The Indian Journal for Research in Law and Management
Open Access Law Journal – Copyright © 2026
Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

DEEPFAKES AND CYBER LAW: IS INDIA'S LEGAL FRAMEWORK READY?

~ Bhumi Pal

INTRODUCTION

A few years ago, deepfakes required a studio, a budget and weeks of work. Today all it takes is a phone and an afternoon. That puts the issue squarely in the domain of cyber law. A deepfake is a person's audio, video or image that has been generated or altered with machine learning so that it appears to show that individual in a real-life situation they never took part in. The risks to individuals are clear: reputational damage, fabricated intimate imagery of women, fraudulent impersonation of family members, and doctored footage with implications for public discourse. The tougher question, which this article attempts to explore, is whether Indian law has kept up with the technology.

THE LAW BEFORE THE LABEL

India does not have a statute that specifically mentions ‘deepfake’, so victims have had to rely on general provisions meant for similar issues. The Information Technology Act, 2000 (IT Act) provides the most straightforward starting points. Section 66C deals with the fraudulent use of another person's unique identification feature, and section 66D with cheating by personation through a computer resource.[1] If a deepfake involves private or sexually explicit imagery, it falls under sections 66E, 67 and 67A.[2] The Bharatiya Nyaya Sanhita, 2023 adds cheating by personation, forgery (including forgery intended to damage a person's reputation) and defamation.[3]

While this is a decent toolkit, each provision applies clumsily. Section 66C was aimed at passwords and digital signatures, and stretching ‘unique identification feature’ to include a face or voice is an argument, not a settled reading. The defamation route requires proof of

[1] Information Technology Act, 2000, No. 21 of 2000, §§ 66C–66D, India Code (2000).
[2] Id. §§ 66E, 67, 67A.
[3] Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023, §§ 319, 336, 356, India Code (2023).

reputational harm and involves lengthy trials. None of these provisions offers a concrete answer to what a platform should do at 2 a.m. when a fake video is spreading and the victim needs help.

THE 2026 AMENDMENT: NAMING THE PROBLEM

The government's response came when the Ministry of Electronics and Information Technology notified amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, effective from 20 February 2026.[4] For the first time, Indian law defines what 'synthetically generated information' (SGI) is.

SGI means audio, visual or audio-visual content that is created or altered by a computer resource so that it appears real and portrays a person or event in a manner that is, or is likely to be perceived as, indistinguishable from a real person or event.[5] Routine editing and good-faith academic or training material are excluded from this definition.

The rules then impose obligations on intermediaries. Platforms that enable the creation of SGI must use reasonable technical measures, including automated tools, to prevent unlawful synthetic content. Lawful content must be prominently labelled and carry embedded metadata, and platforms may not help remove such markers.[6] Takedown deadlines have also been compressed: where a court order or reasoned government intimation has been received, access must be disabled within three hours rather than thirty-six.[7] This is important because platforms keep their safe harbour under section 79 of the IT Act only if they observe due diligence, and these obligations are linked to that.[8]

WHAT THE COURTS HAVE BEEN DOING

In tandem with legislative developments, the Delhi High Court has begun to uphold personality rights. In *Amitabh Bachchan v. Rajat Nagi*, the court restrained the unauthorised commercial use of the actor's name, voice and likeness.[9] In *Anil Kapoor v. Simply Life India*, the court went further and granted an injunction against misuse of the actor's identity, which

[4] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026 (India) (notified Feb. 10, 2026; in force Feb. 20, 2026).
[5] Aakriti Bansal, MeitY Notifies New Amendments to IT Rules to Regulate Synthetic Media and Deepfakes, MediaNama (Feb. 10, 2026), https://www.medianama.com/2026/02/223-meity-amendments-it-rules-synthetic-media-deepfakes/.
[6] India Introduces Mandatory Labelling for AI and 3-Hour Takedown for Illegal Content, Hogan Lovells (Feb. 2026), https://www.hoganlovells.com/en/publications/india-introduces-mandatory-labelling-for-ai-and-3hour-takedown-for-illegal-content.
[7] Id.
[8] Information Technology Act, supra note 1, § 79(2)–(3).
[9] Amitabh Bachchan v. Rajat Nagi, 2022 SCC OnLine Del 4110 (India).

explicitly included AI-generated and deepfake content.[10] These orders have been quick and effective, but to date they have largely protected high-profile individuals with litigation budgets. An ordinary student whose face has been pasted onto a fake video has few options.

There is also a constitutional angle. In *Justice K.S. Puttaswamy (Retd.) v. Union of India*, the Supreme Court recognised privacy as a fundamental right, in which dignity and bodily autonomy are central.[11] The Digital Personal Data Protection Act, 2023 adds another layer: a person's face and voice, when used to train or generate a deepfake, are personal data processed without consent.[12] Neither was designed for deepfakes, but both give victims a basis to build on.

THE FREE SPEECH BALANCING ACT

Any rule on synthetic media must be consistent with Article 19(1)(a), subject to the reasonable restrictions in Article 19(2).[13] Parody, satire and political commentary often use manipulated media, and a poorly worded takedown regime can inadvertently capture them. The Supreme Court's decision in *Shreya Singhal v. Union of India* serves as a helpful reminder. The Court struck down section 66A and read down the takedown power in section 79, finding that an intermediary has to act only on a court order or government notification, not on a private complaint.[14] The three-hour deadline in the new rules is tied to such orders, which keeps it closer to that principle, but the speed itself raises a fair concern: a platform with three hours to decide will usually delete first and ask questions later.

WHERE THE GAPS REMAIN

Despite the 2026 amendment, some gaps remain. First, the rules apply to intermediaries, but the person who makes the fake is often untraceable or overseas, and cross-border enforcement is slow. Second, labelling only helps if the label stays. A clip that is downloaded, re-recorded and shared through an encrypted message loses its metadata in seconds. Third, detection technology is imperfect, and automated filters can wrongly flag legitimate content or miss sophisticated fakes. Fourth, personality rights in India are still judge-made. There is no statute that gives an individual a right to say, ‘this is my face and my voice, and you cannot use it without my consent.’

[10] Anil Kapoor v. Simply Life India, 2023 SCC OnLine Del 6914 (India).
[11] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).
[12] Digital Personal Data Protection Act, 2023, No. 22 of 2023, India Code (2023).
[13] India Const. art. 19, cl. 1(a), cl. 2.
[14] Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1 (India).

THE WAY FORWARD

A workable solution would combine law, technology and awareness. Parliament could create a statutory right over one's likeness and voice, with exceptions for satire, news reporting and criticism. A fast-track remedy for victims, particularly for non-consensual intimate deepfakes, would save individuals from months of litigation over an image that has done its damage in minutes. Platforms should be obliged to publish transparency reports on the number of synthetic-content complaints they receive and how quickly they act. Finally, no law is a substitute for public awareness. Schools, colleges and workplaces should teach people to question viral media before sharing it, because the cheapest and quickest way to stop a deepfake is a sceptical individual.

CONCLUSION

India has moved from having no deepfake-specific rules to having one of the more detailed regulatory frameworks for synthetic media. The 2026 amendment deserves credit for defining the problem and setting duties for platforms, but a framework that focuses only on what platforms ought to do cannot fully protect individuals. The next step is to give people enforceable rights of their own while preserving freedom of expression. Technology will continue to evolve, and the law must keep up with it.