



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.

DEEP FAKES AND AVAILABLE LEGAL REMEDIES

~ Anshika Jain

ABSTRACT

Deepfake technology uses computer programs to create videos and audio that sound very real. This can cause a lot of problems such as hurting someone's reputation making porn cheating people and spreading false information about politics. Deepfakes started on websites like Reddit in 2017. People can use intelligence for bad things even though deepfake technology can also be used for good things, like education and entertainment. In India there are laws that try to stop these problems, such as the Information Technology Act from 2000 and the Bharatiya Nyaya Sanhita from 2023. These laws also include the Digital Personal Data Protection Act from 2023. Article 21 of the Constitution. These laws are supposed to protect people from having their identity stolen their privacy. Their reputation damaged. There was a court case called Sadhguru Jagadish Vasudev v. Igor Isakov in 2025. In this case the court said that fake content had to be removed from the internet and that special tools had to be used to detect this content. Now the laws are not very good at stopping deepfakes because they are not strong enough and are not well organized. There is a law called the Digital India Bill that might help fix these problems. To make things better we need laws that're just about deepfakes. These deepfake laws should say that people have to agree before their picture or voice is used. These deepfake laws should also say that websites are responsible for what's on them that they have to be honest, about how they decide what to remove and that they have to use the best technology to find and stop deepfakes. This will help keep people from cyber threats and protect democracy, privacy and dignity. Deepfake technology is a problem. We need to make sure we have deepfake laws to stop deepfake technology.

INTRODUCTION

Contemplate the possibility of a very famous celebrity known as Shahrukh Khan said in a video that “rape should not be criminalized.” Which is impossible but it can be made possible by a synthetic media tool like “Deepfake.” There was a saying that every coin has two sides, same goes with recent AI tools which can be boon for one and bane for another depending on the use by the user. The issue arises when the tool which was made for the ease of one become a nightmare for many. Deepfake is one of them which can harm in various ways such as defamation, non-consensual porn, fraud, political disinformation, erosion of trust in evidence etc.

BACKGROUND ON DEEPPFAKES

1. WHAT IS DEEPPFAKES:

According to Oxford dictionary “a video or audio recording that has been digitally altered in order to present a particular person doing or saying something that they never actually did or said.” Deepfakes can produce hyper-realistic simulations that are hard to detect without forensic tools. Those simulations are created using deep-learning models particularly generative adversarial intelligence GANs which can replicate someone’s appearance, voice, and the mannerism. The Deepfakes can be used for development in education, entertainment, and other fields but mostly they are being used for malicious purposes like misinformation, identity theft, and nonconsensual pornography etc.¹

2. ORIGIN OF DEEPPFAKES:

Deepfakes was originated in 2017 when a reddit user created a community for AI-generated modified films specifically posted videos that swapped the faces of celebrities onto porn performers. It is evolved with the AI and machine learning.²

¹Abhinandhan .B, *Legal Implications Of Deepfake Technology: Privacy, Defamation, And Consent Research Project*, Issn - 2583-2344, INDIAN JOURNAL OF LEGAL REVIEW (Ijlr), 5 (2) Of 2025, Pg. 49-63.

² Cybersecurity Centre of Excellence, <https://ccoe.dscl.in/blog/understanding-deepfakes> (last visited May 10, 2026).

LEGAL FRAMEWORK IN INDIA

1. INFORMATION TECHNOLOGY ACT, 2000:

- The Information Technology Act, 2000 has various provision which addresses crime committed by using deepfake but those are not specific in nature as they are very broader in term and generalize to cover various aspect of cybercrimes.
- Section 66C of the act focuses on Identity theft and mentioned Any person who make use of any other person's electronic signature, password or any other unique identification features fraudulently or dishonestly will be liable for committing Identity theft and will be punishable with imprisonment up to three years and fine up to rupees one lakh. This can be used in case of fraudulent impersonation caused by using Deepfake.³
- Section 66D addresses cheating through impersonation, where an individual pretends to be another person using electronic communication. The person committing cheating by personation will be punished with imprisonment up to three year and fine up to rupees one lakh. This provision can cover frauds done through voice cloning or scams based on impersonation by deepfake.⁴
- Section 66E mentioned violation of privacy which is committed when any person captures, publishes or transmits the image of a private area of any person without his or her consent whether it is intentionally or knowingly, he shall be punished with imprisonment up to three years or with fine up to two lakh rupees or with both. This section has been expanded to cover morphed or deepfaked intimate images.⁵
- Section 67 criminalizes the act of publishing or transmitting in the electronic form, any material which is obscene, lascivious or appeals to the prurient interest shall be punished in case of first conviction with imprisonment up to three years and fine up to rupees five lakh and in case second or subsequent conviction with imprisonment up to five years and fine up to rupees ten lakh.⁶
- Section 67A addresses that any person who publishes or transmits any sexually explicit material in electronic form shall be punished in case of first conviction with

³ Information Technology Act, 2000, § 66C, No. 21, Acts of Parliament, 2000 (India).

⁴ Information Technology Act, 2000, § 66D, No. 21, Acts of Parliament, 2000 (India).

⁵ Information Technology Act, 2000, § 66E, No. 21, Acts of Parliament, 2000 (India).

⁶ Information Technology Act, 2000, § 67, No. 21, Acts of Parliament, 2000 (India).

imprisonment up to five years and fine up to rupees ten lakh and in case second or subsequent conviction with imprisonment up to seven years and fine up to rupees ten lakh.⁷

- Section 79 provides a “safe harbor” for online platforms. The platforms generally will not be held responsible for content created and posted by their users, if the intermediary or platforms act in good faith and when remove content whenever it is required by the law.⁸

2. BHARATIYA NYAYA SANHITA, 2023:

- Section 353 mentioned statements conducing to public mischief it states that whoever makes, publishes or circulates any statement, false information, rumour, or report, including through electronic means shall be punished with imprisonment which may extend to three years, or with fine, or with both.⁹
- Section 356 addresses the Defamation that Whoever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes in any manner, any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person. Fake speech modules and morphed video that harm the person’s reputation will come under this.¹⁰
- Section 111 addresses organized cybercrime which also involve deepfake campaigns. Moreover Section 212 criminalizes the person who furnish false information through synthetic content.¹¹

3. DIGITAL PERSONAL DATA PROTECTION ACT, 2023:

The fundamental of Digital Personal Data Protection Act, 2023 is based on consent and deepfake that process biometric data without meaningful consent violate that fundamental principle. The fine for violating that principle is up to two hundred and fifty crore rupees.

⁷ Information Technology Act, 2000, § 67A, No. 21, Acts of Parliament, 2000 (India).

⁸ Information Technology Act, 2000, § 79, No. 21, Acts of Parliament, 2000 (India).

⁹ Bharatiya Nyaya Sanhita, 2023, § 353, No. 45, Acts of Parliament, 2023 (India).

¹⁰ Bharatiya Nyaya Sanhita, 2023, § 356, No. 45, Acts of Parliament, 2023 (India).

¹¹ Bharatiya Nyaya Sanhita, 2023, § 111, No. 45, Acts of Parliament, 2023 (India).

4. CONSTITUTION OF INDIA:

Article 21 mentions right to life and personal liberty which was in question due to the emergence of deepfakes, so this article act as a safeguard against the deepfake synthetic content to protect the personality rights and right to live with dignity.¹²

DEEPFAKES AND PERSONALITY RIGHTS

Under Article 21 of the Constitution of India, the Right to privacy is inculcated by the judiciary to protect the personality right of the celebrity. Personality consists of mannerisms, voice, style and so on by which the person has to be identified by the masses. In *Karan Johar v. Indian Pride Advisory Pvt. Ltd.* the High Court of Bombay stated that public figures have rights in their persona and any misuse of that persona for commercial gain is a legal wrong.¹³

The perfect Indianization solution to this problem is hidden in the intricacy of laws, that if a celebrity wants to protect their personality right, they have to go with various laws at the same time, first the Trademark Act of 1999 for the protection of copyright of signature, registration of name, catchphrases for commercial purpose, second to take down morphed or deepfake A.I generated video Information Technology Act, 2000 may be applied.

THE DIGITAL INDIA BILL 2023

The Digital India Bill, which was meant to take place of the Information Technology Act, 2000. The aim of this Bill is to provide a more detailed and sophisticated framework for regulating digital activities. The final draft of this will is still waiting to be enacted and various reports shows that the Bill will include provisions to address AI and Deepfake-related harms.

The expected reforms mention regular risk evaluation for Online platforms, proper classification of cybercrimes like impersonation and identity theft and it also aims to provide different types of online intermediaries which will eventually end regulatory gaps which allowed misuse of emerging technologies.¹⁴

¹² INDIA CONST. art. 21.

¹³ *Karan Johar v. Indian Pride Advisory (P) Ltd.*, 2024 SCC OnLine Bom 2444.

¹⁴ Krish Arya, *Deepfake Regulation India 2025: MeitY's Comprehensive IT Rules Amendment*, KHURANA & KHURANA, (June, 8, 2026, 10:21 PM), <https://www.khuranaandkhurana.com/deepfake-regulation-india-2025-meity-s-comprehensive-it-rules-amendment>.

CASE STUDY

1. SADHGURU JAGADISH VASUDEV AND ANR. V. IGOR ISAKOV AND ORS.

On 30th May 2025 the defendants created a fake website using AI-morphed deepfakes of Sadhguru's voice, image and appearance. To exploit the reputation Sadhguru for financial gains the defendants created fraudulent content based on fabricated claims such as false arrest and fake endorsement materials. The plaintiffs argued that it not only harmed their personality rights but also caused defamation by harming their public image and dignity in the digital space.

Justice Saurabh Banerjee issued a injunction which is very special known as dynamic+ injunction. It is designed to protect a victim from misuse of their identity, specifically that misuse is driven by AI. The legal judgment analysed that modern deepfake technology have a new type of threat to a person's right to their own image and personality rights. Deepfakes create new types of harm that existing legal frameworks for Intellectual property infringement will not be able to address properly.

The court established 36-hour schedule for taking down content and it also directed YouTube and various other similar type of platform to install technology which will automatically detect and delete Identical content which are infringing in nature.¹⁵

RECOMMENDATIONS

A horse is running at its best speed and a human is try to chase it, this is the same scenario in case of cybercrimes it will just keep on running and ever evolving and to tackle it the legislation has to make updated law instead of relying on traditional one, as these law will never be sufficient to handle the area like cybercrimes where even a minute contributes towards its growth in cyber space. Indian need to enforce specific Laws to handle the creation and distribution of AI-generated content. The term Consent should be given absolute priority by strengthening mechanisms and legislation. Technology Should be updated and deployed to detect and track deepfakes. Intermediaries and platform should be held liable by creating proper liability frameworks which must have easy removal protocols and their moderation processes should also be transparent.

¹⁵ Sadhguru Jagadish Vasudev and Anr. v. Igor Isakov and Ors., (CS (COMM) 578/2025).

CONCLUSION

Deepfakes represent a fundamental change in harm done in cyberspace, which raised questions on the adequacy on the legislation which based on paper centric crimes. In present time India have only Information technology Act, 2000, Bhartiya Nyaya Sanhita, 2023 and Constitutional provision to tackle and address the growing digital crime, but this law is currently reactive, not well-coordinated and not specific in nature. The global trend is creating specific laws for online platforms which increases their responsibilities and require transparency regarding of AI technologies. It is very important for India to adopt a regulation that focuses on individual rights, understands technology and have clear legal definitions, fast and accurate legal solutions. These regulations is essential to protect personal rights, consent, privacy and the very integrity of democracy in the face of deepfakes.