps to block faked stuff. The aim: keep out anything tampered with. Experts in law point out how trade secret laws often clash with the core right to challenge evidence through questioning, a conflict that lingers without clear fixes.

In this phase of AI's role in U.S. evidence rules, things seem headed toward demanding more clarity overall. Business motives frequently cloud how reliable this evidence really is, pitting openness against claims of ownership in ways that spark ongoing debates. Overall, U.S. evidence law in the Al era is moving toward a stronger expectation that Al systems be explainable. Judicial bodies have now started to confront the concept of AI in procedure implementation with constitutional protections, amid a context where evidentiary trustworthiness is often veiled by commercial interests.

7. CONCLUSION

On a concluding note, we can observe that the world of AI brings not only a wave of growth, development and innovation in Indian Courts but also bring with itself a whole new set of challenges. The provisions of BSA serves as a fresh upgrade from its predecessor, free from its colonial vestiges, but its existing provisions does not fulfil the minimum needs of the rising use and misuse of AI. Certain specific electronic evidence such as CCTV footages, the core internal data of certain software, face recognition as well as use of AI in hacking computer resources exposes the existing traditional system of evidence appreciation at the mercy of expert opinions, which may or may not be up to date with the unprecedented pace of AI advancement. Here, purely as an academic opinion it becomes essential to inculcate specialized education and awareness drives for personnel involved in cyber security as well as agencies responsible for collection and investigation of electronic evidence at the ground level. AI not only raises investigative eyebrows with a high sense of distrust but also increases the possibility

[61] Fed. R. Evid. 901 (b) (9) (2012).

of implantation of false and fabricated evidences, which might look so compelling prima facie that it may change the very direction of police investigation or on the flip side, sway the whole prosecution story apart. Though existing penal laws covers almost every dimension of offences involving use or presentation of false/fabricated evidence in courtroom, the procedural and evidentiary arms of law demand some additional strength for holding and securing justice in today's unpredictable hour of AI.

BIBLIOGRAPHY

INDIAN CASES

1. Ankur Warikoo & Anr. v. John Doe & Anr. CS(COMM) 514/2025
2. Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473
3. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.
4. State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600, (India).

STATUTES

1. 509 U.S. 579 (1993).
2. 881 N.W.2d. 749 (Wis 2016).
3. Digital Personal Data Protection Act, 2023, § 1, No. 23, Acts of Parliament, 2023 (India).
4. DIGITAL SERVICES ACT (DSA) | FINAL TEXT, Digital Services Act (DSA) | Final Text (last visited Dec. 22, 2025).
5. Fed. R. Evid. 28 U.S.C. app (2012).
6. Fed. R. Evid. 702, (2012).
7. Fed. R. Evid. 901 (b) (9) (2012).
8. GENERAL DATA PROTECTION REGULATION, General Data Protection Regulation (GDPR) – Legal Text (last visited Dec. 22, 2025).
9. Information Technology Act, 2000,§ 1, No. 21, Acts of Parliament, 2000 (India).
10. THE ACT TEXTS | EU ARTIFICIAL INTELLIGENCE ACT, The AI Act Explorer | EU Artificial Intelligence Act [hereinafter *EU AI Act*] (last visited Dec. 22, 2025).

FOREIGN CASES

1. Daubert v. Merrell Dow Pharm., 509 U.S. 579 (1993)

JOURNALS & PERIODICALS

1. Danille Keats Citron & Robert Chesney, *Deep Fakes: A Looming Challenge for Privacy, Democracy and National Security*, 107 CALIF. L. REV. 1753, 1757-60 (2019).

2. Deepanker Singhal & Pragya Narang, *Ai-Generated Evidence in Indian Courts: Admissibility, Reliability and The Chain of Custody Challenge*, Vol. V. Issue. V IJIRL 186, 186-204 (2025) [hereinafter *Deepanker*].

3. Dr. Deepti Singhla, *Navigating Deepfakes in, Indian Criminal Law*, Vol. V Issue III IJIRL 1943, 1943-1960 (2025) [hereinafter *Deepti S*].

4. E. Hydara et al.: *Empirical Assessment of Deepfake Detection: Advancing Judicial Evidence Verification,* Volume 12 IEEE Access 151188, 151191 (2024).

5. Hany Farid, Seeing Is No Longer Believing: Detecting Deepfakes, 372 Science 1396 (2021).

6. Harmanjeet Singh & Dr. Ritu Panta, *Deepfake Evidence and the Indian Criminal Justice System: Challenges of Authenticity, Consent and Admissibility in Law, 2025,* Volume 7 Issue 6 IJFMR 1, 3-4 (2025) [hereinafter *Harmanjeet*].

7. Irene Amerini et al., *Deepfake Media Forensics: Status and Future Challenges,* J.Imaging 11, 73 (2025) [hereinafter *Status & Future Challenges*].

8. Irene Amerini; *Deepfake Media Forensics: State of the Art and Challenges Ahead, [cs. CV] arXiv:2408.00388*, 1, 1-2, (2024) [hereinafter *DMF: Challenges Ahead*].

9. Lisa Fazio*, Repetition Increases Perceived Truth Even for Known Falsehoods*, 28 Collabra Psychol. 4 (2022).

10. Navin Kumar, *From Surveillance to Sentencing: Evaluating AI's Role in Indian*

Criminal Justice, Vol. XXX, No. 1(59) SCIENTIFIC BULLETIN 68, 68-78 (2025).

11. Patrick Esser et al., Improving Image Generation with Better Captions, Proc. IEEE/CVF Conf. Computer Vision & Pattern Recognition 11937 (2024).

12. Sukhandeep Kaur et. al., *Hindi audio-video-Deepfake (HAV-DF): A Hindi language-based Audio-video Deepfake Dataset*, arXiv:2411.15457v1 [cs.SD] 1, 1-22 (2024).

13. Tanmay Pradeep, *Comparison Analysis between the Indian Evidence Act, 1872 and the Bharatiya Sakshya Adhiniyam, 2023,* Volume 16 Issue 1 IJSAT 1, 1-3 (2025).

14. Tanmay Pradeep, *Comparison Analysis between the Indian Evidence Act, 1872 and the Bharatiya Sakshya Adhiniyam, 2023,* Volume 16, Issue 1, IJSAT, 1, 1-3 (2025).

15. Trishita Chatterjee*, Admissibility of Ai-Reviewed Digital Evidence in Legal Investigations,* V, IJIRL, 2056, 2060-2062, (2025).

16. Vinay Kulkarni et. Al., *Centrify DC Authentication Failures: Patterns, Prevention, and Protocols,* Vol.§ 10 Issue 6 IJSRET 1, 1 (2024) .

17. Zhang, H. (2025). 2(2), 34-41. ISSN Print: 3079-515X; ISSN Online: 3079-5168. [Hua Zhang, *The Evidentiary Value of AI-Generated Data: A Framework for Reliability and Admissibility*, 2(2) EDUCATION AND SOCIAL WORK 34, 34-41 (2025).

OTHER AUTHORITIES

1. Badiye A, Kapoor N, Menezes RG. Chain of Custody. [Updated 2023 Feb 13]. In: StatPearls [Internet]. Treasure Island (FL): StatPearls Publishing; 2025 Jan-. Available from: https://www.ncbi.nlm.nih.gov/books/NBK551677/ .

2. Deepfake Detection Challenge Results: An open initiative to advance AI, https://ai.meta.com/blog/deepfake-detection-challenge-results-an-open-initiative-to-advance-ai/ (Last Visited Jan. 10, 2026).

3. EU ARTIFICIAL INTELLIGENCE ACT, High-level summary of the AI Act | EU Artificial Intelligence Act (last visited Dec. 22, 2025).

4. Google DeepMind, Veo: A New Frontier in Video Generation (2024), https://deepmind.google/technologies/veo

5. *How to determine the admissibility of AI-generated evidence in courts?,* UNESCO NEWS (July 21, 2023), https://www.unesco.org/en/articles/how-determine-admissibility-ai-generated-evidence-courts?.com.

6. Int'l Org. for Standardization, ISO/IEC 42001:2023, AI Management Systems (2023)

7. Introducing gen-3 alpha: A new frontier for video generation (2024) Runway Research. Available at: https://runwayml.com/research/introducing-gen-3-alpha (Last Visited: 01 January 2026).

8. Lok Sabha Debates on Bharatiya Sakshya Bill, 2023, (Dec. 2023) (India).

9. Nat'l Inst. Of Standards & Tech., NISTIR 8456: Face Recognition Vendor Test (FRVT) Part 9: Face Recognition Accuracy with Synthetic Images (2024).

10. Report of the Standing Committee on Home Affairs (Bharatiya *Sakshya Bill, 2023), Lok Sabha Secretariat, (Nov. 10, 2023).*

11. Statement of Objects and Reasons, The Bharatiya Sakshya (Second) Bill, 2023, Bill No. 130 of 2023, Lok Sabha (India).

12. Taylor and Francis, Cognitive vulnerability – Knowledge and References, (last visited Dec. 22, 2025).

13. Timo Gaudszun, et al., *AI Watch: Global regulatory tracker - European Union,* WHITE & CASE (July 21, 2025),https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-european-union?.com.