
DEEPFAKES AND THE LAW: AN ANALYSIS OF THE LEGAL FRAMEWORK IN INDIA

Tapasya Dwivedi, Atal Bihari Vajpayee School of Legal Studies,
Chhatrapati Shahu Ji Maharaj University, Kanpur

ABSTRACT

The rapid development of Artificial Intelligence has led to the emergence of deepfakes, digitally manipulated or synthetically generated content that can be used to impersonate individuals, spread misinformation, commit fraud and violate privacy. This paper examines the existing legal framework in India for dealing with deepfakes, particularly the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023 and the Information Technology Rules. It further examines the constitutional protection of privacy and dignity under Article 21 and analyses real-life instances to understand the practical challenges associated with deepfake-related offences. A comparative perspective is also adopted by examining the approach of the United States towards AI-generated non-consensual content. The paper argues that although existing Indian laws provide provisions that may be applied to deepfake-related offences, the effectiveness of these provisions remains a significant concern. It therefore highlights the need for a more specific and effective legal framework capable of addressing the rapidly evolving nature of deepfake technology while protecting individual privacy, dignity and security.

INTRODUCTION

In recent times there is a surge in the use of AI, there remains one issue which stays untouched, that is “Deepfakes”.

Deepfakes are digitally manipulated content formed by using Artificial Intelligence, creation of someone’s deepfakes for malicious use, fraud, non-consensual pornography or to cause harm to someone’s privacy is a legally actionable act. As the technology is relentlessly advancing, it becomes extremely hard for a reasonable person to distinguish between reality and hyper-realistic deepfakes.¹

LEGAL FRAMEWORK IN INDIA

This raises questions about whether there are laws governing this issue, accountability and discussing the legal consequences? There are provisions and laws dealing with identity theft, fraud, violation of privacy such as section 66C, 66D and 66E of the IT Act 2000, respectively.²

Sections from Bharatiya Nyaya Sanhita also include some provisions dealing with cybercrimes in India, these are general provisions dealing with organised crime such as cyber law, furnishing false information and publishing false information including via social media/electronic means, section 111, 212 and section 353, these are the general provisions from Bharatiya Nyaya Sanhita that could be applied in any instances of deepfakes without consent.³

In 2026, an Intermediary guidelines was issued by the Information Technology after performing amendments (Intermediary Guidelines and Digital Media Ethics Code) in order to regulate the intermediary platforms to mandate due diligence in case of any illegal, Impersonating, privacy invasive content or content such as deepfakes, to be removed from the intermediate platform. In the year 2025 and 2026 there have been some significant amendments to the IT Rules, to regulate “Synthetically Generated information”.⁴

¹ U.S. Gov’t Accountability Off., Science & Tech Spotlight: Deepfakes (2020).

² Information Technology Act, No. 21 of 2000, §§ 66C–66E (India).

³ Bharatiya Nyaya Sanhita, No. 45 of 2023, §§ 111, 212, 353 (India).

⁴ Ministry of Electronics & Information Technology, The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026 (India).

LEGISLATIVE DEVELOPMENTS

The issue of deepfakes was also discussed in the Indian Parliament, The Deepfake Prevention and Criminalisation Bill, 2023. Addresses that the AI generated content primarily used for fraud, to threaten someone's privacy shall be seen as a criminal offence furthermore the bill also discusses the need to incur culpability for anyone indulging in such acts of dissemination of falsely fabricated content to invade privacy or to harass someone by misusing their data or prevarication through AI.⁵

Another Bill in the year 2024 was discussed in the lower house of the Parliament, The Regulation of Deepfake Bill, 2024. The bill discussed the need for platform responsibility and the need to seek consent before striving for the creation of someone's deepfake.⁶

There was one similarity in both the Bills, it was seeking the criminalisation of acts related to creation and as well as the dissemination of deepfakes, and also both the Bills included the need for a "Task Force" to regulate, recognise and removal of content created by the intent to tarnish someone's public image.⁷

CONSTITUTIONAL PERSPECTIVE

As discussed in the case "Justice K.S Puttaswamy vs Union of India" right to privacy is guaranteed by the Constitution, the right to privacy comes under Article 21. The idea of privacy is not related to secrecy rather it is directly proportional to a dignified life.⁸

In the case of deepfakes the Article 21 clearly gets undermined because deepfakes do not only target the privacy but also try to tarnish the reputation of an individual.⁹

The right to life isn't only about having a physical existence, it is also inclusive of living a life with dignity.¹⁰

CORE ISSUE

⁵ Mausam B. Noor, The Deepfake Prevention and Criminalisation Bill, 2023 (Private Member's Bill). The Bill was introduced in the Rajya Sabha.

⁶ Shrikant Eknath Shinde, The Regulation of Deep Fake Bill, 2024, Bill No. 193 of 2024 (India).

⁷ Id

⁸ Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

⁹ Id

¹⁰ Id

Even after all these provisions that can be applied to instances related to deepfakes, one issue still persists; that is “whether the existence of general provisions amounts to effectiveness of these provisions?”.

Moreover, Cybercrimes have been momentarily expanding its network. Similarly, there have been provisions, laws and acts related to cybercrimes but how much do they actually prevent? Even though deepfakes is a part of cybercrime but it is an enormous issue in itself because privacy is a crucial area of everyone’s life, the Constitution of India, itself recognises privacy to be a part of individual’s life, privacy is not something they can ask for rather it is something they can demand.¹¹

REAL LIFE SCENARIOS

Some real life instances that have been registered in recent times and these issues give us a clearer picture of what the damage done due to these deepfake videos could actually look like.

Around the mid of 2025 there was a highly circulated deepfake video of India’s Finance Minister, Smt. Nirmala Sitharaman. In that video she could be seen endorsing an investment platform which promises extremely high returns. The video was later clarified to be fake and AI generated. But the damage had been done, upon coming across that video a 71-year-old retired doctor from Hyderabad was duped around ₹20 lakhs due to the fake AI generated video.¹²

The case was booked by the cyber security wing of the Hyderabad police.¹³

Cases are registered under the general legal provisions like fraud but investigation becomes prolonged, due to limited traceability and anonymity.

Deepfakes sometimes also result from underlying vengeance, reports suggest that there have been 12 cases registered related to deepfakes in Karnataka alone, within the span of two years.¹⁴

¹¹ Id

¹² Hyderabad Doctor Duped by Fake AI Ad: Rs 20 Lakh Lost in Bitcoin Scam; Cybercrime Probe Launched, Times of India (June 18, 2025).

¹³ Id

¹⁴ Karnataka: Jilted Lover Created Deep Fake Photos of Love Interest and Her Friends, Arrested, OpIndia (Nov. 12, 2023).

In a similar case in 2023 from Khanapur, Belagavi, a man was arrested for creating and disseminating morphed images of a female colleague after she refused his advances, the action was done with the sole intent to tarnish her reputation.¹⁵

In 2024, a doctored video of Union Home Minister, Amit Shah was created in which he could be seen offering support for abolition of SC, St and OBC reservation. The video was fabricated and this was later clarified, the video was modified from a speech about a completely distinct topic.¹⁶

The video was created by opposition party workers.¹⁷

The above two cases reflect how a normal individual could suffer harm; it could be monetary or reputational harm. The third case reflects how such frivolously created deepfakes could cause political instability and could also result in civil unrest if they end up touching highly controversial and sensitive topics even if the intent is not sedition, these actions could lead to compromising of peace.

It is not hard to fathom how easily accessible such an advanced mechanism is to the general public, it poses a threat to not only the individuals residing but also towards the peace of the country. With the technology ceaselessly evolving everyday, the government shall be able to cope up with it by bringing legal evolution in the areas of cybercrimes and better parameters for the criminalisation of the act.

Because the existence of provisions never equals the effectiveness of provisions.

COMPARATIVE PERSPECTIVE

The issue of deepfakes is not bound by territory it is a global digital pandemic being faced by almost every country around the globe, we could get the insight from the recent “Take it down” act passed by The Parliament of the United States of America, it marks development of non consensual images of anyone without their consent and including the deepfakes formed

¹⁵ Id.

¹⁶ Amit Shah Deepfake Video: Viral Video Falsely Shows Home Minister Promising to End Reservations, BOOM (Apr. 30, 2024).

¹⁷ Id

by AI with the intent to harm, as a federal crime.¹⁸

The approach adopted by the United States differs considerably from India's approach towards deepfake-related harm. The "Take It Down" Act is specifically aimed at addressing non-consensual intimate content, including AI-generated content.¹⁹ While India has general provisions that can be applied to such issues, these provisions do not appear to be adequate to comprehensively deal with the emerging challenges associated with deepfakes.

The United States' "Take It Down" Act provides specific consequences for non-compliance, including enforcement by the Federal Trade Commission.²⁰ The Act also provides a dedicated mechanism through which victims can submit complaints.²¹ In cases of valid complaints, the content is required to be removed by the platform as soon as possible and not later than 48 hours after receiving the request, thereby attempting to prevent further dissemination of the content.²² Such measures provide victims with a more direct mechanism for seeking immediate action against harmful content.

The "Take It Down" Act has its own limitations and does not provide a complete solution to every form of deepfake-related harm. However, it represents a significant step towards specifically addressing the creation and dissemination of non-consensual intimate content and establishing mechanisms through which victims can seek removal of such content.²³

India recognises several forms of AI-related harm through its existing legal provisions, but falls short of having a similarly dedicated mechanism specifically focused on receiving complaints and providing remedies for harmful deepfake content.²⁴ The reliance on general provisions may make it more difficult to determine the appropriate legal provision applicable to a particular form of deepfake-related conduct. The situation becomes even more complicated when the creation or dissemination of such content involves individuals or platforms located across different jurisdictions.

¹⁸ TAKE IT DOWN Act, Pub. L. No. 119-12, 139 Stat. 55 (2025).

¹⁹ TAKE IT DOWN Act, Pub. L. No. 119-12, §§ 2(a), 3, 139 Stat. 55, 60–61 (2025).

²⁰ Id. § 3(b), 139 Stat. 61 (2025).

²¹ Id. § 3(a)(1)–(2), 139 Stat. 60 (2025).

²² Id. § 3(a)(1)–(2), 139 Stat. 60 (2025).

²³ TAKE IT DOWN Act, Pub. L. No. 119-12, §§ 2–3, 139 Stat. 55, 60–61 (2025).

²⁴ Information Technology Act, No. 21 of 2000, §§ 66C–66E (India); Bharatiya Nyaya Sanhita, No. 45 of 2023, §§ 111, 212, 353 (India); Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended (India).

The absence of a clearly defined and consolidated framework may create uncertainty regarding the classification of different forms of deepfake-related conduct, the liability of creators and platforms, and the remedies available to victims. The comparison therefore demonstrates that the central challenge is not merely the existence of laws, but the ability of those laws to provide an effective and timely response. The speed of removal, nature of accountability, accessibility of remedies and ability to address the cross-border nature of digital content are equally important factors in determining the effectiveness of a legal framework.

A more dedicated legislative framework may therefore benefit the public by providing greater clarity regarding their rights and the remedies available to them. It could also establish clearer responsibilities for platforms and provide a more structured mechanism for dealing with harmful AI-generated content while maintaining a balance with legitimate expression and technological innovation.

The main emphasis of this comparison is to highlight that Artificial Intelligence is a rapidly developing field which creates new legal challenges not only domestically but also globally. Therefore, addressing deepfake-related harm requires legal mechanisms capable of evolving alongside the technology. The effectiveness of a legal framework ultimately depends not only on whether it criminalises harmful conduct, but also on whether it provides accessible, timely and effective remedies to those affected.

CONCLUSION

Deepfakes present a growing legal challenge as technology continues to develop faster than existing laws. Although India has provisions that can be applied to deepfake-related offences, the analysis shows that the existence of such provisions does not necessarily ensure their effectiveness. The comparative approach further highlights the importance of dedicated mechanisms, timely content removal and clear accountability for platforms and creators. India therefore needs to strengthen its existing framework and develop more specific mechanisms to ensure that victims have accessible and effective remedies against deepfake-related harm.