LEGAL AMENITY LAW JOURNAL – ISSN 3107-9148

Volume II Issue II March – April 2026

DEEPFAKE PORNOGRAPHY AND THE LAW IN INDIA

By: - Varsha Nair

Law Student, Vivekanand Education Society's College of Law Chembur.

ABSTRACT

The rapid advancement of artificial intelligence has significantly transformed the creation and dissemination of digital content, giving rise to technologies such as deep fakes. While deep fake technology has legitimate applications, its misuse, particularly in the creation of nonconsensual pornographic content, has emerged as a serious legal and ethical concern. This research article examines the scope and implications of deep fake technology, focusing on its impact on fundamental rights such as privacy and dignity under Article 21 of the Constitution of India[1].

The study highlights how deep fake pornography violates individual autonomy, causes reputational harm, and disproportionately affects women. It further analyses the inadequacy of the existing legal framework in India, including provisions under the Information Technology Act, 2000 and related criminal laws, in effectively addressing AI-generated harm. The article also identifies key challenges such as difficulties in detection, lack of a dedicated legal framework, insufficient penalties, and issues relating to intermediary accountability.

A comparative perspective is provided by examining regulatory approaches adopted in other jurisdictions. The article concludes by emphasizing the urgent need for specific legislation, stronger enforcement mechanisms, victim-centric remedies, and increased digital awareness to address the growing misuse of deep fake technology. It argues that timely legal reform is essential to ensure that technological advancements do not undermine fundamental rights and human dignity in the digital age.

[1] *The Constitution of India, 1950, art. 21*

Keywords: Deepfake pornography, Artificial intelligence regulation, Right to privacy and dignity (Article 21), Cyber law in India, Intermediary liability, Gendered online abuse, Digital rights and ethics.

INTRODUCTION

Artificial intelligence is growing and changing quickly in this digital age, which has a big effect on the kinds of content that are made today. Deep fake technology is one of the most talkedabout developments. It lets people make videos that look real but aren't real, which means they were made with AI. Artificial intelligence has become an integral part of everyday life, yet its potential risks are often overlooked.

Deep fake has many uses that are useful, especially in entertainment and media. However, it is also often used in the wrong way, which is very worrying. Deep fake technology has been used in the last few years to make pornographic content without the person's permission, which raises serious legal and moral questions. This means changing a person's image or identity and putting them in sexual situations without their knowledge or permission. These actions not only infringe upon an individual's autonomy but also undermine the concept of consent in the digital era. The consequences of deep fake pornography can be severe. The seriousness of the issue was highlighted in a widely reported incident involving Rashmika Mandanna[2], where a deep fake video falsely depicted her in an explicit context. The incident sparked widespread public concern and brought attention to the urgent need for stronger legal safeguards against such misuse. It directly impacts an individual's privacy, dignity, and reputation, frequently resulting in emotional distress, social stigma, and enduring harm to personal and professional life. This has a big effect, especially on women, who are often the main targets and are treated badly because of it. In India, the quick spread of internet access and social media has made it easier for this kind of content to be made and shared quickly. Even though the problem is very serious, India's laws are still not fully ready to deal with it. Because there aren't enough specific laws and the current cyber laws aren't strong enough, it's hard to punish criminals and help victims quickly. This research article explores the scope of deep fake technology and analyses how it has evolved into a tool of harm against individuals in today's digital age.

[2] *"Rashmika Mandanna Deep fake Video Sparks Concern," The Indian Express (2023).*

CONCEPT OF DEEP FAKE TECHNOLOGY

Deep fake technology refers to the process of creating or editing audio-visual content to make it appear incredibly realistic. The term "deep fake" is formed by combining the words "deep learning" and "fake" with the use of strong machine learning algorithms to create false information. A persons face, voice or expression can be altered or layered on another person's body using this very technology, giving off the impression that they are saying or doing things they normally never would. Deep fakes are made using deep learning[3] models, specifically neural networks, which assess and duplicate patterns in photos, videos, and voice.

The final product received from the algorithms that are trained on vast datasets accurately mimic facial movements and speech as well as expressions, which makes it impossible to identify genuine content without using specific tool or equipment. Deep fake apart from entertainment purposes also has potential applications in education, virtual reality, and accessibility aids, such as reproducing voices for people who have lost the capacity to speak. These examples emphasize that beneficial potential do arise from technological advances if used appropriately.

But no doubt the same technology is frequently used for malicious reasons. Deep fakes have been used to create misleading videos, spread false information, and sway public opinion. This raises significant ethical issues as well as challenging legal issues, particularly with regard to controlling such information and protecting victims. It has also been misused in the political sphere to create misleading videos, thereby influencing public perception and raising concerns about its impact on democratic processes.

IMPACT ON PRIVACY AND DIGNITY

The essential fundamental rights of privacy and dignity[4] are severely violated due to deep fake pornography, as it degrades both dignity and private life itself. Both of these components are protected under Article 21 of the Constitution of India. The right of privacy was established in Justice K.S. Puttaswamy v. Union of India[5] which reiterated that control by an individual over their personal information, identity, and image is a fundamental right.

[3] *Apar Gupta & Rishika Singh, Deep fakes and the Law in India, Internet Freedom Foundation (2021).*

Putting a person's face in a deep fake without permission violates his/her legal interest of protection of name and image, which means that people lose control over their own digital image. The author of the deep fake moreover is simply taking over someone else's likeness, blatantly disregarding the dignity of the person for his own ideas. And what makes it worse is that most of the people who are affected by this just go unnoticed, or they themselves don't know that such type of content with their face on it exists, this is how dangerous deep fake has become. Majorly because how easily it has become available, there are free tools and apps online allowing anyone on the internet to misuse your video for pornographic content and you wouldn't even be aware about it.

Certainly without consent there exists deep fakes that show individuals naked or doing pornographic things. This is tantamount to making an explicit and pornographic video with another person. Deep fake pornography not only infringes on privacy; it also runs counter to the "right to live a life in dignity" stated in article 21 of India's Constitution. The creation and dissemination of explicit content without consent also makes people victims of shame, turns them into objects to be gazed upon with objectification, and does great moral harm to other people. Such content not only distorts reality but harms the social status of victims, and often leads to irreversible consequences.

The consequences of violating privacy are severe but also affect the lives of victims in other ways. For instance, individuals subjected to deep fake pornography suffer psychological distress, symptoms consistent with clinical depression and stigma from society at large for their constant viewing over personal computers or iPhones. Because digital content spreads so quickly and uncontrollably, their personal and professional connections may suffer, and in many circumstances, the harm to their reputation is long-lasting. Women are disproportionately affected because they are more often targeted and face more scrutiny and criticism from society. Another popular example can be of Mrs. Alia Bhatt[4], Similar concerns were raised in instances involving Alia Bhatt, where manipulated content was circulated online without consent, highlighting the serious invasion of privacy and reputational harm caused by such technologies.

[4] *"Deep fake Videos and Privacy Concerns in India," The Hindu (2023).*

EXISTING LEGAL FRAMEWORK IN INDIA

As of now there are no clear legislative restrictions that regulate the creation and use of deep fake technology, neither are there any clear safeguards laid down and neither are the people completely aware of the atrocities this has caused. Instead, reliance is placed on existing provisions under cyber and criminal laws, which are often inadequate in dealing with technologically advanced offences.

Under the Information Technology Act, 2000[5], certain provisions attempt to address privacy violations and obscene content. Section 66E deals with the violation of privacy by capturing, publishing, or transmitting images of a private area without consent. Similarly, Sections 67 and 67A criminalise the publication and transmission of obscene and sexually explicit material in electronic form. While these 4 provisions may be applied to cases involving deep fake pornography, they do not explicitly recognise or address AI-generated or manipulated content, leading to ambiguity in interpretation.

In addition to the IT Act, provisions under criminal law, including those relating to defamation and offences against the modesty of women[6], can also be invoked. However, these provisions are indirect and were not designed to address digitally fabricated content, thereby limiting their effectiveness in tackling deep fake-related harm.

Information Technology Rules (Intermediary Guidelines and Digital Media Ethics Code) [6]exist to regulate content available on social media platforms, however their implementation takes time, it's effectiveness is therefore reduced due to long delays in resolution.

Overall, while existing laws provide some level of protection, they are not sufficiently equipped to address the unique challenges posed by deep fake pornography.

ISSUES AND CHALLENGES

Several legal and practical challenges accompany the regulation of deep fake pornography in India. One of the primary issues is the absence of a dedicated legal framework [7]specifically

[5] *Indian Penal Code, 1860, Sections 499, 500, 354C, 509.*

[6] *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. 499*

[7] *Internet Freedom Foundation, "Regulating Deep fakes in India" (2021), available at: https://www.internetfreedom.in*

addressing deep fake technology. This creates uncertainty in the application of existing laws and makes prosecution more complex.

Detecting and proving deep fake content proves to be another significant challenge. As Artificial intelligence keeps on upgrading, the quality and quantity of generated content keeps increasing making it difficult to differentiate from real and reel content, as a result complicating evidentiary processes.

Additionally, the penalties under existing laws are often inadequate when compared to the severity of harm caused. This reduces the deterrent effect and fails to address the long-term consequences faced by victims.

The rapid availability and sharing of content on digital platforms further aggravates the problem. Once such content is uploaded, it can spread widely and quickly, making effective removal and damage control extremely difficult.

As mentioned before, the role of intermediaries remains a concern. Social media platforms often respond too slow to takedown requests, and the lack of strict accountability mechanisms allows harmful content to remain accessible for longer durations.

Lastly, there is a lack of awareness and digital illiteracy among users, which increases vulnerability to such forms of misuse and limits the ability of individuals to seek timely remedies.

COMPARATIVE ANALYSIS

Such technology and its risks have been identified by several countries as critical and they have taken major steps to regulate any misuse. For instance, in the United States, certain states have introduced laws specifically targeting the use of deep fakes in non-consensual pornography and political misinformation[8]. As seen in the case of Taylor Swift[12], where AI-generated explicit images were widely circulated, demonstrating the global scale and seriousness of the issue. Similarly, the United Kingdom has considered legal reforms to address the creation and

[8] *U.S. Congressional Research Service, "Deepfakes and National Security" (2020).*

distribution of intimate images without consent, including those generated through artificial intelligence[9].

There has risen a global growth in the recognition of the need to regulate such technology. In comparison, India's reliance on general cyber laws highlights the absence of a targeted legal response.

CRITICAL ANALYSIS

The current legal framework in India reflects a significant gap [10] between technological advancement and legal regulation. While existing provisions under the IT Act and criminal law offer some degree of protection, they are not designed to address the complexities associated with AI-generated content.

The lack of strict explicit recognition of deep fake technology creates ambiguity in legal interpretation, leading to contradictory application of laws. This undermines the effectiveness of the Indian legal system in addressing such offences.

The limited availability of compensation mechanisms and the lack of quick remedial measures make it evident that this legal system lacks a victim centric approach.

Intermediaries must also be scrutinised more closely. The existing system does not impose sufficiently strong requirements on platforms to proactively detect and remove harmful information, consequently allowing deep fake material to spread widely.

This inadequacy of the existing framework clearly highlights the need for urgent reform to ensure that the law can match its pace with technological developments.

SUGGESTIONS AND RECOMMENDATIONS

In light of the challenges identified in this research article, several measures can be adopted to address the issue of deep fake pornography in India.

[9] *European Commission, "Proposal for Artificial Intelligence Act" (2021).*

[10] *Rebecca Delfino, "Pornographic Deepfakes: The Case for Federal Criminalization," 51 University of Richmond Law Review 987 (2019).*

- Deep fake technology needs to be directly regulated and criminalised for its misuses which requires the enactment of specific legislation, particularly in cases involving nonconsensual content.
- existing cyber laws should be amended to explicitly include AI-generated and manipulated content within their scope, thereby reducing ambiguity in interpretation.
- To reflect the severity of harm caused, along with provisions for victim compensation and rehabilitation, stricter penalties should be introduced.
- there is a need to establish fast-track mechanisms for the prompt removal of harmful content from digital platforms, ensuring timely relief for victims.
- Imposing stricter compliance requirements and penalties will strengthen the accountability of social media intermediaries.
- Finally, efforts should be undertaken to increase digital literacy and awareness among users in order to reduce susceptibility and encourage responsible use of technology.

If timely action is not taken, the impact of deepfakes will continue to grow, making it increasingly difficult to distinguish between reality and manipulation.

CONCLUSION

Deep fake pornography poses a significant threat to the protection of privacy and dignity in the digital era. While technological improvements have provided several benefits, their misuse has revealed substantial weaknesses in the current legal framework. The current rules in India, while somewhat applicable, are insufficient to effectively address the intricacies of AIgenerated harm. The lack of explicit legislation, along with enforcement obstacles, leaves victims vulnerable and unable to seek timely relief. There is an urgent need for thorough law change, better institutional systems, and proactive regulation. Addressing these challenges is critical to ensuring that technological advancement does not come at the expense of fundamental rights and human dignity.