



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.

DEEPFAKE CRIMES: IS INDIAN LAW READY?

~Jashandeep Kaur

INTRODUCTION

Imagine you received a voice note that sounds exactly like your father asking for an urgent bank transfer. Although this is not real, but no one can tell it is fake. This is no longer a hypothetical scenario but has become a harsh reality that deceives people. Now, deepfake technology is not confined to only film studios or viral celebrity hoaxes. It has become the most common and dangerous tool of fraud, harassment, and disinformation in the country. And the Indian law is only beginning to catch up to what that actually means.

MEANING OF DEEPFAKES

Deepfakes are used to fabricate sensitive or compromising videos of ordinary women, to clone the voices of the business owners or relatives for financial fraud. Deepfakes are used to implant evidence that does not even exist. It is used to make false speeches from politicians during election season. So, the problems caused by deepfakes are no longer speculative.

Initially, this technology was only used in film studios, but now it is accessible to everyone on free apps. India became well aware of deepfakes when a fabricated video of a well-known film actor went viral, and even the prime minister addressed it as a matter of national concern. As the technology keeps changing at a very high pace, and the Indian law is facing challenges to keep up with this pace. The deepfakes are providing the hardest test to the existing laws.

Deepfakes are used for committing crimes like identity theft, digital impersonation, financial fraud, cybercrimes, deepfake pornography and gender-based harm, which are the most dangerous forms of these offences. Deepfakes put eminent danger to democratic institutions.¹

¹ Isha Goel, *Deepfake Technology and Criminal Liability in India: Are India's Existing Criminal Laws Sufficient to Deal with AI-Generated Deepfakes?* 8 Indian Journal of Law and Legal Research Iss. III, 5694 (2026).

LEGAL CHALLENGES REGARDING DEEPPFAKES

In India, there is a lack of statute which particularly deal with deepfakes. The prosecution has to depend upon indirect existing provisions in other statutes, although these indirect existing provisions are never drafted for deepfake crimes. The sections of cheating by impersonation, forgery, defamation, or stalking of Bharatiya Nyaya Sanhita are used to prosecute the accused.² In addition to these provisions, the Information Technology Act is also applied. For example, section 66C is used in cases of identity theft caused by deepfakes, and section 66E is used if there is a violation of privacy by deepfakes. If the deepfake circulates content of a sexual nature, then section 67A of It act is invoked by the prosecution, as this section criminalises the publication of sexually explicit material.³

GAPS IN THE LEGAL SYSTEM OF INDIA

The main issue is that the provisions mentioned above are actually applicable to real videos or photos. So, these provisions are not directly applicable to synthetic or fabricated content. This creates a grey area in the legal system of India. For example, section 66A of the IT Act, 2000 deals with the publication or transmission of sexually explicit material, but it is silent about AI-generated content that never actually exists. Although this section can be invoked but ground reality is that it was not specifically designed to deal with synthetic media. The actual injury in the deepfake case is not that something obscene was shared, but the real harm is that the person, without consent, was made to appear in an act which he has nothing to do with. This is not only a question of decency but also a violation of dignity and anonymity, and it is broader than the obscenity problem.

STEPS TAKEN BY THE GOVERNMENT

The government of India has taken a step toward deepfake crimes. It started to respond to the challenges imposed by the deepfakes. In October 2025, the Ministry of Electronics and Information Technology released draft amendments to the Information Technology (intermediary guidelines and digital media ethics code) Rule, 2021, for consultation of public. The amendment provided for the proposal of a statutory definition of “synthetically generated information” (SGI). After considering the consultation of the stakeholders, on 10 February 2026, the amendments were officially notified, and on 20 February 2026, these amendments came into force. This amendment is important to note because it is the first time that the Indian

² *Bharatiya Nyaya Sanhita*, No. 45 of 2023 (India).

³ *Information Technology Act*, No. 21 of 2000 (India).

law expressly recognises AI-generated content within the regulatory framework. It marks the beginning of addressing problems caused by the deepfakes. Along with the definition, the amended rules now require labelling. It means that the platforms which allow the generation of AI content must ensure it carries a visible disclaimer. So that viewers can know that what they are watching is not real. The most significant amendment is on takedown timelines. Now platforms are required to remove flagged deepfakes immediately within hours instead of waiting for orders from the court. If the platforms failed to act immediately, it could cost a platform its safe harbour protection under section 79 of the IT act, the shield which has historically protected the intermediaries from liability for what the users post.⁴

SUGGESTIONS

The job is still not fully done. Existing laws enable authorities to prosecute offences committed through deepfakes. But the current legal system is reactive in nature. There is a lack of preventive laws. India should form a comprehensive legal framework that provides a statutory definition of deepfakes, imposes criminal penalties for the malicious creation and distribution of harmful deepfakes, and invests in AI-based forensic detection tools. There should be specialised cybercrime training for police, prosecutors and judges. There should be strong safeguards to protect privacy, dignity, and digital identity. There should be public awareness campaigns on identifying manipulated media. In this way, the threat of deepfakes can be reduced.

⁴ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (as amended by the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026)