

DEEPPAKES AND EVIDENCE LAW: REDEFINING AUTHENTICITY IN COURTS

A Critical Analysis of Electronic Evidence Admissibility Under Indian Law

Ms. Anisha Shetty¹, Ms. Pranali Rane², Ms. Mitali Manore³

¹Student, ²Student, ³Student,

¹KES' Shri Jayantilal H. Patel Law College, Mumbai- 400067, Maharashtra

Abstract

“Privacy is the constitutional core of human dignity.” — Justice D.Y. Chandrachud, in *K.S. Puttaswamy v. Union of India*.

The rapid growth of artificial intelligence, especially deepfake technology, has started to challenge the very foundations of evidence law in India. Courts have traditionally trusted audio and video recordings as strong proof of facts; however, deepfakes complicate this belief by making it possible to create highly sophisticated and realistic yet entirely fabricated content. This article critically examines the adequacy of the *Bharatiya Sakshya Adhiniyam, 2023*, especially Section 63, which governs the admissibility of electronic evidence through its certification framework. While the provision ensures that digital records are properly produced, it fails to fully address whether the content itself is real. This becomes a serious concern in cases involving deepfakes. By connecting these issues to constitutional values like privacy, dignity, and informational self-determination, as recognized in *Justice K.S. Puttaswamy v. Union of India*, the paper argues that existing evidentiary standards need to evolve. It suggests the need for stronger safeguards, including forensic verification and stricter scrutiny, to ensure that justice is not compromised in the digital age.

Keywords: Deepfakes, Electronic Evidence, *Bharatiya Sakshya Adhiniyam*, Admissibility, Right to Privacy.

1. Introduction

The rise of artificial intelligence has changed how digital content is created and distributed in ways that few anticipated. Among its more unsettling consequences is deepfake technology AI-generated audio, video, or images that can make a person appear to say or do something they never did. These fabrications can be remarkably convincing, and that is precisely what makes them legally significant.

Evidence law has traditionally placed considerable trust in audio-visual recordings. A video or photograph was understood to reflect reality, not construct it. Deepfakes disturb this assumption in a fundamental way. If footage can be manufactured with sufficient realism, then the mere existence of a recording no longer establishes that the events shown actually took place. Courts are left with a harder question than they are accustomed to asking.

India has made gradual progress in recognising electronic evidence. The *Bharatiya Sakshya Adhiniyam, 2023* (BSA) provides a framework for the admissibility of electronic records, with Section 63 establishing a certification requirement intended to verify their authenticity. This is a meaningful step, but the provision was not drafted with AI-generated synthetic media in view. Whether it can bear the weight now being placed on it is an open question.

The constitutional dimension matters too. In *Justice K.S. Puttaswamy v. Union of India*, the Supreme Court recognized privacy as a fundamental right under Article 21, rooting that right in the values of dignity, personal autonomy, and control over one's own identity. When deepfakes place words in someone's mouth or actions to their name without consent, these values are directly implicated not only as a matter of privacy law, but as a concern for how the legal system treats individuals.

This paper takes up these questions. It examines what deepfakes mean for the admissibility and authentication of digital evidence in India, considers whether the current framework is equipped to respond, and makes the case for stronger procedural safeguards to protect the reliability of electronic evidence in court.

2. Understanding Deepfake Technology

Deepfakes are a form of synthetic media which rely on artificial intelligence that allows audio, video, or images to be digitally manipulated in a highly realistic manner. The term "deepfake" is a combination of "deep learning" and "fake", referring to the use of advanced machine learning techniques to produce fabricated yet convincing content. Unlike traditional editing techniques which merely alter existing video or footage, deepfake technology can fabricate entirely new media in which individuals seem to speak or act in ways that never actually occurred. With rapid evolution of artificial intelligence tools and their increasing accessibility, the creation of such manipulated content has become easier and led to broader use in recent years.¹

The development of deepfakes takes place through machine learning systems that are trained on extensive datasets includes images, videos, or voice recordings of individuals. These systems learn patterns such as facial expressions, speech pattern, and body movements, which they then use to create realistic imitations. One of the commonly used methods is Generative Adversarial Networks (GANs). In this method, two algorithms work together in a competitive process; one generates synthetic media; while other checks whether the produced content appears as real. Through continuous changes and feedback, the system improves its ability to create highly realistic fabricated content. As a result, modern deepfakes match subtle facial movements, lip synchronization, and voice patterns, making it increasingly difficult to differentiate between authentic and manipulated content.

Even though deepfake technology can be used for appropriate purposes, such as in movies, digital art, or educational tools, it has also been increasingly misused. Lately, deepfakes have been used to spread misleading political claims, generated non-consensual explicit content, and fabricating statements or actions of well-known people. Such uses raise serious concerns as manipulated media can spread quickly through social media and digital platforms, influencing public view and likely cause reputational damage. The difficulties in recognizing which content seems genuine or manipulated further complicates the problem.

Because of the rise of deepfake technology, legal systems now face significant challenges, particularly related to digital proof. Traditionally, courts have relied on audiovisual recordings as credible forms of evidence because they seem to provide an unbiased account of events. However, smarter algorithms have made it possible to create fabricated content that always closer resemblance to genuine recordings. This shift weakens the traditional assumption that visual or audio evidence necessarily shows reality. Consequently, the increasing

¹ Chesney, R., & Citron, D. K. (2018). Deep Fakes: a looming challenge for privacy, democracy, and national security. SSRN Electronic Journal. <https://doi.org/10.2139/ssrn.3213954>

spread of deepfakes raises important questions about how courts can verify the authenticity of digital evidence and whether the existing evidentiary rules remain sufficient in the era of artificial intelligence.²

3. Legal Framework Governing Digital Content in India

Although India's digital content rules operate on statutory laws and constitutional protections, their foundation is based on older models of online interaction. As communication increasingly depend on electronic platforms, the legal system has developed frameworks to include digital information while balancing concerning with free speech and expression. While current legal mechanisms were designed to address conventional cyber activities, they struggle to adequately respond to emerging technologies such as deepfakes.

The Information Technology Act, 2000 stands as the primary legislation governing digital communication and cyber activities in India. Under this Act, electronic records and digital signatures gain legal status equivalent to traditional handwritten papers, so long as they meet defined standards.³ This recognition allows electronic material including digital documents, audio recordings, and online communication, to function as legitimate forms of information within the legal system. Though built at the turn of the century, it continues shaping how data is treated inside judicial processes today.

Beyond acknowledging electronic records, the Act also criminalizes various kinds of cyber misconduct, including identity theft, cheating by personation using computer resources, and violation of personal privacy.⁴ These provisions indirectly apply to situations involving deepfakes, such as fake videos which have impersonation or unauthorized use of a person's identity. Nevertheless, the legislation mostly addresses misuse of existing digital data rather than the creation of AI-generated audiovisual content.

Recently introduced the Digital Personal Data Protection Act, 2023 provides a framework for regulating the processing of personal data in digital world. The Act emphasis managing consent-based data and imposes obligations on entities that collect or process personal information.⁵ While its mainly concerned with data governance, the protection of personal data becomes relevant where tools such as deepfakes manipulate individual's image, voice, or identity without consent.

Constitutional protections also play an important role in regulating digital expression. Article 19 (1)(a) of the Constitution guarantees the freedom of speech and expression, which covers messages through digital platforms. The Supreme Court affirmed this principle in *Shreya Singhal v. Union of India*, where Section 66A of the Information Technology Act was struck down because of its vague restriction on online speech.⁶ The Court emphasis that limitations on digital speech and expression must fall within the specific grounds under Article 19(2)(a).

Meanwhile, concerns related to self-determination and control over personal information fall within the protection of Article 21. In *Justice K. S. Puttaswamy v. Union of India*, the Supreme Court recognized privacy

²Citron, D. K., & Chesney, R. (2018). Deepfakes and the new disinformation war. eYLS (Yale Law School). https://scholarship.law.bu.edu/shorter_works/76

³Information Technology Act, 2000, §§ 4–5 (legal recognition of electronic records and digital signatures).

⁴Information Technology Act, 2000, §§ 66C–66E.

⁵Digital Personal Data Protection Act, 2023.

⁶*Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

as a fundamental right and emphasized on the need for safeguards from intrusive use of personal data in digital environment.⁷

Even with current laws and constitutional protections, the existing legal framework mainly regulates digital communication and privacy rather than focusing on the authenticity of digital content. Because of technologies like deepfakes enable the creation of highly realistic fabricated content and recordings, courts may increasingly face challenges to assess the reliability of digital evidence.

4. Admissibility of Electronic Evidence in Indian Courts

When the BSA replaced the Indian Evidence Act, 1872 (IEA), one of its central tasks was to bring clarity to the law on electronic evidence. Section 63⁸ is the key provision here. It provides that an electronic record a video clip, a voice recording, a CCTV file, a WhatsApp message is admissible in evidence only if accompanied by a certificate signed by a person in a responsible official position relative to the device or system that produced it. That certificate must identify the record, describe the manner of its production, and confirm that the device was functioning properly and that the record was generated in the ordinary course of its operation.

This requirement is not bureaucratic formality. Digital files can be altered and circulated without leaving visible traces, and a certificate creates legal accountability it pins down a responsible person who attests, under penalty of law, that the record is what it claims to be. Section 63 is essentially a refined Section 65B of the IEA, clarified to reduce the ambiguity that had long plagued courts. But the certificate speaks only to process it confirms the machine worked correctly. It says nothing about whether the content that machine recorded is genuine.

5. Judicial Approach to Electronic Evidence

Indian jurisprudence has already grappled with issues concerning electronic evidence. In *Anvar P.V. v. P.K. Basheer*, the Supreme Court emphasized the mandatory requirement of certification for electronic records, while *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* reaffirmed the centrality of procedural safeguards in ensuring authenticity.⁹ However, these rulings were developed in a pre-deepfake context and do not fully address AI-driven manipulation.

In 2017, a nine-judge bench of the Supreme Court unanimously held in *Justice K.S. Puttaswamy v. Union of India*, that the right to privacy is a fundamental right under Article 21 of the Constitution, grounded in the deeper values of human dignity and individual autonomy. Privacy, the Court held, protects a person's capacity to control their own identity and how they are perceived by others and by the State.⁷

This has a direct bearing on deepfakes and evidence law. When a fabricated video is used in court placing words in a real person's mouth that they never spoke it does not merely threaten evidentiary accuracy. It strikes at the very interest Puttaswamy protects: the right to control the truth of one's own identity and conduct. A deepfaked confession weaponizes a person's voice and image against them in the highest-stakes arena

⁷Justice K. S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

⁸Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023, § 63 (India). BSA on IndiaCode: <https://indiacode.nic.in>

⁹*Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473; *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1. <https://indiankanoon.org/doc/1871105/>

imaginable. Reading Puttaswamy purposively, courts should treat the authentication of audio-visual evidence not as a purely procedural question but as a constitutional one. An evidentiary standard that a certified deepfake can satisfy is not merely technically deficient it is constitutionally inadequate.

6. Deepfakes and the Crisis of Authenticity in Evidence Law

To understand the scale of the threat, it helps to understand what deepfakes actually are. They are produced using generative adversarial networks (GANs) an AI architecture in which two neural networks compete, one fabricating and one detecting, until the fake is refined to the point where the detector can no longer tell it apart from genuine material. The technology can superimpose a person's face on another's body, generate realistic lip-sync to words they never spoke, or fabricate a conversation that never took place. Crucially, professional forensic examiners, without access to specialized detection software, often cannot distinguish deepfakes from authentic footage by visual inspection alone.¹⁰

Now put that inside the Section 63 framework. A party tenders a video of the accused confessing, with a fully compliant certificate the device was functioning, the file was produced regularly. The evidence clears the admissibility threshold. But the video is a deepfake. Under current law, it is in. A person's liberty or their family may hinge on whether anyone in the courtroom has the tools and mandate to look beyond that certificate and ask whether the content is actually real.¹¹ This is a structural blind spot a framework never designed for this kind of threat.

The core problem is that Section 63 conflates two entirely different questions: whether a record was properly produced, and whether its content is authentic. The certificate answers the first. The second is what we are watching real, or was it fabricated? is left almost entirely open. That is the gap deepfake technology exploits.

7. Comparative Legal Responses to Deepfakes

The emergence of deepfakes has raised significant legal concerns across jurisdictions, demonstrating that the issue is not confined to India but is inherently global in nature. Different legal systems have responded in varied ways, reflecting their constitutional values and regulatory priorities.

In the United States, the legal approach to deepfakes remains fragmented. There is no comprehensive federal legislation specifically governing deepfakes; instead, regulation is largely state-driven and issue-specific. States such as California and Texas have enacted laws targeting particular harms. For example, California prohibits the use of deceptive deepfakes in political campaigns within a specified period before elections and provides civil remedies against non-consensual deepfake pornography.¹² At the federal level, legislative proposals such as the DEEPFAKES Accountability Act seek to introduce mandatory labelling of synthetic media, though these efforts remain limited in scope.¹³ A key constraint in the U.S. framework is the strong

¹⁰Farid, H. & BRAND X PICTURES. (2009). Image Forgery Detection: A survey. In IEEE SIGNAL PROCESSING MAGAZINE (pp. 1053–5888). <https://doi.org/10.1109/MSP.2008.931079>

¹¹M.P. Jain, Indian Constitutional Law (8th ed., LexisNexis 2018).

¹²California Civil Code § 1708.86 (deepfake pornography law):

https://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=202520260AB621

¹³DEEPFAKES Accountability Act (H.R. 3230): <https://www.congress.gov/bill/116th-congress/house-bill/3230>

protection of free speech under the First Amendment to the United States Constitution, which makes broad prohibitions difficult to sustain.¹⁴

In contrast, the European Union has adopted a more structured and proactive regulatory framework. The Artificial Intelligence Act introduces a risk-based classification of AI systems and imposes obligations on developers and deployers. Deepfake content is specifically addressed through transparency requirements, mandating clear disclosure when content is artificially generated or manipulated. Complementing this, the Digital Services Act imposes duties on online platforms to mitigate systemic risks and enhance accountability in the digital ecosystem.¹⁵

8. Strengthening Evidentiary Standards in the Age of AI

The rapid advancement of artificial intelligence, particularly in the creation of deepfakes, poses a serious challenge to traditional principles of evidence law. As digital content becomes increasingly susceptible to manipulation, there is an urgent need to recalibrate evidentiary standards to preserve the integrity of judicial processes.

Reading Puttaswamy alongside the BSA, a constitutional argument emerges for reform. Courts must draw a clear line between formal authenticity what the Section 63 certificate establishes and substantive authenticity whether the content is genuine. If dignity and informational self-determination are fundamental rights, then a framework that admits a certified deepfake without any content-level verification falls short of constitutional obligations. Clearing the certificate threshold should open the door, not close the inquiry. Whether the evidence behind that door is real must remain a live question, challengeable at any stage.

One crucial reform is the introduction of mandatory "AI-based forensic verification" before the admission of digital evidence. Courts should require that audio-visual material, particularly when disputed, undergo verification through certified forensic tools capable of detecting synthetic manipulation. This would act as a preliminary safeguard against fabricated evidence.¹⁶

Closely linked to this is the need for "enhanced authentication standards." Existing provisions under the Bharatiya Sakshya Adhiniyam, 2023 recognize electronic evidence, but they do not adequately address AI-generated content. A higher threshold of proof should be mandated, incorporating metadata analysis, chain-of-custody verification, and expert certification. An important shift would be to move from a "presumption of authenticity" to a "presumption of contestability" for digital evidence. Unlike traditional documents, AI-generated media can be fabricated with high realism; therefore, courts should treat such evidence as inherently suspect unless independently verified. This would fundamentally recalibrate evidentiary evaluation in line with technological realities.

Another key reform is the creation of a specialized cadre of "digital evidence verification experts." These experts would assist courts in evaluating technically complex material, ensuring that judicial determinations are not undermined by a lack of technical expertise. Additionally, India could consider introducing a "statutory obligation of disclosure for AI-generated content," particularly when relied upon as evidence. Failure to

¹⁴First Amendment (U.S. Constitution – official text, National Archives): <https://www.archives.gov/founding-docs/bill-of-rights-transcript>

¹⁵Artificial Intelligence Act (official proposal): <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206>
Digital Services Act (official EU law): <https://eur-lex.europa.eu/eli/reg/2022/2065/oj>

¹⁶Bharatiya Sakshya Adhiniyam, 2023: <https://www.indiacode.nic.in/handle/123456789/20062>

disclose the synthetic nature of content could attract adverse evidentiary inferences. This would align Indian law with emerging global practices and promote transparency.

Practically, courts should require a forensic integrity report alongside the Section 63 certificate for audio-visual evidence in serious proceedings from an accredited examiner confirming the recording was tested for synthetic manipulation. Courts already have the power under Section 30 of the BSA to appoint expert witnesses independently; that power must be used proactively where authenticity is in dispute. Legislatively, the BSA should be supplemented by rules mandating minimum forensic verification standards for audio-visual evidence in criminal trials. The constitutional values affirmed in *Puttaswamy* demand no less.

9. Conclusion

Deepfake technology has profoundly transformed our comprehension and trust in evidence within the digital era. For a long time, courts have thought that what they could see and hear was strong proof of the truth. But this assumption is no longer completely trustworthy. As we talked about, Section 63 of the *Bharatiya Sakshya Adhiniyam, 2023* makes sure that electronic records are properly documented and certified. However, it does not address the more important question of whether the content itself is real. This gap in the law is becoming more and more worrying now that AI can make fake videos and audio recordings that look and sound very real.

Deepfakes represent something genuinely new in the history of evidentiary manipulation not a forged signature or a coached witness, but a fabricated human being, saying things they never said, in a place they never were. The BSA does important work. Section 63 does important work. But neither was built for a world where that kind of fabrication is possible on a consumer laptop. The constitutional framework that *Puttaswamy* established grounding privacy, dignity, and identity in Article 21 gives Indian courts the tools to demand more. The question is whether courts and the legislature will use those tools before the next deepfake walks through a courtroom door and changes someone's life forever.

When we look at this problem from the point of view of constitutional values like privacy, dignity, and a person's right to control their own identity, the risks get even worse. A fake video or audio clip can hurt people's reputations, trick courts, and make justice less fair. So, courts need to do more than just accept certified electronic records; they also need to check to see if they are real. Forensic analysis, expert involvement, and stricter standards for evidence are all needed to make things safer. In today's digital world, seeing is not always believing, and the law needs to change to fit this new reality.

Key References

1. Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., (2017) 10 SCC 1 (Supreme Court of India, 9-Judge Bench). <https://indiankanoon.org/doc/91938676/>
2. Chesney, R., & Citron, D. K. (2018). Deep Fakes: a looming challenge for privacy, democracy, and national security. SSRN Electronic Journal. <https://doi.org/10.2139/ssrn.3213954>
3. Citron, D. K., & Chesney, R. (2018). Deepfakes and the new disinformation war. eYLS (Yale Law School). https://scholarship.law.bu.edu/shorter_works/76
4. Information Technology Act, 2000, §§ 4–5 (legal recognition of electronic records and digital signatures).
5. Information Technology Act, 2000, §§ 66C–66E.

6. Digital Personal Data Protection Act, 2023.
 7. Shreya Singhal v. Union of India, (2015) 5 SCC 1.
 8. Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023, § 63 (India). BSA on IndiaCode: <https://indiacode.nic.in>
 9. Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473; Arjun Panditrao Khotkar v. Kailash iKushanrao Gorantyal, (2020) SCC 1. <https://indiankanoon.org/doc/1871105/>
 10. Farid, H. & BRAND X PICTURES. (2009). Image Forgery Detection: A survey. In IEEE SIGNAL PROCESSING MAGAZINE (pp. 1053–5888). <https://doi.org/10.1109/MSP.2008.931079>
 11. M.P. Jain, Indian Constitutional Law (8th ed., LexisNexis 2018).
 12. California Civil Code § 1708.86 (deepfake pornography law): https://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=202520260AB621
 13. DEEPFAKES Accountability Act (H.R. 3230): <https://www.congress.gov/bill/116th-congress/house-bill/3230>
 14. First Amendment (U.S. Constitution – official text, National Archives): <https://www.archives.gov/founding-docs/bill-of-rights-transcript>
 15. Artificial Intelligence Act (official proposal): <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206> Digital Services Act (official EU law): <https://eur-lex.europa.eu/eli/reg/2022/2065/oj>
 16. Bharatiya Sakshya Adhiniyam, 2023: <https://www.indiacode.nic.in/handle/123456789/20062>
-