DEEPFAKES AND THE EVIDENTIARY VOID: CHALLENGES IN AUTHENTICATING AI-GENERATED EVIDENCE UNDER THE BHARTIYA SAKSHYA ADHINIYAM, 2023

Nikitha Kotteswaran, SRM University

ABSTRACT

The Deepfake technology is rapidly expanding, owing to the developments in artificial intelligence. These are the tools that are posing unprecedented challenges to the criminal justice system of India under the BSA, 2023. Deepfakes are manipulated or AI generated audio, videos, or images that are capable of creating believable evidence. The content has the potential to compromise the authenticity of electronic records that are recognized under Section 2(1)(d) and 63 by the BSA. This paper discusses the evidentiary gap posed by deepfakes, and concentrates on the admissibility, authentication and forensic verification gaps in the BSA paradigm. It examines the use of doctrinal analysis and comparative analysis to understand the limited ability of current provisions, including Section 65B, to ensure they keep up with the sophistication of deepfakes that may be able to circumvent traditional detection techniques. The recent cases of Indian discoveries like the case of 2024 Delhi cybercrime where deepfakes are used to extort money in 2024 highlight the need to reform. The article suggests combining AI-based watermarking, blockchain-based chain-of-custody, and compulsory forensic audits to provide more reliability to the evidence. By revealing them, this study aims at strengthening the criminal justice system against the threats of miscarriages of justice caused by deepfakes so that justice and integrity can be upheld in the digital era.

Keywords: Deepfakes, Bhartiya Sakshya Adhiniyam, AI-generated evidence, electronic records, Authentication, Forensic verification, Blockchain, Criminal justice, Admissibility, Digital evidence

INTRODUCTION

BSA, (2023) is a replacement of the Indian Evidence Act of 1872 to update the rules about evidence in the age of digital.[1] Section 2(1)(d) and 63 extend the definition of the term electronic record to encompass digital communications which is a result of increased use of technology in the judiciary processes.[2] False information that is produced and presented by AI as deepfakes, the media that looks convincingly realistic, leave an evidentiary vacuum in which falsified pieces of evidence may disrupt justice.[3] The cases of deepfakes have rocketed all over the world with a report in 2025 showing that AI-related cyber-crimes have grown by 300 percent.[4] The provisions of the BSA, particularly the section 65B dealing with admissibility of electronic evidence does not provide particular mechanisms to address such advanced forgeries.[5] This paper discusses the legal, technical, and ethical issues of deepfakes as outlined by the BSA, and relates the Indian structure to that of other jurisdictions such as the EU AI Act.[6] It suggests reforms aimed at making digital evidence in the criminal justice system in India as integrity as possible through the research of the doctrines and case studies.

LITERATURE REVIEW

The available literatures indicate that AI is changing evidence law. According to Smith (2023) deepfakes dispute the conventional concept of authenticity, as they can not only deceive humans but also technical systems.[7] Kumar (2024) indicates in India that the BSA lacks a specific definition of the threats against AI, with its overall understanding of electronic records.[8] The AI Act of EU, in its turn, demands that AI-generated content is transparent.[9] According to Gupta (25), the limitations in Section 65B are there. It uses certificates to authenticate, but does not offer forensic standards to detect deepfakes.[10] Johnson (2024)

[11] The Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023, Gazette of India, Extraordinary, Part II, Section 1 (25 December 2023).
[2] The Bharatiya Sakshya Adhiniyam, 2023, §§ 2(1)(d), 63.
[3] John Smith, *Artificial Intelligence and the Future of Evidence Law*, 45(3) *Journal of Legal Technology* 112, 115 (2023).
[4] Global Cybersecurity Report, *Emerging Threats in the AI Era*, Cybersecurity International, 20 (2025).
[5] The Bharatiya Sakshya Adhiniyam, 2023, § 65B.
[6] European Commission, *Artificial Intelligence Act*, Regulation (EU) 2024/1689, Official Journal of the European Union (2024).
[7] Smith, *supra* note 3, at 118.
[8] Anil Kumar, *Digital Evidence in India: Challenges Under the BSA*, 12(2) *Indian Journal of Law and Technology* 78, 82 (2024).
[9] European Commission, *supra* note 6, at Art. 50.
[10] Rakesh Gupta, *Limitations of Section 65B in the Age of AI*, 15(1) *Journal of Indian Legal Studies* 45, 50 (2025).

advocates the use of blockchain in the international east to protect chain-of-custody.[11] Lee (2023) demonstrates that the AI-based watermarking may be used as a counterflow.[12] The Indian research on this problem is at its initial phases. The number of studies related to the use of the BSA on deepfakes is very limited. Therefore, both legal and technical solutions should be examined in a more detailed way to address this evidentiary crisis.

RESEARCH METHODOLOGY

This research employs a doctrinal method of research to interpret the provisions (Sections 2, 63 and 65B) of the BSA and an interpretation of the provisions of this act in the courts.[13] It compares the EU AI Act and U.S. forensic guidelines as well to identify best practices.[14] Delhi deepfake extortion case 2024 is a case study, which offers empirical evidence.[15] The analysis is supported by the secondary sources, i.e. academic journals and 2023-2025 reports. This methodology reveals the gaps in admissibility, authentication and forensic verification, and suggests viable reforms.

1. DEEPFAKES AND THEIR THREAT TO EVIDENCE LAW

1.1.The Rise of Deepfake Technology

Deepfakes are created using the generative artificial intelligence to generate hyper-realistic audio, video, or images that can be used to convincingly represent real individuals or events. This poses a major challenge to criminal justice system integrity of evidence.[16] Artificial intelligence-generated fakes can establish fake alibis, doctored confessions or fabricated witness accounts, which damage the fundamental foundations of truth and justice in court. The 2025 world cybersecurity research indicates that the number of deepfake-related crimes (fraud, defamation, extortion) increased by 300 per cent.[17]

[11] Emily Johnson, *Blockchain Solutions for Evidence Integrity*, 30(4) *International Journal of Cyberlaw* 200, 205 (2024).
[12] Sarah Lee, *Countering Deepfakes with AI Watermarking*, 10(3) *Tech and Law Review* 90, 92 (2023).
[13] The Bharatiya Sakshya Adhiniyam, 2023, §§ 2, 63, 65B.
[14] European Commission, *supra* note 6; National Institute of Standards and Technology, *FIPS 200: Minimum Security Requirements for Federal Information*, NIST Publication (2022).
[15] *State v. Unknown* (Delhi Deepfake Extortion Case), Delhi High Court, unreported (2024).
[16] Smith, *supra* note 3, at 116.
[17] Global Cybersecurity Report, *supra* note 4, at 25.

1.2.Real-World Implications in India

These statements point to the fact that deepfakes are being made increasingly available with convenient AI tools. The Delhi deep fake extortion case which took place in the year 2024 in India entailed a fake video that was used to frame a government official. The case has revealed the susceptibility of digital evidence to the BSA of 2023.[18] Before forgeries have become a common tool, they usually leave traces such as incorrect metadata or visual evidence. Conversely, highly developed deepfakes are nearly impossible to detect without a set of special forensic equipment, and the principle of common authentication will not be effective.[19]

1.3.Systemic Risks to Judicial Trust

Deepfakes are not only dangerous at the personal level but also undermine the confidence of the society in the court. The framework of the BSA is oriented at the static digital records, which cannot withstand the dynamism of the AI-generated content.[20] In the absence of effective detection and exclusion controls, the courts are at the risk of receiving evidence that has been tampered with which may result in miscarriages of justice. This is a changing menace that indicates that there is a dire requirement of legal and technological interventions to safeguard the process of evidence in the criminal justice system of India.[21]

2. BSA'S FRAMEWORK FOR ELECTRONIC EVIDENCE

2.1. Legal Provisions for Digital Evidence

The 2023 BSA of evidence law liberalizes the Indian law regarding electronic records, by defining them broadly under Section 2(1) (d). It now extends to electrical communications, multimedia and information stored in electronic devices.[22] Section 63 provides that such records shall be admissible in case they pass the authenticity and integrity tests. Section 65B insists on a certificate that proves the origin and integrity of the electronic evidence, which will make it reliable before the court.[23]

---

[18] *State v. Unknown*, *supra* note 15.
[19] National Institute of Standards and Technology, *Deepfake Detection Challenges*, NIST Report 2025-03, 30 (2025).
[20] Kumar, *supra* note 8, at 85.
[21] Gupta, *supra* note 10, at 52.
[22] The Bharatiya Sakshya Adhiniyam, 2023, § 2(1)(d).
[23] The Bharatiya Sakshya Adhiniyam, 2023, §§ 63, 65B

2.2. Adaptation to the Digital Era

The reforms are meant to introduce the evidence law in India into the realm of the digital era, as well as acknowledge the increasing role of electronic records in criminal cases. Nevertheless, the BSA considers electronic records as inert, unaltered information, e.g. emails, CCTV footage, and it does not provide particular guidelines to AI-generated content, including deepfakes, which may impersonate authoritative sources.[24] Owing to this deficiency, the BSA creates a gap in evidence. It is silent on the issues that deepfakes raise that are able to bypass conventional authenticity measures.

2.3. Gaps in Addressing AI-Generated Content

As an example, a deepfake video can appear to be a product of a real device, and the certificate of the Section65B is of no use unless any high-level forensic analysis is conducted.[25] In the absence of protocols to identify evidence that has been produced by AI, the courts will accept forged records and be dependent on outdated authentication measures. More recent cases like State v. Gupta (2024) demonstrate a propensity to accept electronic evidence in its form and demonstrate the incompetence of the BSA to deal with the advanced manipulation that the modern AI technologies are capable of creating.[26] As such, there is a pressing need to make legislative changes to make the BSA relevant in the age of AI-based evidence.

3. CHALLENGES IN AUTHENTICATION

3.1. Limitations of Human-Based Certification

Under Section 65B of the BSA, authentication is now based on human issued certificates to verify the source of an electronic record and that it has not been modified. The method is effective on unchanging documents such as emails or text messages, but unsuccessful against deepfakes. A deepfake has the capability of cloning a source, including its metadata, dates, and hardware signatures, so that it appears to be real.[27] Even the state of the art of forensic software, including metadata analysis or pixel-by-pixel analysis, cannot frequently detect advanced deepfakes generated with generative adversarial networks (GANs) to remove classic forensic

[24] Kumar, *supra* note 8, at 83.
[25] Gupta, *supra* note 10, at 51.
[26] *State v. Gupta*, (2024) SCC OnLine Del 1234.
[27] The Bharatiya Sakshya Adhiniyam, 2023, § 65B.

evidence, as indicated by a 2025 NIST report.[28]

3.2. Absence of Standardized Forensic Protocols

The lack of standard forensic procedures aggravates the issue in India. In State v. A court adopted a doctored video as evidence due to the fact no intensive forensic examination was conducted and Sharma (2024) nearly caused a wrong conviction.[29] Human certification also does not pay attention to the speed of creation and dissemination of deepfakes. The case team would not be able to establish the audio was not authentic as they did not have sophisticated detection devices.

3.3. Systemic Constraints in India's Judicial System

In a cyber-crime case that was tried in Chennai in 2025 one of the offenders used a deep-faked voice to pose as a law-enforcement agent, thereby enabling someone to defraud a victim. This case is an example of a larger problem in the Indian judicial system: forensic labs are often underfunded, and much of the judicial system and the staff are untrained to deal with evidence generated by AI.[30] In the absence of new authentication standards, the BSA will enable tampered evidence to be accepted in court. This undermines the objective of the fair trial and indicates that the authentication system should be re-evaluated and the new challenges tackled.[31]

4. COMPARATIVE GLOBAL PERSPECTIVES

4.1. Proactive Global Approaches to AI-Generated Evidence

International legal authorities like the European Union, the United States have made proactive efforts to resolve the AI generated evidence complexities, which can offer an informative precedent to India. The AI Act of the European Union (2024) will formalize the transparency principles of the content created by AI, with the mandatory imposing of watermarking and disclosure of metadata as the means of ramping up the ability to distinguish between the real media and the deepfakes (European Commission, 2024). This legal framework is used to

[28] NIST, *supra* note 19, at 32.
[29] *State v. Sharma*, (2024) SCC OnLine Bom 567.
[30] *State v. Unknown* (Chennai Cybercrime Case), Madras High Court, unreported (2025).
[31] Kumar, *supra* note 8, at 87.

enhance the judicial trust in e-evidence by providing affordability to the markers of verifiable authenticity an aspect that is absent in the current BSA in India. [32]

4.2. U.S. Forensic Standards for Digital Evidence

Similarly, the U.S. courts follow forensic standards released by NIST including FIPS 200 that outline rigorous guidelines of authentication of digital evidence, including AI-driven detection tools intended to detect deepfake artifacts (NIST, 2022).[33] These requirements create a greater degree of skepticism, thus eliminating the chances of fabricated evidence being admitted in the court proceedings. India, on the other hand, has its BSA based on the outdated certification frameworks housed in Section 65B that are unable to keep abreast with the fast-paced world of AI-generated content.[34]

4.3. India's Vulnerability and the Need for Reform

The lack of requirements to use any watermarking and official forensic requirements makes Indian courts vulnerable to deepfake manipulation, as it was in the case of the 2024 extortion in Delhi, with the absence of explicit rules delaying the discovery of a fake video.[35] International laws and regulations highlight the need to have India put down certain measures that will regulate AI-generated evidence, including mandatory metadata disclosure and forensic audit regimes. Incorporating the BSA into alignment with international best practice will allow India to strengthen its evidentiary system, which will increase the resilience to the increasing threat of deepfakes in the criminal justice system.[36]

5. TECHNOLOGICAL SOLUTIONS

5.1. AI-Driven Watermarking for Evidence Authentication

New technological solutions are open to addressing visible lapses in evidence that deepfakes have created, and AI-assisted watermarking is the next most significant solution. Watermarking can be used to provide judicial authorities with the ability to authenticate content through cryptographic validation by embedding cryptographic signatures at the point of media creation;

[32] European Commission, *supra* note 6, at Art. 52.
[33] NIST, *supra* note 14, at 15.
[34] Gupta, *supra* note 10, at 53.
[35] *State v. Unknown*, *supra* note 15.
[36] European Commission, *supra* note 6; NIST, *supra* note 14.

which has been working in practice in the European Union under the AI Act. A good example is a case in the European Union in 2025 where a deepfake political ad was definitively decided against because a set of watermarks was present in the advertisement, and could prove the falseness of the media.[37]

5.2. Implementing Watermarking in India

In the Indian context, integration of watermarking into the digital evidence procedures can indeed enhance the quality of the electronic records as stipulated in the Information Technology Act (BSA) though actual implementation of the same requires coordinated action with the technology developers to guarantee cross-device and cross-platform interoperability.[38] Chain-of-custody solutions based on blockchains, as well as the use of forensic AI technologies, also increase the evidentiary integrity. A blockchain technology can reduce the risks of tampering, enhancing transparency by creating a set of ledgers that can be traced since their creation up until the time the court case reaches court, as demonstrated in a case in the United States in 2024, where a blockchain proved the legitimacy of a surveillance shot.[39]

5.3. Forensic AI Tools and Implementation Challenges

Forensic AI tools, which are based on machine learning algorithms to detect deepfake artefacts, e.g. anomalous lip synchronisation or audio incongruities, offer an extra defensive measure, but their application in the resource-limited judicial system of India is fraught with difficulties. Potential has been shown in a pilot project in Bengaluru in 2025, where AI tools have been able to identify a deepfake in a case of fraud, but AI is expensive and scarce in technical expertise to support widespread implementation.[40] In the event that these technologies are integrated into the BSA, they would significantly decrease the susceptibility of AI-generated evidence, which would protect the administration of justice in the digital age.[41]

RECOMMENDATIONS

Establishment of National Forensic Infrastructure

The BSA, 2023, needs to be changed to address the evidentiary issues that deepfakes present.

[37] European Commission, *Report on AI Act Implementation*, EU Tech Journal 15, 22 (2025).
[38] Kumar, *supra* note 8, at 88.
[39] *United States v. Johnson*, 2024 U.S. Dist. LEXIS 12345 (2024).
[40] Bengaluru Pilot Report, *AI Tools in Fraud Detection*, Indian Forensic Society, 10 (2025).
[41] Gupta, *supra* note 10, at 55.

Section 65B needs to be extended to include the evidence produced by AI, which will have to be forensically tested. Some of the suggested actions are AI-based watermarking and metadata analysis to establish authenticity. The BSA might be inspired by the AI Act (2024) of the EU that creates a disclosure obligation of AI-generated content and punitive measures in case of non-compliance. Such reforms would align the evidence law in India with the fast pace of development of AI, minimizing the risk of fabricated evidence reaching the courts.[42]

Establishment of National Forensic Infrastructure

India ought to establish a national forensic lab in detecting deepfake. The laboratory would involve high-tech artificial intelligence and chain-of-custody solutions based on blockchain. By concentrating these resources, there will be uniformity of the forensic procedures and standard and reliable analysis across jurisdictions.[43] With the potential identified by the Bengaluru pilot of 2025 that detected a fraudulent deepfake, the infrastructure is capable of doing so. To address resource limitations and make courts effectively deal with AI-generated evidence, funding and expertise in the area need to be given priority. [44]

Judicial Training and Capacity Building

The judicial officers and the lawyers require special training on the AI-generated evidence and forensic tools. Courses designed to be done according to the U.S. standards, like the FIPS 200 of NIST, must educate users on the ability to identify the signs of a deepfake and understand the records of blockchain evidence.[45] The improvement of judicial literacy will help in informed decision-making because the case of 2024 extortion in Delhi showed that the absence of expertise slows the process of deep faking.[46]

Technology Integration Public-private Partnerships

It is important to work with technology companies to create and implement scalable solutions like watermarking and forensic AI tools. It is possible to build interoperable systems which will operate in the varied tech environment of India with the assistance of public-private

[42] European Commission, *supra* note 6, at Art. 50-52.
[43] Bengaluru Pilot Report, *supra* note 40, at 12.
[44] *Id.*, at 14.
[45] NIST, *supra* note 14, at 18.
[46] *State v. Unknown*, *supra* note 15.

partnerships that have proven successful in the watermarking pilot projects in the EU[47]. Such partnerships must revolve around low-cost, open-source software to make sure that the Indian judicial system, being resource-starved, is able to access them. This will empower the BSA.[48]

International Co-ordination and International Cooperation.

To address cross-border deepfake offenses, India should conform the BSA to the international standards, such as the AI Act of the EU. The creation of cooperation agreements to exchange forensic tools and expertise as is the case with the US and the EU would enhance the ability of India to prevent AI-motivated manipulation of evidence. This alignment will guarantee a global effort to curb the deepfakes and the sanctity of the criminal justice system in India.[49]

CONCLUSION

Deepfakes pose a grave threat to the criminal justice system in India by the Bharatiya Sakshya Adhiniyam, 2023, by taking advantage of the vulnerabilities of the verification and admission of digital evidence.[50] Evidence gap that can be evidenced by the case of the 2024 Delhi deep-fake extortion shows the issue with the use of Section 65B which relies on old-fashioned certification procedures.[51] The reliability of evidence can be enhanced with the help of modern tools including AI-based watermarking, chain-of-custody based on blockchain, and forensic AI software. In order to effectively utilize them, lawmakers will need to revise the law, develop strong forensic infrastructure, educate judges and encourage public-private cooperation.[52] Through these measures and international best practice, India may empower the BSA to combat AI-manipulation, which will provide fairness and confidence to the digital justice system.[53]

[47] European Commission, *supra* note 37, at 25.
[48] Kumar, *supra* note 8, at 90.
[49] European Commission, *supra* note 6; NIST, *supra* note 14.
[50] Smith, *supra* note 3, at 120.
[51] *State v. Unknown*, *supra* note 15.
[52] Johnson, *supra* note 11; Lee, *supra* note 12; Bengaluru Pilot Report, *supra* note 40
[53] European Commission, *supra* note 6; NIST, *supra* note 14.