CALL FOR PAPERS & ARTICLES 2025–26
Organised by LaWGiCo (Nivisam Lawgico Innovation Pvt. Ltd.)

Title:

Regulation of Deepfakes and Generative AI Under Indian Laws: A Need For Reform

By:

Mridul Choudhary
(Banaras Hindu University)

&

Saurabh Singh
(Babu Banarasi Das University)

Abstract

Technology, which was once a boon to the mankind, is becoming their worst nightmare. This sudden change got introduced by the misuse of the generative AI that was initially used to create parodies of people by swapping their faces in memes. However, this changed when such generative AI got into the hands of people who used it to create deepfakes. These deepfakes created a problem as the real world got mixed up with the virtual world, and the twist is that there is no dedicated statute available to regulate these deepfakes. This article delves into the legal structure that supervises the corruption of artificial intelligence, challenges that are being faced, and the path for the future. Therefore, such content needs to be regulated as soon as possible; otherwise it will continue to haunt people with the spread of fake images and videos of close ones.

Introduction

"Artificial intelligence is the need of the hour" is a familiar statement in the 21st century. This assertion portrays Artificial Intelligence (AI) as a knight in shining armor. However, it is a known fact that every invention has a drawback that is not inherent to it but incidental when it comes into hands of the wrong people. One such downside of AI is deepfake. Deepfakes are digitally altered images and videos created with the help of generative AI, which is based on the deep learning model of AI. Deep learning is a special kind of machine learning that involves "hidden layers." There are two algorithms involved that create these deepfakes. One algorithm is programmed to produce the best fake replicas possible of real images. The other model is trained to distinguish the real image from the fake one[1]; this process is repeated endlessly until there is no difference left. Recent examples include a video of Elon Musk promoting a fake crypto scheme that went viral, leading people to lose thousands of dollars. The other video involved Taylor Swift's deepfake, which aimed at tarnishing her reputation. In India, deepfakes are no exception, as a deepfake of actress Rashmika Mandanna went viral, which created chaos in the media. The sad reality is that there are no regulations

[1]University of Virginia Information Security Office, 'What the Heck Is a Deepfake?' (University of Virginia Information Security Office) https://security.virginia.edu/deepfakes accessed 12 August 2025.

specifically dealing with the abuse of artificial intelligence including, the deepfakes and generative AI in India. However, there are provisions under IT Law that second-hand regulates the horrors created by deepfakes to some extent. Still, the present legal framework is not adequate and India requires a comprehensive legal foundation which not only governs artificial intelligence but also resolve the challenges that are posed towards privacy, democracy, and cybersecurity of the nation.

Legal Framework Regulating Deepfakes in India

With all the escalation in crimes relating to generative AI and the lack of dedicated deepfake laws, the Information Technology Act and Bhartiya Nyaya Sanhita play a predominant role in regulating these digital malpractices. Under the IT Act, 2000, the relevant sections would include section 66C and D, dealing with identity theft and impersonation, respectively. At last, Section 67 deals with obscenity. Under the BNS, Section 294 talks about the sale etc., of obscene books etc.; Section 353 aims to curb the misinformation and Section 356 penalizes defamation. Moreover, the Press Information Bureau, while replying to the Rajya Sabha on the question relating to the measures taken by the Government of India in tackling deepfakes, stated that amendments will be brought in the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, to address the ongoing challenges regarding cyberspace. To better understand the incidental regulations, it is important to first examine the relevant provisions of the IT law and Bhartiya Nyaya Sanhita.

IT Law Provisions

- **Section 66C** of the Information Technology Act, 2000, states that any person who fraudulently or dishonestly uses the digital signature, password, and other unique identification feature of another person shall be punished with maximum imprisonment of three years and with a maximum fine imposed of one lakh rupees. In this provision the important takeaway is the use of the term “unique identification feature” which implies biometrics that include the unique biological characteristics such as fingerprints, facial recognition, etc. Therefore, the use of the individual’s face in the deepfakes without their consent would impose a penalty under this section.
- **Section 66D** of the Information Technology Act, 2000, is one of the most important provisions to regulate the deepfakes, as it penalizes any person who, by means of a communication device or computer resource, impersonates and commits cheating. For such impersonation and cheating, the maximum punishment defined is imprisonment of three years with a maximum fine of one lakh rupees. This provision is relevant in the context that

the deepfakes are used with the sole purpose of either tarnishing the reputation of someone by using the individual's face in an adult video or for extorting money from the individual by creating a fake video of some relative, friend, or close one who is in dire need of money with the help of generative AI.

- **Section 67** of the Information Technology Act, 2000, penalizes any person who transmits or publishes lascivious or any content, in electronic form, that tends to corrupt or deprave the minds of those who can read, see, or hear such content. Such a person, on his first conviction, shall be punished with imprisonment of either description for a maximum period of three years with a fine of up to five lakh rupees, and if the offense is subsequently committed by the same person, then the imprisonment may extend to five years with a fine that may extend to ten lakh rupees. The obscene content generated with the help of generative AI or the deepfakes created with the aid of the faceswap also fall under this section.

Bhartiya Nyaya Sanhita Provisions

- **Section 294** deals with the offense of obscenity. According to the provision, any sale, public exhibition, distribution, import, export, taking part, advertisement, etc. of a book, pamphlet, paper, writing, drawing, painting, representation, figure, or any other object, including display of any content in electronic form, should be deemed to be obscene[2] if it reflects an overt sexual interest and such action depraves or corrupts persons who are likely to read, see, or hear it. This section, to some extent, is similar to section 67 of IT law. Deepfakes are primarily created to degrade the reputation; this includes producing obscene content of people that leaves the victim traumatized. Such obscene videos make it easier for extortionists to demand money, as it is a direct attack against an individual's personality. As deepfakes are initially an electronic media and they are published on social media platforms, this makes them a subject of regulation under this section. The punishment includes imprisonment up to two years and a fine of five thousand rupees on first conviction. For a subsequent offense, the punishment is imprisonment up to five years with a fine of ten thousand rupees.

  Section 353 regulates the offense of spreading misinformation. The provision states that any person who makes, publishes, or circulates any statement, false information, rumor, or report the medium of communication also includes electronic means with the intent to cause commotion in the society, military, or between communities. According to the Press Information Bureau, the Union Minister of State for Electronics and Information Technology submitted in Rajya Sabha that Section 353 aims to curb the spread of misinformation and

[2] *Bharatiya Nyaya Sanhita* 2023, s 294.

disinformation by penalizing the act of making false or misleading statements, rumors, or reports that can cause public mischief or fear. [3]

- **Section 356** provides for defamation; the provision states that any person who in a verbal, written, or signs(symbols) or by visible representations makes or publishes in any manner any allegation that intends to harm the reputation of such person except in the case of publication being made in good faith, made for public good, etc. A deepfake can harm someone's reputation by falsely depicting them in a compromising, criminal, or immoral situation and showcasing people committing or saying something unprecedented. Therefore, the section is clear that any visible representation i.e., a video, made with the intention to diminish the reputation of another would be defamation. Punishment includes simple imprisonment up to two years, or with a fine, or both, or with community service.

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

According to the Press India Bureau, the Union Minister of State for Electronics and Information Technology informed the Rajya Sabha on the question of measures taken by the Government of India to tackle the deepfakes that the IT Act and the rules made apply to any information that is generated using Artificial Intelligence (AI) tools or any other technology and those which are generated by users themselves for the purpose of defining offenses. Moreover, amendments would be brought in the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.[4] The IT Rules, 2021, impose an obligation on the social media platforms to not store or publish any sensitive information. They are also reminded from time to time about their obligations and are also advised to combat the unlawful data, including malicious "synthetic media" and "deepfakes," to curb the spread and ensure the prompt removal of harmful material from online platforms.

To deal with cybercrime expeditiously, the Ministry of Home Affairs established a framework called the Indian Cyber Crime Coordination Centre (I4C), and it also launched the National Cyber Crime Reporting Portal. This allows the public to report various types of cybercrime.

Judicial Determination on Deepfake

---

[3] Press Information Bureau, Government of India, 'India Well-Equipped to Tackle Evolving Online Harms and Cyber Crimes; Government to Parliament: India's Multi-Layered Cyber Response System Combines Laws, Institutions, and Public Outreach to Tackle Cyber Crimes and Deepfakes' (Press Information Bureau, 2025) https://www.pib.gov.in/PressReleasePage.aspx?PRID=2154268 accessed 12 August 2025.

[4] Press Information Bureau, Government of India, 'Government of India Taking Measures to Tackle Deepfakes' (Press Information Bureau) https://pib.gov.in/PressReleasePage.aspx?PRID=2119050 accessed 10 August 2025.

With the rapid increase in deepfakes, the total amount recorded in 2023 is 95,820, which is 550% more than in 2019.[5] These scams and videography have become common because of the accessibility of the generative AI tool, and with the need for a reform in the laws, the judiciary plays a vital role in the adjudication of matters relating to deepfakeswith the aid of available provisions. Some of the critical judgments are as follows:

Nirmaan Malhotra v. Tushita Kaul[6]

- **Facts**: The plaintiff and the defendant married on 06.02.2018. They have a daughter who is approximately five years old. Due to suspicion of adultery, they divorced each other, and after that, the wife filed for maintenance. The husband provided a video as evidence, which showcased the wife with another man. The evidence was submitted in order to evade the maintenance on the ground of adultery.
- **Reasoning**: The court ordered the husband to provide the maintenance. The reasoning behind such judgment was that when the review was done, it was unclear whether the person in the photograph was the wife. The court recognized the possibility of deepfake and announced that the husband would be required to present concrete evidence before the family court.

Karti Chidambaram v. Union of India[7]

- **Facts:** Karti Chidambaram, son of P. Chidambaram, filed a petition against the fake video uploaded on social media of him involved in some unprecedented illicit act. His contention was that the aim of the video was to harm his reputation, and he asked for removal of all the videos from the social media platform.
- **Judgment:** The court held that morphed and deepfake videos fall under the offense of defamation. The court also pronounced that the social media platforms should remove the video as soon as the complaint is received.

National Stock Exchange of India Ltd. v. Meta Platforms, Inc. & Ors.

- **Facts:** The National Stock Exchange of India (NSE) filed a case against Meta Platforms, Inc., and other social media intermediaries because of the circulation of

---

[5] Security Hero, 'State of Deepfakes: Realities, Threats, and Impact' (Security Hero, 2023) https://www.securityhero.io/state-of-deepfakes/?form=MG0AV3 accessed 14 August 2025.

[6] (2024) SCC OnLine Del 4326 (Delhi High Court, 28 May 2024).

[7] (2020) SCC OnLine Mad 605.

fake videos on such social media platforms featuring the MD and CEO of the National Stock Exchange. These videos were created using generative AI that depicted the CEO recommending investors join a WhatsApp group for stock tips and also promised reimbursement in case of losses.

- **Judgment:** The Bombay High Court issued an injunction directing Meta and its intermediaries to take immediate action and remove the videos from their platforms within ten hours of receiving the complaint. The court also asked these platforms to exercise due diligence under the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

Challenges Faced in Regulation of Deepfakes

- **No statutory definition of "Deepfake":** In the contemporary scenario, legislation such as the Information Technology Act, 2000, the Bhartiya Nyaya Sanhita, etc., does not define the meaning of the term "deepfake." This paves the way for multiple interpretations by the judicial authorities; some deepfakes might be brought under the category of defamation by one judge, and the other judge might categorize the same deepfake as a cyber fraud. Therefore, leading to an inconsistent application of the legislation.
- **Non-Binding Advisories:** The advisories issued by the Ministry of Electronics and Information Technology to label or watermark the generated AI are not binding in nature, as advisories are merely some serious suggestion that don't impose any legal liability. Some platforms label a video as AI-generated, but other small platforms do not necessarily oblige.
  For example, a video of someone promoting a scam might be uploaded on YouTube with a label (AI generated), but it might be uploaded on other platforms without any watermark.
- **Jurisdictional Challenge:** There are also jurisdictional challenges involved in regulating deepfakes. It is not necessary that the deepfakes be created and uploaded in the same country. However, it is plausible that offenders are operating from diverse nations. Under such circumstances the question relating to jurisdiction will arise, and without the cooperation of the countries, it would be untenable for a particular country to exercise its jurisdiction, as the mutual legal assistance treaties take months to process.
- **Ground-level Implementation:** The enforcement depends heavily on the state and interagency coordination. The same level of infrastructure is not available in all the cities. For example, in metro cities, the quality of infrastructure to regulate the cybercrime is better than that of smaller cities. The people in lower cities generally are not aware of the redressal portal

and cyber attacks. Therefore, it might be a little difficult for them to get redressed before the deepfake goes viral.

Way Forward

A common proverb is "better late than never," which in our matter implies that even though rapid technological developments have been made, there are still ways through which we can cope with the advanced issues, following are the suggestions that should be kept in mind during the production of statute:

- **Creation of Statute:** The first and foremost thing that is to be done to regulate the deepfake is to draft a dedicated legislation. The statute should not be restricted to the substantive aspect, but it should also include the procedural aspect. Excessive use of technology showcases the need for governance and punishments for the misuse of such mechanisms. As the statute is created to govern the offenses committed with the aid of technology, the procedural provisions should include both the online and offline modes of filing and adjudication. The online procedure will provide quick accessibility and effectiveness to the people in remote areas and it will also create a sense of reliance of people on the technology that will help them in adopting and accepting a techno-centric approach.
- **Uniform Takedown Timelines:** Currently, platforms remove content at an inconsistent speed, which means harmful material can stay online for days. Setting deadlines, such as 24 hours for sexual deepfakes, 3 to 6 hours for election-related deepfakes, and 48 hours for other harmful deepfakes, would create standard response times. It should be kept in mind that the removal should take place within the estimated limit from the date of filing of the complaint.
- **State-level Cyber Forensic Unit:** Even with the uniform timelines, fast removal of such content is not possible unless there is a strong state-level cyber forensic unit. These units should be equipped with the latest deepfake detection tools that would allow them to recognize and distinguish between the real and the fake media. This will aid in rapid response against deepfakes.
- **Consent:** Consent is a necessity. That's why it should be mandatory for the person creating such deepfakes to take the consent of such individuals before creating or sharing a deepfake that uses his voice or facial characteristics. If an image combines a fake depiction of one person with a real depiction of another, consent must be obtained from both. While seeking consent, the purpose of creation, the data to be used, and how it will be shared must be announced beforehand. Importantly, consent to create a deepfake does not automatically

include consent to distribute it. Therefore, any deepfake created without the consent of the individuals involved in the video should be taken down at the earliest instance.

Conclusion

Deepfakes, created using generative AI, poses a serious threat to privacy, dignity, etc. of a person. In India, the Information Technology Act, 2000, the Bhartiya Nyaya Sanhita, 2023, and the IT Rules, 2021, govern the deepfakes, but not comprehensively. The lack of legal clarity, coupled with jurisdictional challenges, inconsistent takedown mechanisms, and weak detection infrastructure lead to slow and ineffective enforcement. The rapid spread of deepfake content means that even immediate action may not undo reputational damage or emotional distress.

A dedicated legal framework is urgently needed. This should include a clear definition of deepfakes, mandatory informed consent for creation and distribution, definite penalties, and strict takedown timelines. State-level AI forensic units must also be strengthened. Public awareness campaigns can empower citizens to identify and report manipulated content, while clear protections for satire, parody, and art will ensure that free expression is preserved.

India’s regulation of deepfakes will not only protect individual rights but also reinforce trust in technology. Without such measures, deepfake technology will continue to abuse the privacy, leaving victims unprotected and justice delayed.