Jus Corpus Law Journal

Open Access Law Journal – Copyright © 2025 – ISSN 2582-7820

Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

Criminal Law in the Age of Deepfakes: A Looming Evidentiary Crisis

Vibha Rana[a]

[a]Galgotias University, Greater Noida, India

Received 07 July 2025; *Accepted* 08 August 2025; *Published* 12 August 2025

The advancement of artificial intelligence in multimedia generation has given rise to deepfakes, highly convincing audio-visual manipulations that replicate real individuals. Originally intended for entertainment, deepfakes have now infiltrated legal and criminal domains, posing a significant threat to the justice system. Their near-perfect realism makes them hard to identify, enabling their misuse as deceptive or fabricated evidence, particularly in criminal trials where digital proof is pivotal. Under Indian law, the Bharatiya Sakshya Adhiniyam (BSA) 2023, offers a broad structure for electronic evidence admissibility but fails to address synthetic media like deepfakes specifically. This gap creates a critical evidentiary void, undermining fairness, authenticity, and chain of custody, and jeopardising the presumption of innocence and the right to a fair trial under Article 21 of the Constitution. This paper examines the threats deepfakes pose to evidentiary standards in Indian criminal law. It evaluates the shortcomings of the current legal framework, including the BSA, Bharatiya Nyaya Sanhita (BNS), and the IT Act, in tackling sophisticated AI-generated manipulations. A comparative study with jurisdictions like the U.S. and China provides insights for potential solutions. The article concludes with reform recommendations, such as AI-driven forensic tools, legislative updates, and judicial safeguards, to fortify Indian courts against synthetic evidence.

Keywords: *deepfakes, criminal justice, evidence law, chain of custody, judicial reform.*

INTRODUCTION

In today's rapidly evolving digital age, visual and auditory evidence once considered irrefutable can no longer be inherently trusted. The rapid advancement of Artificial Intelligence (AI) has ushered in an era where hyper-realistic forgeries, known as deepfakes, can be seamlessly generated using sophisticated machine learning techniques such as Generative Adversarial Networks (GANs).[1] What began as a technological novelty has now morphed into a potent tool for malicious actors, enabling everything from revenge[2] pornography and political disinformation to financial fraud[3] and the deliberate tampering with criminal evidence.[4] As these AI-generated fabrications grow increasingly indistinguishable from genuine content, their potential to disrupt legal systems, manipulate public perception, and erode trust in digital media has become a pressing global concern.

India's criminal justice system, like many others, has come to rely heavily on digital evidence—ranging from CCTV footage and call recordings to social media posts and electronic documents. However, the infiltration of deepfakes into legal proceedings poses an unprecedented challenge, threatening to undermine fair trials, violate the rights of the accused, and distort the very foundations of justice. Despite these risks, India's newly enacted Bharatiya Sakshya Adhiniyam (BSA) 2023[5], which replaces the archaic Indian Evidence Act, 1872, provides only a generic framework for electronic evidence without explicitly addressing the unique threats posed by AI-generated forgeries. Similarly, the Bharatiya Nyaya Sanhita (BNS), 2023[6], which supersedes the Indian Penal Code (IPC)[7], fails to specifically criminalise the creation or malicious use of deepfake-based evidence, leaving a significant gap in the legal framework.

[1] Ian Goodfellow et al., 'Generative Adversarial Networks' (2014) Machine Learning <https://arxiv.org/abs/1406.2661> accessed 01 July 2025

[2] Paul Mozur, 'A Genocide Incited on Facebook, With Posts from Myanmar's Military' *The New York Times* (15 October 2018) <https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.htm> accessed 01 July 2025

[3] Jesse Damiani, 'A Voice Deepfake Was Used to Scam a CEO Out of $243,000' *Forbes* (03 September 2019) <https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-2> accessed 01 July 2025

[4] Bobby Chesney and Danielle Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107(1) California Law Review 175 <https://doi.org/10.15779/Z38RV0D15J> accessed 01 July 2025

[5] Bharatiya Sakshya Adhiniyam 2023

[6] Bharatiya Nyaya Sanhita 2023

[7] Indian Penal Code 1860

This article examines how deepfakes erode fundamental legal principles—authenticity, chain of custody, and evidentiary reliability—while exploring the inadequacies in India's current legislative and judicial response. It further conducts a comparative analysis of global approaches to regulating synthetic media, highlighting best practices from jurisdictions that have taken proactive measures.[8] Finally, the article proposes critical reforms, including AI-powered forensic verification tools, legislative amendments to criminalise deepfake manipulation, and judicial safeguards to ensure the admissibility of only verifiable digital evidence. By addressing these challenges head-on, India's legal system can safeguard the integrity of criminal proceedings in an era where reality itself can be artificially constructed.

THE DEEPFAKE THREAT TO CRIMINAL JUSTICE

Deepfakes are synthetic media generated using advanced artificial intelligence techniques such as Generative Adversarial Networks (GANs). These technologies enable the hyper-realistic manipulation of audio, video, and image content, allowing the creation of fraudulent media that is nearly indistinguishable from authentic recordings. While initially developed for entertainment or satire, deepfakes have now emerged as a potent threat to criminal justice systems worldwide.

Global Threat Landscape: The misuse of deepfake technology has already demonstrated alarming implications across multiple jurisdictions. In the United Kingdom, fraudsters used a deepfake voice clone of a CEO to impersonate him during a phone call, successfully deceiving a subordinate into transferring $243,000 to a fraudulent account. Similarly, in India, morphed political videos—including manipulated speeches of party leaders—have repeatedly gone viral during election periods, spreading disinformation and damaging reputations. Beyond financial and political exploitation, a disturbing trend has emerged in the form of non-consensual deepfake pornography, which disproportionately targets women activists and journalists. Such malicious use not only violates personal dignity but also erodes public trust and credibility, highlighting the urgent need for legal and technological countermeasures.

[8] 'Report Summary on A Free and Fair Digital Economy' (*PRS India*) <https://prsindia.org/policy/report-summaries/free-and-fair-digital-economy> accessed 01 July 2025

Specific Threats to Criminal Trials: Within the courtroom, deepfakes create an evidentiary minefield, threatening the integrity of judicial processes. Their ability to simulate human behaviour with alarming precision enables the fabrication of false confessions or statements attributed to an accused or witness, fundamentally distorting the evidentiary foundation of a case. Even more dangerously, deepfakes can place individuals at fabricated crime scenes, directly violating their right to a presumption of innocence under Article 21 of the Indian Constitution.[9] The manipulation of crucial digital evidence—such as CCTV footage, call recordings, GPS logs, and forensic voice samples—poses an additional challenge, as these elements often form the backbone of modern prosecutions. Furthermore, the mere possibility of deepfake tampering allows defence counsel to cast doubt on even authentic recordings, arguing that they may have been synthetically altered. This erodes trust in digital evidence altogether, blurring the line between truth and deception and complicating the pursuit of justice.[10]

Impact on Fair Trial and Due Process: The growing dependence of India's criminal justice system on electronic and audiovisual evidence - especially in urban crime investigations and terrorism cases - faces unprecedented challenges with the advent of deepfake technology.[11] These hyper-realistic digital forgeries threaten to fundamentally disrupt judicial processes in multiple ways: they cast doubt on the reliability of digital evidence that courts have come to trust; create systemic bottlenecks as overburdened forensic labs struggle to authenticate questionable content; and unfairly disadvantage defendants who typically lack the resources to contest sophisticated media manipulations. Perhaps most alarmingly, this technology undermines the very foundation of justice by enabling fabricated evidence to potentially determine case outcomes.

This emerging crisis exposes dangerous gaps in India's legal framework. Without proper legislative protections and adequate technological countermeasures, the judiciary remains

[9] Constitution of India 1950, art 21

[10] Dr. Deepti Singla, 'NAVIGATING DEEPFAKES IN INDIAN CRIMINAL LAW: NAVIGATING EVIDENTIARY AND LEGAL REFORMS UNDER THE BSA AND BNS, 2023' (2025) 5(3) Indian Journal of Integrated Research in Law <https://ijirl.com/wp-content/uploads/2025/06/NAVIGATING-DEEPFAKES-IN-INDIAN-CRIMINAL-LAW-NAVIGATING-EVIDENTIARY-AND-LEGAL-REFORMS-UNDER-THE-BSA-AND-BNS-2023.pdf> accessed 01 July 2025

[11] Harshvardhan Mudgal, 'The deepfake dilemma: Detection and decree' *Bar & Bench* (18 November 2023) <https://www.barandbench.com/columns/deepfake-dilemma-detection-and-desirability> accessed 01 July 2025

vulnerable to deception by artificially-generated 'evidence' that may be virtually indistinguishable from reality. When synthetic media can be presented as factual proof, the fundamental principles of justice - built upon verifiable truth and authentic evidence - face existential threats. The criminal justice system now stands at a critical juncture, where immediate action is needed to preserve its integrity against this new form of digital manipulation that could erode public trust in legal institutions. The time to develop robust safeguards against deepfake evidence is now, before this technology becomes weaponised to distort justice on a systemic level.

THE INDIAN LEGAL FRAMEWORK AND DEEPFAKES

Bharatiya Sakshya Adhiniyam (BSA) 2023: The Bharatiya Sakshya Adhiniyam (BSA), 2023[12], which supersedes relevant provisions of the Indian Evidence Act, 1872[13], establishes the legal framework for admitting digital and electronic records as evidence. However, it fails to adequately address the challenges posed by AI-generated content. While Section 63[14] retains the certificate requirement for digital evidence admissibility (previously under Section 65B of the IEA), it does not provide specific guidelines for handling AI-synthesised or manipulated media. This legislative silence creates a critical gap, as courts may inadvertently admit deepfakes or other synthetic forgeries without proper scrutiny, potentially leading to miscarriages of justice. Moreover, the absence of mandatory forensic protocols for verifying audiovisual evidence leaves the justice system vulnerable in an era where generative AI can produce highly convincing fabrications. As digital evidence becomes increasingly central to judicial proceedings, this regulatory vacuum undermines the reliability of court outcomes and exposes the legal system to manipulation through technologically sophisticated means. The BSA's failure to incorporate safeguards against AI-altered content represents a significant oversight that could compromise the integrity of India's justice delivery mechanism.[15]

Information Technology Act 2000: The Information Technology Act, 2000, designed to combat conventional cybercrimes, remains woefully inadequate in addressing the

[12] Bharatiya Sakshya Adhiniyam 2023

[13] Indian Evidence Act 1872

[14] Bharatiya Sakshya Adhiniyam 2023, s 63

[15] Vaishnavi Singh and Abhijeet Raj, 'DISSECTING THE CONUNDRUM OF DEEPFAKE TECHNOLOGY AND ARTIFICIAL INTELLIGENCE IN LIGHT OF THE NEW PENAL LAWS OF INDIA' (*NLIU-CLT*) <https://clt.nliu.ac.in/?p=1097> accessed 01 July 2025

sophisticated challenges posed by AI-generated manipulations. While Section 66E penalises violations of bodily privacy through unauthorised image capture, its provisions fail to account for synthetic recreations or digital impersonations enabled by deepfake technology. Similarly, Sections 67 and 67A,[16] which criminalise the transmission of obscene or sexually explicit material, make no distinction between authentic and AI-generated content—leaving victims of deepfake pornography or defamation without specific legal remedies. Most critically, the Act contains no dedicated provisions to counter the creation, dissemination, or malicious use of deepfakes for impersonation, reputational damage, or evidence tampering in judicial proceedings. As AI tools become increasingly accessible to the public, this legislative gap enables new forms of digital deception to flourish unchecked. The rapid evolution of synthetic media demands urgent amendments to the IT Act, ensuring it can effectively combat emerging threats to privacy, security, and the integrity of legal processes in the age of artificial intelligence.[17]

Bharatiya Nyaya Sanhita (BNS) 2023: The Bharatiya Nyaya Sanhita (BNS), 2023, while representing a modernisation of India's penal framework, critically fails to address the growing threat posed by AI-generated deepfakes. Despite its progressive intent, the new criminal code contains no specific provisions criminalising the creation or malicious use of synthetic media for fraud, defamation, or judicial manipulation. This legislative gap leaves victims of deepfake fabrication—whether those falsely implicated in crimes or subjected to reputational harm—without clear legal recourse. Furthermore, the BNS[18] lacks essential procedural safeguards to help courts and investigators authenticate digital evidence, rendering the justice system vulnerable to technologically sophisticated manipulation. As deepfake technology becomes increasingly indistinguishable from reality, this statutory silence creates a dangerous void in India's criminal jurisprudence, potentially enabling bad actors to exploit synthetic media for unlawful purposes with impunity. The absence of dedicated offences and verification protocols in the BNS represents a significant oversight

[16] Information Technology Act 2000, ss 66E, 67, 67A

[17] Chaksham Kumar Das, 'Deepfakes and Indian Law: Is the IT Act Enough in the Age of AI?' (*Century Law Firm*) <https://www.centurylawfirm.in/blog/deepfakes-and-indian-law-is-the-it-act-enough-in-the-age-of-ai/> accessed 01 July 2025

[18] Bharatiya Nyaya Sanhita 2023

that must be urgently addressed to protect both individual rights and the integrity of legal proceedings in the digital age.[19]

Constitutional Implications: The proliferation of deepfakes in judicial and quasi-judicial proceedings raises significant constitutional concerns that demand urgent attention. At its core, the unregulated admission of AI-fabricated evidence constitutes a direct violation of Article 21's guarantee of the right to a fair trial and personal liberty.[20] When courts admit synthetic media without rigorous authentication protocols, they risk basing life-altering judgments on potentially fabricated evidence, thereby compromising fundamental due process rights. This technological threat creates a two-fold constitutional crisis: first, by exposing individuals to prosecution or reputational damage through unverifiable synthetic evidence; and second, by eroding the foundational principles of natural justice that require decisions to be based on verifiable facts. Perhaps most alarmingly, the very credibility of the judicial system hangs in the balance - as deepfakes gain sophistication, they threaten to create a pervasive 'liar's dividend' where even genuine evidence may be dismissed as potentially fabricated.[21] This erosion of evidentiary certainty strikes at the heart of constitutional governance, where public trust in judicial outcomes forms the bedrock of the rule of law.[22] Without immediate safeguards, the justice system risks becoming complicit in the violation of the constitutional rights it was designed to protect, as synthetic media could systematically distort truth-finding processes and undermine the integrity of legal outcomes.[23]

COMPARATIVE JURISPRUDENCE: GLOBAL LEGAL RESPONSES TO DEEPFAKES

In addressing the legal challenges posed by deepfakes, several jurisdictions have adopted distinct legislative and judicial strategies. The comparative approaches of the United States, China, and the European Union highlight both innovative regulatory models and areas of potential reform for India.

[19] Tasnimul Hassan Md, 'The Perils and Promises of Artificial Intelligence in Criminal Sentencing' (2024) 19(2) Indian Journal of Law and Technology <https://repository.nls.ac.in/ijlt/vol19/iss2/1> accessed 01 July 2025

[20] Constitution of India 1950, art 21

[21] Lawrence Lessig, *Code: And Other Laws of Cyberspace* (Basic Books 2006) 89

[22] Constitution of India 1950, art 14

[23] Shinu Vig, 'Regulating Deepfakes: An Indian perspective' (2024) 17(3) Journal of Strategic Security <https://digitalcommons.usf.edu/jss/vol17/iss3/5/> accessed 01 July 2025

United States: The United States has developed a comprehensive legal and technological framework to address the challenges posed by deepfakes. At the federal level, Rule 902(14) of the Federal Rules of Evidence streamlines the authentication process for electronic evidence by allowing self-authentication through qualified certification, reducing procedural delays while maintaining evidentiary integrity.[24] U.S. courts have also institutionalised digital forensic analysis to verify the chain of custody and authenticity of audiovisual evidence. Federal agencies and state prosecutors actively employ AI-assisted forensic tools to detect synthetic manipulations, creating a robust system for identifying deepfakes in judicial proceedings.

Complementing these federal measures, several states have enacted targeted legislation to combat malicious deepfake use. California and Texas have emerged as leaders, passing laws[25] that specifically criminalise deepfakes in political campaigns (California AB 730[26]), non-consensual pornography (Texas HB 2984[27]), and identity fraud cases. This multi-layered approach - combining federal evidentiary standards with state-level criminal prohibitions and advanced forensic capabilities - provides a balanced model for addressing both the evidentiary and criminal aspects of deepfake technology. The U.S. system demonstrates how technological adaptation, procedural reforms, and specialised legislation can work together to mitigate the risks posed by synthetic media while preserving judicial efficiency.

China: China has implemented a stringent regulatory framework to govern synthetic media technologies, prioritising state oversight and compliance. A key component of this approach is the mandatory disclosure policy introduced in 2020, which requires all AI-generated or deepfake content to bear clear watermarks or labels identifying its synthetic nature.[28] This measure specifically targets the risks of misinformation, impersonation, and public deception by ensuring transparency in digital content. Beyond disclosure rules, China has strengthened its Criminal Law to impose harsher penalties for malicious uses of deepfake technology,

[24] Federal Rules of Evidence, r 902(14)

[25] Mohamed Chawki, 'Navigating legal challenges of deepfakes in the American context: a call to action' (2024) 11(1) Cogent Engineering <https://doi.org/10.1080/23311916.2024.2320971> accessed 01 July 2025

[26] California Assembly Bill 730 2019; California Elections Code 2020, s 20010

[27] Texas House Bill 2984 2019

[28] Laney Zhang, 'China: Provisions on Deep Synthesis Technology Enter into Effect' (*The Library of Congress*, 26 April 2023) <https://www.loc.gov/item/global-legal-monitor/2023-04-25/china-provisions-on-deep-synthesis-technology-enter-into-effect/> accessed 01 July 2025

including defamation, fraud, and the spread of fake news. These legal provisions serve as strong deterrents against the weaponisation of synthetic media.[29]

The Cyberspace Administration of China (CAC) plays a proactive role in enforcing these regulations by closely monitoring AI-generated content platforms and demanding algorithmic transparency. By requiring tech companies to disclose how their AI models function, the government ensures accountability and ethical compliance in the development and distribution of synthetic media. This dual strategy—combining strict legal consequences with technological oversight—reflects China's pre-emptive approach to mitigating the societal risks posed by deepfakes.[30] Rather than reacting to misuse after the fact, China's regulatory model emphasises early intervention, deterring malicious actors while maintaining tight control over the ethical deployment of AI technologies.[31]

European Union: The European Union has developed a comprehensive approach to regulating deepfake technology, grounded in its strong commitment to data protection, digital integrity, and fundamental human rights.[32] At the core of this framework is the General Data Protection Regulation (GDPR)[33], which treats unauthorised deepfake content featuring personal likenesses as a violation of privacy rights, subject to stringent penalties. This legal stance reinforces the principle of consent in digital spaces, ensuring individuals retain control over their biometric data. Beyond data protection, EU member states are actively enhancing their forensic capabilities through specialised digital labs and AI-detection task forces, enabling judicial systems to reliably authenticate digital evidence and identify synthetic manipulations.

The proposed Artificial Intelligence Act further strengthens this regulatory landscape by introducing a risk-based classification system that designates harmful or deceptive AI applications, including deepfakes, as 'high-risk' technologies subject to strict oversight. This forward-looking legislation aims to pre-emptively curb malicious uses of synthetic media

[29] Criminal Law of the People's Republic of China 1979, arts 246, 253, and 286

[30] Jiang Xinyi, 'China Proposes Mandatory Labeling of AI-Generated Content' *Sixth Tone* (24 September 2024) <https://www.sixthtone.com/news/1015923> accessed 01 July 2025

[31] Yuqi Wang and Jiaxin Li, 'China's Emerging Data Governance Framework: Implications For MNCs' (*APCO*, 20 April 2022) <https://apcoworldwide.com/blog/chinas-emerging-data-governance-framework-implications-for-mncs/> accessed 01 July 2025

[32] General Data Protection Regulation 2016, arts 4(1) and 6

[33] General Data Protection Regulation 2016

while promoting ethical AI development.[34] The EU's rights-based model, which prioritises human dignity, technological accountability, and procedural safeguards, aligns closely with India's constitutional protections under Article 21.[35] By balancing innovation with fundamental freedoms, the European approach offers valuable insights for jurisdictions seeking to combat deepfake threats without compromising democratic values or due process rights.[36]

ADMISSIBILITY, CHAIN OF CUSTODY, AND BURDEN OF PROOF IN THE AGE OF DEEPFAKES

The increasing prevalence of deepfakes in digital litigation poses critical challenges to the evidentiary framework of Indian law. These challenges relate directly to three key pillars of evidence law: admissibility, chain of custody, and the burden of proof.

Admissibility: Under Section 63 of the Bharatiya Sakshya Adhiniyam (BSA) 2023[37], electronic records remain admissible in court only if accompanied by a certification of authenticity—a provision carried forward from Section 65B[38] of the Indian Evidence Act. However, this safeguard is vulnerable to exploitation by deepfake technology, which can alter content at the source level.[39] Even certified evidence may be compromised, as the certification process verifies only the storage medium's integrity, not the originality or truthfulness of the content itself.

This loophole highlights a critical gap in India's legal framework. While the BSA ensures procedural compliance for digital evidence, it lacks mechanisms to detect AI-generated forgeries embedded within certified records. As deepfakes grow more sophisticated, the current admissibility standards risk admitting manipulated content, undermining judicial

[34] Mateusz Labuz, 'Deep fakes and the Artificial Intelligence Act—An important signal or a missed opportunity?' (2024) 16(4) Policy & Internet <https://doi.org/10.1002/poi3.406> accessed 01 July 2025

[35] 'NAVIGATING THE DEEPFAKE DILEMMA: LEGAL PERSPECTIVES FROM INDIA AND THE EU AI ACT' (*With Law*) <https://www.withlaw.co/blog/Technology-and-Innovation-1/NAVIGATING-THE-DEEPFAKE-DILEMMA:-LEGAL-PERSPECTIVES-FROM-INDIA-AND-THE-EU-AI-ACT> accessed 01 July 2025

[36] 'Strategic communication and countering foreign information manipulation and interference' (*European Commission*) <https://commission.europa.eu/topics/countering-information-manipulation_en> accessed 01 July 2025

[37] Bharatiya Sakshya Adhiniyam 2023, s 63

[38] Indian Evidence Act 1872, s 65B

[39] Dr. Ajit Singh and Dr. Pawan Kumar, 'Digital Evidence and Deepfake: A Challenge to Criminal Justice System in India' (2025) 12(8) JETIR <https://www.jetir.org/papers/JETIR2508273.pdf> accessed 01 July 2025

reliability. Without updates to address synthetic media, the certification requirement becomes a procedural formality rather than a guarantee of authenticity.

Chain of Custody: Maintaining a clear chain of custody is crucial to ensuring the evidentiary value of digital content, but deepfakes present unique challenges. AI-generated alterations can be introduced at any point during transmission or storage, breaking the chain of authenticity. Without a secure, tamper-proof system—such as blockchain-based preservation or metadata tracking—courts lack a reliable way to verify that the presented content matches the original recording.[40] Additionally, digital footprints and timestamps can be manipulated, making it nearly impossible to trace the origin or modifications of evidence without advanced forensic tools. Unless a robust technological framework is adopted, the credibility of electronic evidence remains vulnerable to manipulation.[41]

Burden of Proof: The infiltration of deepfakes into judicial processes has complicated the application of the burden of proof. When deepfake evidence is presented, the onus often shifts to the accused to disprove its authenticity, particularly in the absence of clear forensic standards. This undermines the presumption of innocence, a fundamental principle under Article 21[42] of the Constitution. Moreover, resource-constrained defendants, especially those without legal or technical expertise, face significant challenges in contesting synthetic evidence, depriving them of a fair opportunity to defend themselves.

The lack of institutional support, such as public access to certified forensic experts or court-appointed technical evaluators, exacerbates this imbalance. The evidentiary burden falls disproportionately on marginalised or indigent individuals, violating the principle of equality before the law (Article 14)[43]. Allowing unverified synthetic content to influence judicial outcomes not only erodes fairness but also threatens the integrity of the justice system as a whole.

[40] Anuska Jain, 'Securing the Links: A Framework for Chain of Custody in Indian Courts' *SCC Online* (30 November 2024) <https://www.scconline.com/blog/post/2024/11/30/securing-the-links-a-framework-for-chain-of-custody-in-indian-courts/> accessed 01 July 2025

[41] 'BLOCKCHAIN EVIDENCE & ADMISSIBILITY IN INDIA' (*Sud and Sud*, 03 May 2025) <https://www.sudsud.in/post/artificially-intelligent-entities-as-legal-persons-navigating-the-frontiers-of-legal-personhood-in> accessed 01 July 2025

[42] Constitution of India 1950, art 21

[43] Constitution of India 1950, art 14

KEY CASE LAWS ON ELECTRONIC EVIDENCE AND DEEPFAKES

1. Anvar P.V. v P.K. Basheer:[44]

Facts: Anvar P.V., a candidate in the 2011 Kerala Assembly elections, filed an election petition against P.K. Basheer, alleging corrupt practices, including using recorded songs and speeches to influence voters. Anvar sought to admit CDs as evidence without submitting a certificate under Section 65B[45].

Issues:

1. Whether electronic evidence (CDs) could be admitted without a Section 65B certificate?
2. What are the conditions under which electronic records are admissible?

Judgment: The Supreme Court overruled the earlier position taken in *State (NCT of Delhi) v Navjot Sandhu* (2005)[46] and held that:

- A certificate prescribed under section 65B is mandatory for the admissibility of electronic evidence.
- Oral evidence or cross-examination cannot substitute for the certificate requirement.
- Original electronic records (e.g., hard drives) are not needed if proper certification is provided.

Relevance to Deepfakes: This case lays the procedural foundation for admitting digital evidence, but does not address manipulation at the source, making it inadequate against AI-generated falsified content like deepfakes.

[44] *Anvar P.V. v P.K. Basheer* (2014) 10 SCC 473

[45] Indian Evidence Act 1872, s 65B

[46] *State (NCT of Delhi) v Navjot Sandhu @ Afsan Guru* (2005) 11 SCC 600

2. Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal:[47]

Facts: The petitioner challenged the admissibility of electronic evidence submitted in the form of WhatsApp messages and call data records, which were not accompanied by a Section 65B[48] certificate.

Issues:

1. Is a Section 65B certificate always mandatory for the admissibility of electronic evidence?
2. Are there exceptions to this requirement?

Judgment: A three-judge bench of the Supreme Court held:

- The requirement of a Section 65B certificate is mandatory, and there are no exceptions unless the original device is produced in court.
- If the certificate cannot be produced, the party must explain why and attempt to summon the responsible authority under Section 91 CrPC[49].

Relevance to Deepfakes: The judgment reiterates procedural integrity but does not ensure content authenticity—a major concern in the era of AI-manipulated data. It emphasises compliance but lacks a framework to detect deepfakes or forged content.

3. State v Mohd. Afzal & Ors (Parliament Attack Case):[50]

Facts: This high-profile case involved the December 13, 2001 attack on the Indian Parliament. The accused, including Mohd. Afzal Guru was convicted based largely on electronic evidence such as CD recordings of phone conversations, laptop data, and call records.

Issues:

1. To what extent can electronic and telephonic evidence be relied upon to secure a conviction?

[47] *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal* (2020) 7 SCC 1

[48] Indian Evidence Act 1872, s 65B

[49] Code of Criminal Procedure 1973, s 91

[50] *State v Mohd Afzal & Ors* 2003 (71) DRJ 178

2. What are the safeguards required to ensure such evidence is not tampered with?

Judgment: The Delhi High Court accepted the electronic evidence as credible, leading to convictions, including the death penalty. The judgment stated that there was no suggestion of fabrication, and the chain of custody was presumed to be intact.

Relevance to Deepfakes: This case demonstrates how heavily courts can rely on electronic records, even in capital punishment cases. However, at the time, there was minimal scrutiny of manipulation risks—a weakness that would be catastrophic if deepfakes were involved.

4. United States v Schaffer:[51]

Facts: In this U.S. federal case, the defendant challenged the admissibility of computer-generated records (accounting data) in a fraud case, arguing the system could have been tampered with or malfunctioned.

Issues:

1. Is the proponent of electronic evidence required to prove the reliability of the system that generated or stored the data?
2. What threshold of authenticity is required?

Judgment: The D.C. Circuit Court held:

- The burden is on the party presenting digital evidence to show that the system used to create, store, and retrieve the data was reliable and not vulnerable to tampering.
- The court emphasised the need for a chain of custody and system integrity before evidence can be admitted.[52]

PROPOSED REFORMS: BUILDING A LEGAL FRAMEWORK TO COMBAT DEEPFAKE THREATS

To effectively address the legal, technological, and ethical challenges posed by deepfakes, India must undertake a multi-dimensional reform strategy. These reforms should be

[51] *United States v Schaffer* [2001] 240 F.3d 35

[52] Lester Obbayi, 'Computer forensics: Chain of custody' (*Infosec*, 06 July 2019) <https://www.infosecinstitute.com/resources/digital-forensics/computer-forensics-chain-custody/> accessed 01 July 2025

grounded in statutory amendments, technological innovation, judicial capacity-building, and robust forensic infrastructure.

Statutory and Legislative Reforms: The existing legal framework, including the Bharatiya Sakshya Adhiniyam (BSA) 2023[53] and the Information Technology Act 2000,[54] requires urgent updates to address the challenges posed by synthetic media. Dedicated provisions must be introduced in the BSA to regulate the admissibility of AI-generated content, with precise definitions of deepfakes and standardised evidentiary criteria. Additionally, courts should be mandated to appoint certified AI and digital forensic experts, particularly in cases involving disputed audio-visual evidence, to ensure technical scrutiny.

To further safeguard judicial integrity, a rebuttable presumption against the reliability of electronic media should be established unless authenticated through verified forensic methods or blockchain-based protocols.[55] These legislative reforms are critical to prevent courts from relying on outdated evidentiary principles when adjudicating cases involving advanced technological manipulation. Without such updates, the legal system risks being ill-equipped to handle the growing threat of AI-generated deception.[56]

Integration of Advanced Technology: To strengthen its evidentiary framework, India must embrace technological modernisation through strategic initiatives. This includes collaborating with AI research institutions and forensic laboratories to develop indigenous deepfake detection tools capable of identifying, analysing, and verifying manipulated content in real time.[57] Such solutions would empower courts and investigative agencies to assess the authenticity of digital evidence more effectively.

Additionally, implementing blockchain-based systems for tracking digital evidence—from creation to preservation—would ensure an immutable chain of custody, enhancing

[53] Bharatiya Sakshya Adhiniyam 2023

[54] Information Technology Act 2000

[55] Bhavya Singh, 'Deepfakes and the Law: Regulating Synthetic Media in the Age of AI' (*Lawful Legal*, 11 June 2025) <https://lawfullegal.in/deepfakes-and-the-law-regulating-synthetic-media-in-the-age-of-ai/> accessed 01 July 2025

[56] Ujwal Jalali, 'Dedicated laws on AI, Deepfake Need of the Hour: Advocate Pawan Duggal' *The New Indian Express* (26 June 2024) <https://www.newindianexpress.com/cities/delhi/2024/Jan/26/dedicated-laws-on-ai-deepfake-need-of-the-hour-advocate-pawan-duggal> accessed 01 July 2025

[57] Dr. Kuldeep Singh Panwar and Nilutpal Deb Roy, 'RISING MENACE OF DEEPFAKES WITH THE HELP OF AI: LEGAL IMPLICATIONS IN INDIA' (2024) 4(3) Indian Journal of Integrated Research in Law <https://ijirl.com/wp-content/uploads/2024/05/RISING-MENACE-OF-DEEPFAKES-WITH-THE-HELP-OF-AI-LEGAL-IMPLICATIONS-IN-INDIA.pdf> accessed 01 July 2025

transparency and reliability.[58] Public-private partnerships should also be fostered to build secure, scalable platforms for storing and authenticating digital records used in legal proceedings. Together, these measures would significantly improve the verifiability and trustworthiness of digital evidence in judicial processes.[59]

Judicial Training and Procedural Guidelines: To effectively address the challenges posed by AI-generated evidence, systemic reforms must enhance judicial capabilities through targeted capacity-building.[60] The National Judicial Academy and State Judicial Academies should implement mandatory training programs to equip judges, prosecutors, and court staff with technical skills to identify and assess AI-manipulated content. These programs should incorporate hands-on workshops demonstrating deepfake creation methods and detection tools to develop practical expertise.

Concurrently, High Courts must issue standardised Practice Directions establishing uniform evidentiary protocols for AI-altered content, including authentication requirements and burden-shifting frameworks. Complementing this, the development of specialised bench books containing digital forensic case studies, verification checklists, and evidentiary red flags would provide crucial reference material.[61] Such comprehensive measures would strengthen judicial competence in evaluating sophisticated digital evidence while safeguarding fundamental due process protections in an era of rapidly evolving synthetic media technologies.[62]

[58]'IDENTIFYING EMERGING CYBER SECURITY THREATS AND CHALLENGES FOR 2030' (*ENISA*, March 2023) <https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Foresight%20Cybersecurity%20Threats%20for%202030.pdf> accessed 01 July 2025

[59] 'OECD AI Principles overview' (*OECD AI Policy Observatory*) <https://oecd.ai/en/ai-principles> accessed 01 July 2025

[60] Trishita Chatterjee, 'ADMISSIBILITY OF AI-REVIEWED DIGITAL EVIDENCE IN LEGAL INVESTIGATIONS' (2025) 5(2) Indian Journal of Integrated Research in Law <https://ijirl.com/wp-content/uploads/2025/04/ADMISSIBILITY-OF-AI-REVIEWED-DIGITAL-EVIDENCE-IN-LEGAL-INVESTIGATIONS.pdf> accessed 01 July 2025

[61] Sakshi Tripathi, 'AI-Generated Evidence in Indian Courts: Admissibility and Legal Challenges' (*Law Jurist*, 02 July 2025) <https://lawjurist.com/index.php/2025/07/02/ai-generated-evidence-in-indiancourts-admissibility-and-legal-challenges/> accessed 02 July 2025

[62] Siddharth Peter de Souza, 'AI and the Indian Judiciary: The Need for a Rights-based Approach *The Hindu Centre for Politics and Public Policy* (28 November 2024) <https://www.thehinducentre.com/incoming/ai-and-the-indian-judiciary-the-need-for-a-rights-based-approach-html-version/article68917505.ece> accessed 01 July 2025

Strengthening Forensic Infrastructure: Combating the threat of synthetic media demands substantial investment in India's forensic capabilities across all judicial tiers. The government should prioritise establishing dedicated cyber forensic units in every district and sessions court, staffed with technically proficient personnel and equipped with cutting-edge tools for detecting and analysing deepfake evidence. [63] These units would serve as first responders in evaluating contested digital evidence at the grassroots level.

Simultaneously, existing forensic science laboratories require enhanced funding and operational autonomy to modernise their infrastructure and accelerate evidentiary analysis. Creating standardised national certification programs for digital forensic experts would ensure consistent competency benchmarks while fostering inter-agency collaboration through centralised databases and knowledge-sharing platforms. Such systemic upgrades would not only improve evidentiary reliability but also create institutional barriers against the weaponisation of synthetic media in legal proceedings.[64]

CONCLUSION

Deepfakes are no longer just a technological novelty—they pose a serious threat to the constitutional guarantees of fair trial and the evidentiary integrity of judicial proceedings. In a legal system that depends on distinguishing truth from falsehood with precision, the rise of AI-generated synthetic content undermines both credibility and the burden of proof.

As India ushers in a new era with overhauled criminal statutes, the absence of explicit legal safeguards against deepfake evidence is a critical shortcoming. The justice system risks being misled by artificially generated images, audio, or videos—potentially convicting the innocent or exonerating the guilty.

To preserve the sanctity of legal processes, India must urgently adopt a holistic response—combining statutory reform, advanced technological tools, and institutional capacity-building. Only through such a forward-looking and accountable framework can we ensure

[63] 'MODERNIZATION OF FORENSIC CAPABILITIES' (*PIB Delhi*, 06 February 2024) <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2003163> accessed 01 July 2025

[64] Kaushtub Mishra and Amit Singh, 'Bridging the Gap: Integrating forensic science and legal frameworks in criminal justice' (2024) 10(12) International Journal of Applied Research <https://doi.org/10.22271/allresearch.2024.v10.i12c.12224> accessed 01 July 2025

that justice is not compromised by the illusions of artificial intelligence, and that truth in the courtroom remains anchored in authenticity, not deception.