ANALYSIS OF DEEP FAKES, DIGITAL MANIPULATIONS AND EVIDENCE LAW IN ARTIFICIAL INTELLIGENCE GENERATED EVIDENCE UNDER THE BHARATIYA SAKSHYA ADHINIYAM (2023).

Bavishya Manasa V, BA LLB (hons), school of Law, SASTRA University, Thirumalaisamuthram, Thanjavur, Tamil Nadu – 613401, India

Abstract:
The rapid advancement of Artificial Intelligence (AI) has significantly transformed the nature of digital evidence in contemporary legal systems. Technologies such as deepfake videos, AI-generated audio recordings, manipulated images, and synthetic documents have created serious challenges regarding the authenticity and reliability of electronic evidence in the legal field. In India, the increasing dependence on digital evidence in judicial proceedings raises important concerns regarding the admissibility, verification, and misuse of AI-generated content. This study examines the admissibility of AI-generated evidence under Indian Evidence Law, which is now being governed under the provisions of the Bharatiya Sakshya Adhiniyam, 2023. Indian courts continue to face significant challenges concerning the admissibility, authenticity, and reliability of technologically manipulated digital evidence in court. Landmark judicial decisions, such as Anvar P.V. v. P.K. Basheer and Arjun Panditrao Khotkar V. Gorantyal highlighted the importance of authenticity and procedural safeguards in the admissibility of electronic evidence. This study adopts a doctrinal method of research by analyzing statutory provisions, judicial precedents, legal principles, and scholarly writings relating to electronic evidence and evidentiary standards. The present study concludes that the existing evidentiary framework in India is not fully equipped to address the complexities of AI-generated evidence. This emphasizes the need for stronger forensic verification mechanisms, specialized legal regulations, and judicial awareness to ensure the authenticity and reliability of digital evidence in the era of artificial intelligence.

KEYWORDS
AI-Generated evidence, electronic evidence, Deep fake technology, Digital manipulation, Admissibility of evidence.

I. INTRODUCTION

Artificial Intelligence (AI) is a field of computer science that focuses on creating systems capable of performing tasks that typically require human intelligence. This includes things like reasoning, learning from past experiences, finding patterns, and making decisions. The rapid growth of artificial intelligence has significantly transformed the nature of evidence used in judicial proceedings. Now a days the increasing technological advancement viz; electronic records such as emails, closed-circuit television (CCTV) footage, mobile phone data, social media communications, digital photographs, and electronic contracts have become important sources of evidence in both civil and criminal cases.

Artificial Intelligence based technologies are now capable of generating highly realistic digital content, including deep fake videos, synthetic voice recordings, manipulated images, and automated documents. Such technologies have created serious concerns regarding the authenticity, reliability, and admissibility of electronic evidence in courts of law. The Indian legal system has recognized electronic evidence through provisions relating to digital records under the Indian Evidence Act (1872), which are now incorporated under the Bharatiya Sakshya Adhiniyam (2023). Under this Act, provision for electronic and digital evidence is made. Sections 65A and 65B are used to prove electronic evidence under the Indian Evidence Act, while similar provisions have been made under Sections 62 and 63 of the new law for the proof of electronic records. Modern civil disputes increasingly face challenges from synthetic media. The procedural validity of a certificate under Section 63 is often insufficient to detect substantively fabricated evidence like deep fakes, necessitating more rigorous forensic checks (White Black Legal, 2025).

In the absence of clear legal standards regulating AI-generated evidence, courts may face difficulties in determining its authenticity and ensuring justice. Therefore, there is a growing need to examine the adequacy of Indian evidence law in addressing the challenges posed by AI-generated electronic evidence. Hence this research paper focusses the legal and ethical concerns associated with AI-generated evidence, including manipulation, privacy violations, the burden of proof, and threats to fair trial principles. A comparative analysis of international approaches towards the regulation of AI-generated evidence is also undertaken to identify possible reforms for the Indian legal framework.

II. LITERATURE REVIEW

Chhatrapati & Prasad (2021); Vichare (2025) stated that the Legal research on electronic evidence (often called digital evidence) focuses on the admissibility, authenticity, and reliability of data stored or transmitted in binary form and also the legal landscape has

shifted from the traditional Indian Evidence Act, 1872 to the Bharatiya Sakshya Adhiniyam, 2023 (BSA), which modernizes the framework for digital evidence. Section 63 of the BSA has replaced the long-standing Section 65B of the Indian Evidence Act (Chadha & Sivaraman, 2024).

Jurnal Hukum dan Peradilan (2023) reported that the digital data is uniquely susceptible to undetectable alterations. Legal systems now rely heavily on Digital Forensics to prove the "Chain of Custody", Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020), established that the certificate as a "condition precedent," remain foundational, though they are now interpreted through the lens of Section 63 of the BSA (White Black Legal, 2025). Legal research on electronic evidence in Indian civil cases centers on the transition from the Indian Evidence Act (IEA), 1872 to the Bharatiya Sakshya Adhiniyam (BSA), 2023, which came into effect on July 1, 2024 (The Indian Journal for Research in Law and Management (IJRLM, 2026).

The BSA modernizes the treatment of digital records by elevating them to the status of primary evidence and introducing stricter technical authentication requirements, such as hash value verification (AIJFR, 2026a). Landmark cases the Digital Personal Data Protection Act (DPDPA), 2023, further complicates civil discovery by regulating how personal data is acquired and stored, emphasizing that dignity and privacy are fundamental rights even within evidentiary procedures (PMC, 2025).

Legal research on electronic evidence in Indian criminal cases currently centres on the transition from the Indian Evidence Act (IEA), 1872 to the Bharatiya Sakshya Adhiniyam (BSA), 2023, which came into force on July 1, 2024. In the 2026 legal landscape, digital records are no longer considered "ancillary" but are treated as a mainstream, primary category of evidence (LawSikho, 2026). Courts in 2026 place a heavy burden on the prosecution to prove the "digital chain of custody." This involves documenting every hand that touched the device or file from the scene of the crime to the forensic lab (INSC, 2026). Judges are now required to look beyond "procedural validity" (the certificate) and scrutinize "substantive authenticity" to detect AI-manipulated evidence (Mishika, 2026). The Digital Personal Data Protection Act (DPDPA), 2023, intersects with criminal trials, requiring courts to balance the search for truth with the privacy rights of the accused and victims (PMC, 2025).

III. RESEARCH METHODOLOGY

This research is done by doctrinal method. Doctrinal research methodology is a systematic, library-based approach to legal research that focuses on analyzing "black letter law" statutes, case law, regulations, and legal principles. It aims to identify the "one right answer" or current legal position on a specific issue through logical reasoning, interpretation, and synthesis of authoritative legal sources

3.1 Steps in the Doctrinal method

1) **Identify the Research Problem**: Formulate the specific legal question or hypothesis, often centered on "What is the law?".
2) **Gather relevant material**: Locate relevant primary (cases/statutes) and secondary sources.
3) **Analyze and Evaluate**: Read, analyze, and synthesize legal materials to establish the legal doctrine.
4) **Synthesize findings**: Systematize legal propositions to resolve the research question.
5) **Formulate conclusions**: Predict the likely future development of the law or provide a definitive interpretation of the existing law

IV. STATEMENT OF PROBLEM

"To evaluate the efficacy of the Bharatiya Sakshya Adhiniyam (BSA), 2023 in addressing the evidentiary challenges posed by AI-generated deepfakes and digital manipulations, specifically examining whether the current legal standards for admissibility and authentication are sufficient to distinguish between 'synthetic' and 'real' electronic records in a court of law."

4.1 Research questions

1. Does the definition of "Electronic Records" under the BSA sufficiently encompass hyper-realistic synthetic media generated by GANs (Generative Adversarial Networks)?
2. How does the Section 63 certificate requirement (successor to Section 65B of the IEA) function when the 'origin' of the evidence is an autonomous AI system rather than a human-operated device?
3. In an era of "liar's dividend" (where parties claim real evidence is fake), should the BSA shift the burden of proof regarding the integrity of digital metadata?
4. How can the BSA bridge the gap between legal "proof" and technical "detection" when AI-driven manipulations are designed to bypass standard forensic hashes?

V. RESULTS AND FINDINGS

Under the Bharatiya Sakshya Adhiniyam (BSA), 2023, the definition of "Electronic Records" is technically broad enough to encompass AI-generated media, but its procedural framework faces a significant "authenticity crisis" when dealing with hyper-realistic synthetic media like GAN-generated deep fakes. One of the most significant shifts in the BSA is the elevation of digital records to Primary Evidence. Section 57, it states that where an electronic or digital record is produced from "proper custody," it is considered primary evidence unless disputed (AIJFR, 2026). The rapid evolution of GANs has outpaced the BSA's procedural safeguards, leading to two primary legal vulnerabilities, they are Substantive vs. Procedural Validity, it defines, the courts may find deep fakes procedurally valid (correct certificate, correct hash) even if they are substantively fake (International Journal of Advanced Legal Research [IJALR], 2025).The Liar's Dividend, the emergence of high-quality AI allows defendants to dismiss genuine evidence of misconduct as "AI-fabricated," fostering a "post-truth" environment that complicates judicial accountability (Mishika, 2026).

The transition from Section 65B of the Indian Evidence Act (IEA) to Section 63 of the Bharatiya Sakshya Adhiniyam (BSA), 2023, introduces a more rigorous "Dual-Certification" regime. When the "origin" of evidence is an autonomous AI system, the requirement shifts from certifying human intent to certifying algorithmic process integrity. Unlike the old Section 65B, which typically required a single certificate from a "person in charge" of the device, Section 63 BSA mandates a two-part certificate as prescribed in the Schedule of the Act: Part A (The Custodian), to be filled by the person who owns, manages, or operates the system. In the case of autonomous AI, this is the individual or entity overseeing the AI's deployment (e.g., a System Administrator or Data Officer). Part B (The Expert), this is a new, mandatory requirement under Section 63(4)(c). An expert must certify the technical integrity of the record. This is crucial for AI evidence to ensure the "black box" of the autonomous system was functioning as intended. Because Section 63 was modelled on human-fed data ("information was regularly fed into the computer"), autonomous AI creates a unique legal friction,

The burden of proof is fueled by the "epistemic crisis" where deep fakes undermine the reliability of all digital records. While the Bharatiya Sakshya Adhiniyam (BSA), 2023, moves toward modernizing evidence, its current structure remains anchored in the "Prover-Led" model. The BSA (Section 63) currently focuses on integrity rather than provenance. A Section 63 certificate attests that the *computer* was working properly and the *hash value* matches. It does not verify if the content was synthetic at the point of origin. Because the law currently accepts "properly functioning hardware" as a proxy for "truthful data," a defendant can easily claim a genuine video is a deep fake, knowing the prosecution may lack the forensic tools to prove the *negative* (that it is NOT AI-generated). The Proposed Solution is "The Probabilistic Shift". Legal scholars suggest that instead of a total shift, the BSA should adopt a tiered burden based on the type of evidence like Standard Records (Primary Evidence), Records from "proper custody" should carry a rebuttable presumption of integrity. The burden shifts to the challenger. Then the High-Risk Media (Secondary Evidence), For videos, voice notes, or photos where the risk of "liar's dividend" or deep fakes is highest (Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal ,2020).

The Bharatiya Sakshya Adhiniyam (BSA), 2023, which replaced the Indian Evidence Act, represents a pivot toward a digital-first legal framework. However, a significant gap exists between legal "proof" (which historically relies on the binary certainty of forensic hashes) and technical "detection" (which, in the AI era, is increasingly probabilistic). When AI-driven manipulations bypass standard forensic hashes (like MD5 or SHA-256) by creating entirely new "original" synthetic data, the BSA bridges this gap through three primary mechanisms: expanded definitions, probabilistic expert testimony, and proactive authentication. Traditional forensic hashes prove that a file has not been altered since it was hashed. AI-generated deepfakes, however, are "born" manipulated; they are technically pristine at the file level but fraudulent in content. Under Section 63(4), the certificate must confirm that the "computer" or "system" was operating properly. For AI, this shifts the burden of proof from "Is this the same file?" to "Does the system that created this file have a record of authentic human input?". The BSA emphasizes the entire lifecycle of the record. If a hash cannot prove the content is real, the legal "proof" relies on the provenance, the verifiable trail of where the data originated before it reached the forensic stage. Since AI detection tools often yield a "probability score" (e.g., "98% likely to be synthetic") rather than a binary hash match, the BSA utilizes Expert Testimony (Sections 39-40) to bridge the gap Zeng, J., et al. (2025).

Technical detection now involves analyzing "physiological markers" (like blinking patterns or ear shape) and "compression artifacts." Under the BSA, a forensic expert can present these probabilistic findings as an "opinion." The court then weighs this against the Section 63 Certificate. If the technical detection shows AI-typical artifacts, the legal proof is established not by a hash match, but by the expert's ability to demonstrate the *unreliability* of the source. The BSA's focus on "digital records" (Section 61) allows for the inclusion of emerging industry standards that go beyond hashes. The Software Alliance advocate for the Coalition for Content Authenticity and Provenance (C2PA). This technology embeds "manifests" directly into the metadata at the moment of capture. While a hacker can change a hash by changing one pixel, C2PA uses a "signed" history. The BSA facilitates this by allowing courts to accept these advanced metadata logs as part of the primary evidence (Section 62), effectively bypassing the need for a 1:1 hash comparison if the provenance chain is cryptographically signed.

VI. CONCLUSION

The shift toward the Coalition for Content Authenticity and Provenance (C2PA) represents a fundamental evolution in how the legal system perceives digital truth. By advocating for embedded "manifests," the Software Alliance (BSA) is effectively moving the goalposts from reactive detection to proactive authentication. While traditional forensic hashes remain a vital tool for identifying exact duplicates, they are increasingly insufficient against the fluid nature of AI-generated manipulations. The Bharatiya Sakshya Adhiniyam (BSA), 2023, anticipates this technological gap by prioritizing the provenance chain and cryptographic signatures over static bit-for-bit identity. Under Section 62, the recognition of these advanced metadata logs as primary evidence allows the judiciary to bridge the gap between technical detection and legal proof. Ultimately, this framework ensures that even as AI makes it easier to "bypass" the signature of a file, the law can still verify the intent, origin, and history of the data, maintaining the integrity of the digital justice system in an era of synthetic media.

VII. REFERENCES

1. AIJFR. (2026). Trial Court as Guardian of Electronic & Digital Record Under Section 63 of the Bharatiya Sakshya Adhiniyam, 2023. *AIJFR*.

2. AIJFR. (2026a). Supply of copy of electronic evidence - Suggested system for District Courts. *Advanced International Journal for Research*, *7*(1).

3. AIJFR. (2026b). Trial Court as Guardian of Electronic & Digital Record Under Section 63 of the Bharatiya Sakshya Adhiniyam, 2023. *Advanced International Journal for Research*.

4. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020): Established that the certificate is a mandatory condition precedent, reinforcing the proponent's burden.

5. Arora, R. (2026). Implications of deepfakes: Ethical and legal challenges. *Supremo Amicus*, *40*, 1–15.

6. Chadha, V., & Sivaraman, J. (2024). Critical analysis of the law on admissibility of electronic evidence in India. *Jindal Global Law Review*. 41020-024

7. Chhatrapati, M. D., & Prasad, D. A. B. (2021). Electronic Evidence–Admissibility and Authentication: A Judicial Perception of Apex Court of India. *GLS Law Journal*, *3*(1).

8. International Journal of Research and Trends in Innovation. (2025). AI-Generated Deep fakes and the Legal Vacuum in India: A Constitutional and Regulatory Analysis. *IJRTI*, *25*(11), 99.

9. Jurnal Hukum dan Peradilan. (2023). Electronic Evidence in the Healthy Justice System: Reimagined. *Jurnal Hukum dan Peradilan*, *12*(3).

10. LawSikho. (2026, April 2). *Electronic Evidence BSA Section 63: Complete Guide for Criminal Lawyers*.

11. Mishika. (2026). 2026 IT rules and the judicial response to India's deepfake proliferation. *Indian Journal of Advanced Legal Research*.

12. PMC. (2025). The Digital Personal Data Protection Act 2023: Implications for Mental Healthcare Practice in India. *PubMed Central*.

13. Vichare, R. (2025). An Admissibility of Electronic Evidence in Criminal Proceedings: A Comprehensive Analysis. *Indian Journal of Integrated Research in Law*.

14. White Black Legal. (2025). A compilation of recent Indian cases re – Deep fake evidence and Section 63 BSA.

15. White Black Legal. (2026). Digital forensics in India: Lawful collection and preservation. *White Black Legal*, *3*(6).

16. Zeng, J., et al. (2025). Tiered anonymity on social-media platforms as a countermeasure against deep fakes and LLM-driven mass misinformation. *25*(11), 99.