



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.

DEEPFAKES AND THE LAW: FROM IT ACT 66E TO BNS

By: Lakshika Sharma

INTRODUCTION

As we progress towards a developed society, juggling through the technological inventions, working towards our development, we come across instances that the world didn't anticipate. Stephen Hawking, while acknowledging the revolutions that await human life, quotes **"Success in creating AI could be the biggest event in the history of our civilization. Or the worst. We just don't know."** Digital communication has enabled revolutionary changes in the world of creation. The creation of realistic images, audios and visuals have catalysed the process of education, healthcare, entertainment as well as filmmaking. However, it has also increased the number of cybercrimes not just in number but also in types.

At present, one of the biggest challenges we face is that of deepfakes. The amount of information that circulates today imitating not just images but even voices, is not just astonishing but also scary and the world is yet to witness its horrors but women have already started facing them. The use of deepfakes is now not just limited to fun and educating content but is now used for financial fraud, election manipulation, identity theft, cyberbullying, defamation, etc. Even the issue is getting acknowledged yet it is not receiving enough recognition as an emerging threat to democracy, privacy, public order as well as security issues.

SAFEGUARDING PROVISIONS IN INDIA

The issue of deepfakes is still under consideration and is yet to find a special act for itself. Nevertheless, there still exists some provisions that can be used including provisions from the

Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 as well as Bharatiya Nyaya Sanhota, 2023.

THE WAVE OF DEEPPAKES

The literal translation amounts to “deep learning” and “fake”.term **"deepfake"** combines the words **"deep learning"** and **"fake."** It is a process through which the neural networks analyse and learn a number of patterns using a huge amount of data generating some synthetic but realistic content. It includes analyzing huge amounts of data relevant to face expressions, voice modulations, non-verbal movements, etc. These are so realistic that it becomes extremely difficult for a layman to differentiate between real and fake.

The process of deepfakes usually starts with a huge amount of data collection functioning in depth, training models using certain diffusion models. The AI models thus trained are then used to generate synthetic content which is then improvised and improved to look real-like. Even though such manipulation to images has been existing for a long time, the intensity and depth has become extremely real to understand the difference between true and false, in addition to their realism also comes the easy accessibility and low effort, making it highly prone to misuse and manipulation. The use of large language models (LLMs) and such similar provisions are the primary reason for such lowered barriers as well as such wide usage.

DEEPPAKES - A COMPLICATED LEGAL CHALLENGE?

Conventional cyber laws have proved not to be adequate for the current legal challenges that face the world. International use of deepfakes to manipulate election information, corporate fraud, impersonate leaders, and produce sexually explicit content, have been seen not just as violation of democratic principles but also a threat to individual rights as well as national security. One deepfake alone has the potential to cause identity theft, violation of privacy, copyright, defamation, etc.

In order to deal with the above, the Indian legal system uses a number of statutory provisions. It has been reiterated time and again that offences related to deepfakes would particularly be dealt under Bharatiya Nayaya Sanhita 2023 as well as Information Technology Act, 2000.

I INFORMATION TECHNOLOGY ACT, 2000

SECTION 66C

The section particularly deals with identity theft. This is inclusive of any dishonest as well as fraudulent use of an individual's password, electronic signature or any such unique identification feature. As already mentioned, deepfakes have the capacity to create a realistic face identity, voice and even biometrics, thus, such provision provides a safeguard from the same. Thus, any AI generated video with the face as well as voice of any political figure to misguide the public amounts to an offence under section 66C of the Act. The punishment for the same can be extended up to 3 years of imprisonment along with a fine which can extend up to an amount of Rs. 1 lakh.

SECTION 66D

The section deals with cheating by personation using either computer resources or even communication tools. It tends to criminalise it with a term of imprisonment extendable up to 3 years and a fine which can be extended up to an amount of Rs. 1 lakh. Thus, use of such technology to make transfers, invest, reveal information, etc through personation is an offence.

SECTION 66E

Privacy stands as part of our fundamental rights and therefore must be protected and thus, any violation of the same is dealt with under this section. Thereby, it tends to criminalise any intentional, transfer, capture or publishing of any personal areas or any such personal information of a person without their consent amounts to such violation. The fine can go up to Rs. 2 lakh or an imprisonment of up to 3 years or even both.

SECTION 67

The transmission or publication of obscene content has been criminalised through this section. Such content which humiliates a victim, tarnishes reputation, harass women, etc can be punished with a fine of up to Rs. 5 lakhs and imprisonment of up to 3 years.

SECTION 67A

The publication as well as electronic transfer of any explicitly sexual act or even conduct. Thus, the section is of significant importance as it provides protection against AI generated explicit sexual content being either transferred or published, with punishment going up to Rs. 10 lakh and imprisonment up to 5 years.

SECTION 67B

Any act either to create or to transfer or to publish or browse, download , collect or advertise any content that is sexually explicit and includes children, then such crime would be punishable under this section.

II THE INFORMATION TECHNOLOGY (INTERMEDIARY GUIDELINES AND DIGITAL MEDIA ETHICS CODE) RULES, 2021

It is important to understand that criminalising conduct is not enough, there is an urgent need of active prevention. Such need is looked upon by this act which incorporates intermediaries and places obligations upon them to protect the users. There have been repeated advisories by varied Government departments including the Ministry of Electronics and Information Technology, advising the public to take down any AI content that is in violation of IT Act or Rules.

DIGITAL PERSONAL DATA PROTECTION ACT, 2023

Deepfakes as discussed can be violative of personal data like face features, voice, biometrics, etc which can bring it under the purview of the **Digital Personal Data Protection Act, 2023**. Under the act, legal grounds require informed consent, security, protection from unauthorised sharing of data and other such acts that need to be scrutinized as necessary. However, it should be noted that no specific mention of deepfakes has been made anywhere.

THE BHARATIYA NYAYA SANHITA, 2023

The act came into force on 1st of July, 2024 replacing the old Indian Penal Code 1860. Bharatiya Nyaya Sanhita provides for certain offences that can be accommodate within the ambit of crimes related to deepfakes and AI violations. AI is now being increasingly utilised

to defame, fraud, exploit, intimidate and deceive and all such actions call for varied sections under the Act.

1. CHEATING BY PERSONATION - SECTION 319

We have already briefed about a similar provision under the Information Technology Act, a similar of which is dealt with under the BNS. Use of AI to impersonate someone can be a punishable offence under the above section and thereby caution must be maintained at all times.

2. FORGERY & USE OF FORGED RECORD & MAKING A FALSE DOCUMENT - SECTIONS 336, 340, AND 335

BNS deals with the offences of forgery and use of forged documents which can be used as The BNS retains offences concerning **forgery**, recognising that false electronic records may be used to deceive others. Fabricated content is most likely depending on the fact and circumstances of the case be categorized and punished under these sections. This is also important as the new age has increased the admissibility of digital evidence thus in order to protect such evidences, more stringent action must be taken.

3. DEFAMATION - SECTION 356

Defamation has been extensively provided for in the act. The provision tends to protect the reputation of a person. The general principle of reputation remains that the content should not lower the reputation of a person in the eyes of right-thinking members of society or a reasonable person. Thus, if the content is violative of it, it can be challenged under the relevant section.

4. EXTORTION & CRIMINAL INTIMIDATION - SECTION 308 & SECTION 351

It is seen that deepfakes and manipulated videos, audios and other such content has been used to blackmail, stalk, harass and manipulate people. In order to punish such individuals, BNS provides for offences of criminal intimidation and extortion which can be applied for such digital offences given the facts of the case.

5. OFFENCES AGAINST WOMEN

A lot of cases involve sexually explicit content against women and their modesty and such cases may be tried as per various sections as provided under Chapter V of BNS, thereby protecting women from such offences and punishing those who need to be punished.

CONSTITUTIONALISM IN THE ERA OF DEEPFAKES

The Constitution is not merely a document of law but is an ever expanding set of principles that guide us through for the functioning of a civilised society. In the era of technology that has expanded its dimension to misuse and criminal offences, constitutionalism steps in to protect the people and stand for the people. However, the question of a balance between freedom of privacy combined with reputation, privacy and digital advancement becomes all the more important in the absence of special laws regulating the new advancement. Article 19 and Article 21 have been significant in protecting the dignity of an individual but with the new age and era, they need to be protected even more fundamentally in order to increase and diversify its corpus of protection. Constitutionalism stands for not just protecting illegitimate but also protecting the legitimate, thereby, any interpretation must be incorporative and protective against and of both.

GAPS AND RECOMMENDATIONS

India is working towards digital development and therefore restrictions should not be the primary focus. Currently, we lack not just definition but also some essential provisions of proper disclosure and consent. It further gets aggravated with slow redressal mechanisms and with the uncertainty of jurisdiction of such cases, the issues remain unresolved for even greater durations. A proper adaptation of clear laws with clearly defined terms clubbed with greater transparency and accountability can be a great step towards better regulation. It is important to make the right people accountable including the intermediaries with greater responsibility attached to all involved. This should also be combined with greater awareness measures and speedy redressals.

CONCLUSION

In order to work towards something, it is necessary to define it first. They say half the problem is resolved once written, but for deepfakes and AI technology as much as necessary, there exists some exponent issues which makes it even more difficult especially when it

comes to content like satire and humorous content. The recent protests at CJP against NEET exam leak, saw some of the most hilarious content, some leaving us really wondering about what's happening, the slogans, the reels, short videos, posters everything depicted a sense of frustration combined with satire but the issue remains as to where to draw a line. A clear, well-researched, and inclusive definition can be a good starting point for a better regulatory system. A more responsible development, transparent mechanisms, greater accountability and swift action should be the way forward towards balancing the use without actually restricting development.

REFERENCES

- Mansoor, S. I. U. (2024). Legal Implications of Deepfake Technology: In the Context of Manipulation, Privacy, and Identity Theft. *Central University of Kashmir Law Review*, 4, 65–92. <https://doi.org/10.66498/CUKLR.4.2024.65-92>
- Minhas, N. R., & Sonkhla, D. (2024). *Exploring legal and technical challenges of deep fakes in India*. *International Journal for Multidisciplinary Research*, 6(4), Article IJFMR240424793. <https://www.ijfmr.com/>
- Panwar, K. S., & Roy, N. D. (2024). *Rising menace of deepfakes with the help of AI: Legal implications in India*. *Indian Journal of Integrated Research in Law*, 4(3).
- *Deepfakes in the AI era: Legal challenges, comparative analysis, and the need for regulatory reform*. (2025). *Advanced International Journal for Research*, 6(4), AIJFR25041117. <https://www.aijfr.com>
- Srivastava, S. (2025). The danger of deepfakes, Indian laws and platform responsibility. *International Journal of Intellectual Property Management*, 15(1), 60–76. <https://doi.org/10.1504/IJIPM.2025.145164>
- Kaushik, P. (2024). Deepfakes and Indian laws. In R. Chandra, A. Chaturvedi, & A. Pant (Eds.), *Artificial intelligence and law: Emerging legal challenges* (pp. 214–229). Springer. https://doi.org/10.1007/978-981-97-9586-4_12

