AICYBERLEX NEXUS

Journal of Artificial Intelligence, Cyber & Contemporary Law

Volume I · **Issue I** · **Jul–Sep 2026** · Article 3
ISSN: Applied for (National ISSN Centre, NIScPR, India) · e-ISSN: TBA
Peer-reviewed · Open Access · https://aicyberlexnexus.com

ARTICLE 3

Deepfakes and the Law: Gaps in the Information Technology Act and the Bharatiya Nyaya Sanhita

Bhavya

ABSTRACT

Synthetic video, audio and images that show real people saying or doing things they never did have moved from novelty to everyday harm. Indian courts have started to respond, mostly through injunctions that protect the personality rights of celebrities. Criminal and regulatory law has been slower. This paper examines how the Information Technology Act, 2000 and the Bharatiya Nyaya Sanhita, 2023 deal with deepfakes today. It finds that no provision targets synthetic media directly, that existing offences fit only some of the harms, and that the heaviest burden falls on victims who must prove, report and wait. The paper looks briefly at how other jurisdictions have responded and suggests a short set of reforms: a clear offence for non-consensual synthetic intimate content, a fixed takedown timeline, labelling duties for generators and platforms, and a streamlined route for ordinary victims.

KEYWORDS: deepfakes; synthetic media; IT Act; Bharatiya Nyaya Sanhita; personality rights; intermediary liability

1. Introduction

A few minutes of someone's voice and a handful of photographs are now enough to build a convincing fake. The same tools that dub films into new languages can place a stranger's face into pornographic footage, copy a company director's voice to authorise a payment, or put invented words into a politician's mouth days before an election. Law has been here before. Forged documents, doctored photographs and impersonation are old problems. What is different about deepfakes is speed, scale and cost. A fake that once took a skilled forger weeks can be made by a teenager in an afternoon and shared with millions before the victim hears of it. This paper asks whether Indian law, as it stands, is up to the task. It looks at the harms in Part 2, the existing provisions in Part 3, the gaps in Part 4, and possible reforms in Part 5, drawing briefly on foreign approaches. Part 6 concludes. The author writes from a legal-policy perspective and make no claim about technical detection, which is a separate and fast-moving field.

2. What deepfakes are and the harms they cause

A deepfake is media generated or altered by machine-learning techniques so that it appears to show a real person doing or saying something. The term covers face swaps, voice cloning and fully synthetic scenes. Four families of

harm recur.

1

The first is sexual abuse. A large share of deepfake material found online is non-consensual pornography, and the targets are overwhelmingly women. The harm is real even though the body in the image is not the victim's: reputation, safety, employment and mental health suffer. The second is fraud. Voice-cloning scams, where a relative or boss appears to call asking for urgent money, have been reported in India and elsewhere. Company payment fraud using cloned executive voices is a growing concern for banks. The third is political manipulation. A short fake clip released shortly before voting can spread faster than any correction. Even a clumsy fake can do damage, because it gives believers something to share and gives wrongdoers the cover of saying a genuine recording is "just a deepfake". The fourth is the commercial misuse of identity. Actors, singers and sportspeople have found their faces and voices used in advertisements they never agreed to.

3. Existing provisions

3.1 Information Technology Act, 2000 Several sections are used in practice. Section 66C punishes identity theft, including fraudulent use of a person's electronic signature, password or other unique identification feature. Section 66D punishes cheating by personation using a computer resource. Section 66E punishes capturing, publishing or transmitting an image of a person's private area without consent, though it assumes an actual image. Sections 67 and 67A criminalise publishing or transmitting obscene and sexually explicit material, and section 67B deals with child sexual abuse material.[1] Section 69A allows blocking orders on specified grounds. On the platform side, section 79 gives intermediaries a safe harbour if they observe due diligence and act on knowledge of unlawful content. The Intermediary Guidelines and Digital Media Ethics Code Rules, 2021 require intermediaries to remove content that shows a person in sexual conduct or in a way that is impersonating, within 24 hours of a complaint from the individual or someone on her behalf.[2] The Ministry of Electronics and Information Technology has also issued advisories asking platforms to deal with deepfakes under these rules, and has indicated an intent to amend them to require labelling of synthetic content. 3.2 Bharatiya Nyaya Sanhita, 2023 The BNS replaced the Indian Penal Code from July 2024. Section 319 deals with cheating by personation. Sections 336 and 340 cover forgery and the use of a forged electronic record as genuine. Section 356 covers defamation, and section 77 punishes voyeurism, which includes watching or capturing an image of a woman in a private act. Section 79 deals with words, gestures or acts intended to insult the modesty of a woman. Section 111 deals with organised crime, including cyber-crime, where a syndicate is involved.[3] Section 353 addresses statements that may cause public mischief, which can reach election-related fakes. 3.3 Personality rights decisions

2

Civil courts have been the quickest to act. In Anil Kapoor v Simply Life India, the Delhi High Court granted an injunction restraining the use of the actor's name, voice, likeness and image, including through AI-generated content.[4] Several similar orders have followed for other public figures. These decisions are valuable, but they mainly help people with the means to litigate in a high court.

4. Gaps in the present law

4.1 No direct offence No section says in terms that creating or sharing a deepfake is an offence. Prosecutors must fit the facts to sections written for other conduct. For instance, section 66E speaks of an image of a person's private area. A synthetic image shows an invented body, so the fit is poor. Section 77 of the BNS has similar difficulty where no real recording was made. Prosecutors and courts can stretch the language, but stretched language invites challenge. 4.2 Weak fit for non-sexual harms A deepfake that shows a candidate making a false statement is not clearly defamatory in the usual sense if it is posted as obvious satire, and it is not clearly forgery unless it is taken as a document. Fraud by voice clone fits cheating provisions well, but only after the money is gone. 4.3 Consent is not the organising idea Almost every harm described in Part 2 comes down to use of a person's likeness without consent. Yet consent does not feature in the criminal provisions as the central test. A clean statutory rule — it is an offence to create or share realistic synthetic media of an identifiable person, in a sexual, deceptive or defaming way, without that person's consent — would be easier to apply than the present patchwork. 4.4 Slow and uneven takedown The 24-hour removal duty is useful on paper. In practice a victim must find each upload, file a complaint, escalate to a grievance officer, and may still face re-uploads. Fakes copy themselves faster than takedowns can chase them. Victims outside big cities and those without legal help are especially exposed. 4.5 Proof Courts will need to decide whether a clip is real. Forensic tools exist, but they are costly, uneven in quality and not available in most district courts. The Bharatiya Sakshya Adhiniyam, 2023 retains the certificate requirement for electronic records, which says little on authenticity in the age of synthetic media. [5] The opposite risk is equally troubling: genuine evidence dismissed by those it harms as "AI". 4.6 Responsibility of generators The law focuses on the person who posts and the platform that hosts. It says little about the companies that build and release tools that make convincing fakes easy. There is no duty to watermark outputs, to refuse obviously abusive requests, or to keep logs that would help trace a creator.

3

5. Looking abroad and proposing reform

Other systems have started to move. Several American states have criminalised sexual deepfakes, and in 2025 the United States passed the federal TAKE IT DOWN Act, which makes it an offence to publish non-consensual intimate imagery including synthetic imagery, and requires covered platforms to remove it within 48 hours of notice.[6] The European Union's AI Act includes transparency duties requiring that synthetic content be disclosed as such.[7] China has rules requiring labelling of synthetic content and consent for use of a person's likeness. The United Kingdom has legislated against creating sexually explicit deepfakes of adults. Drawing on these examples, the author suggests the following for India. A specific offence covering the creation or sharing of realistic synthetic media depicting an identifiable person in a sexual, defamatory or deceptive manner without consent, with higher punishment where the victim is a minor. A fixed and shorter takedown time for intimate synthetic content, perhaps within a few hours of a complaint, with a duty on platforms to block known copies by matching. A labelling and watermarking duty for providers of generative tools and for platforms that distribute synthetic content, with a safe harbour for clearly marked parody and satire. A single-window complaint route for victims, linked to the cyber-crime portal, with free access to basic forensic verification. Training for judges and police on handling electronic evidence in the era of synthetic media, and guidance on how courts should weigh claims that a genuine recording is fabricated. Care is needed with each. Overbroad rules could chill satire and legitimate

commentary, which the Supreme Court has repeatedly protected under Article 19(1)(a), most notably in Shreya Singhal v Union of India.[8] Takedown timelines can be misused to silence criticism. That is why a consent-based, harm-focused definition is preferable to a ban on "fake content" in general.

6. Conclusion

India has partial answers to deepfakes. Civil courts protect celebrities, the IT Act and BNS reach some of the worst conduct, and the 2021 Rules put a clock on platforms. But the system depends on stretching older provisions, and the person least able to fight back, the ordinary victim, carries the heaviest load. A clearly drafted consent-based offence, quicker takedown, labelling duties for those who build the tools, and better forensic support would not stop every fake. They would give victims a clear right and a faster remedy, and give courts a firmer text to apply.

References [1] Information Technology Act 2000, ss 66C, 66D, 66E, 67, 67A, 67B, 69A, 79.

4

[2] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, rr 3(1)(b), 3(2)(b). [3] Bharatiya Nyaya Sanhita 2023, ss 77, 79, 111, 319, 336, 340, 353, 356. [4] Anil Kapoor v Simply Life India (Delhi High Court, 2023). [5] Bharatiya Sakshya Adhiniyam 2023, s 63. [6] Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks (TAKE IT DOWN) Act, Pub L 119-12 (2025). [7] Regulation (EU) 2024/1689 (AI Act), art 50. [8] Shreya Singhal v Union of India (2015) 5 SCC 1.

5

Cite as: Bhavya, “Deepfakes and the Law: Gaps in the Information Technology Act and the Bharatiya Nyaya Sanhita”, *AICyberLex Nexus*, Vol. I, Issue I, Jul–Sep 2026, Article 3. Available at https://aicyberlexnexus.com
© 2026 AICyberLex Nexus. Open access under the terms stated on the journal website.